T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

YAPAY ZEKÂ TEKNOLOJİLERİNİN CEZA MUHAKEMESİNDE KİŞİSEL VERİ TOPLANMASINA ETKİLERİ

DOKTORA TEZİ

Irmak ERDOĞAN

Tez Danışmanı: Prof. Dr. Vesile Sonay EVİK

ARALIK 2021

T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

YAPAY ZEKÂ TEKNOLOJİLERİNİN CEZA MUHAKEMESİNDE KİŞİSEL VERİ TOPLANMASINA ETKİLERİ

DOKTORA TEZİ

Irmak ERDOĞAN

Tez Danışmanı: Prof. Dr. Vesile Sonay EVİK

ARALIK 2021

ÖNSÖZ

"Yapay Zekâ Teknolojilerinin Ceza Muhakemesinde Kişisel Veri Toplanmasına Etkileri" tezinin ve araştırma görevliliği yaptığım sürecin her aşamasında çok büyük destek olan ve kendisinden çok şey öğrendiğim danışmanım ve kürsü hocam Prof. Dr. Vesile Sonay Evik'e özel teşekkürlerimi sunarım.

Türk doktrininde henüz bir tez kapsamında ele alınmamış bu alanda kaynak toplamak ve özellikle profilleme teknolojilere uzun süredir başvurmakta olan ülkelerde araştırma yapmak özel bir öneme sahipti. Bunu mümkün kılan Prof. Dr. Sabine Gless'e İsviçre Mükemmeliyet Hükümet Bursu'nu kazanmamdaki desteği, çalışmamı Basel Üniversitesi'nde sürdürmemi mümkün kıldığı ve teze sunduğu katkılar için teşekkürlerimi sunarım. Yine Floransa Üniversitesi'nde karşılaştırmalı araştırma yapmamı mümkün kılan Prof. Dr. Michele Papa'ya teşekkür borçluyum.

Jüri üyelerim Prof. Dr. Zeynel Kangal, Doç. Dr. Güçlü Akyürek, Prof. Dr. Pınar Memiş Kartal ve Doç. Dr. Eylem Aksoy Retornaz'a teze katkıları ve detaylı önerileri için, sevgili araştırma görevlisi arkadaşım Selin Türkoğlu'na hem kürsüde hem kürsü dışında destekleri için özel teşekkürlerimi sunarım. Yine Galatasaray Üniversitesi kürsü başkanı Prof. Dr. Ümit Kocasakal'a farklı üniversitelerde araştırma yapmamı destekleyerek tezin yazımını mümkün kıldığı, kürsü arkadaşım Mehmet Gürler'e kürsü arkadaşlığı ve yardımları için teşekkürlerimle. Ayrıca Dr. Öğr. Üyesi Öznur Sevdiren'e ve Dr. Öğr. Üyesi Ali Pehlivan'a akademik hayatımın her aşamasında ilgi ve destekleri için teşekkürlerimi sunarım.

Diğer bir teşekkürü ise Bilgi Üniversitesi ve Galatasaray Üniversitesi'nde birlikte ders işlediğimiz, bana araştırma görevliliğini çok sevdiren ve çok şey öğrendiğim tüm mezun ve öğrencilere iletmek isterim.

Son olarak aileme, hiçbir zaman azalmayan güven ve destekleri için sonsuz teşekkürlerimle.

İÇİNDEKİLER

KISALTMALAR

AB	: Avrupa Birliği
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AYM	: Anayasa Mahkemesi
Bkz.	: Bakınız
C.	: Cilt
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CMK	: Ceza Muhakemesi Kanunu
E.	: Esas Numarası
Ed.	: Editör
FSEK	: Fikir ve Sanat Eserleri Kanunu
GDPR	: General Data Protection Regulation
K.	: Karar Numarası
KVKK	: Kişisel Verilerin Korunması Kanunu
LSI-R	: Level of Service Inventory-Revised
m.	: Madde
PAT	: Pre-trial Risk Assessment Tool
PTRA	: Factors Rated Federal Pretrial Risk Assessment
PVSK	: Polis Vazife ve Salâhiyet Kanunu
R.G	: Resmi Gazete
s.	: sayfa
SPG	: Sicherheitspolizeigesetz
ss.	: sayfalar
StPO	: Strafprozeßordnung
T.	: Tarih
TCK	: Türk Ceza Kanunu
TKK	: Tanık Koruma Kanunu

RESUMÉ

Les technologies d'intelligence artificielle ont permis la collecte et l'analyse de quantités illimitées de données. Les technologies de profilage effectuent principalement des analyses de données. Ces technologies inférent des traits de caractère généraux des individus à partir de plusieurs bases de données qui révèlent leur classe, leur statut économique et social. Ensuite, ils déterminent si ces caractéristiques présentent un risque pour la société. Leur utilisation dans les procédures pénales transforme les procédures pénales en un outil de lutte contre les personnes dites à risque et menace inévitablement de nombreux droits et libertés. Néanmoins, cette thèse évalue principalement les menaces envers la protection des données personnelles.

La thèse évalue les technologies d'analyse des risques, qui sont devenues de plus en plus compliquées, en raison des progrès de l'apprentissage automatique. La principale préoccupation de la thèse est de répondre s'il est possible de bénéficier des normes de protection des données personnelles dans les procédures pénales lorsque les technologies de profilage sont appliquées dans les procédures pénales.

L'utilisation du profilage au cours d'une procédure pénale nécessite d'examiner la réglementation relative aux données personnelles, mais il est également nécessaire d'évaluer les principes et mesures de base des procédures pénales. Ainsi, la thèse cherche à interroger davantage la conformité des outils de profilage avec les principes et règles des procédures pénales. Il évalue la nature juridique des technologies de profilage et examine la valeur probante des résultats obtenus par le profilage.

La recherche consiste principalement en une recherche documentaire examinant les réglementations en matière de protection des données et de procédure pénale dans une perspective comparative. Ainsi, les livres, articles et publications pertinents, ainsi que les décisions de la Cour suprême, de la Cour constitutionnelle et de la Cour européenne des droits de l'homme sont évalués. En outre, différentes jurisprudences étrangères sur la valeur probante des technologies de profilage sont élaborées en détail. Enfin, l'acquis de l'Union européenne et les rapports des organisations non

gouvernementales sont examinés pour montrer les applications actuelles des technologies de l'IA et les meilleures pratiques.

Les outils d'analyse des risques nécessitent une connaissance à la fois de la technologie et du droit. Il n'est pas possible de réglementer ces technologies sans comprendre les modèles et concepts de base du profilage. Par conséquent, dans la thèse, les termes tels que intelligence artificielle, algorithme, apprentissage automatique, apprentissage basé sur des règles sont d'abord introduits. Ensuite, les modèles d'apprentissage conformes aux principes des procédures pénales et de la loi sur la protection des données ont été soulignés. De plus, des technologies de profilage dans la justice pénale sont introduites. Ces technologies visent soit à détecter les auteurs potentiels, soit les scènes de crime potentielles. Afin d'expliquer leur fonctionnement, les théories criminologiques sous-jacentes telles que "la théorie de la vitre brisée" et "la théorie de la quasi-répétition" sont discutées. En outre, les types de données qui conduisent aux sorties de profilage sont exposés. Ce chapitre est crucial pour montrer que les outils déjà utilisés en Europe et aux États-Unis ont permis d'identifier des personnes d'une certaine classe, d'un certain style de vie et d'une certaine vision du monde comme groupes à risque ou de marquer des quartiers minoritaires comme zones à risque.

Les technologies de profilage attribuent des scores de risque aux individus en fonction de leur identité et de leur personnalité, mais ils ne sont pas basés sur l'acte criminel en question. Il est très crucial de leur fixer des limites, car les scores de risque étiquettent les gens et les impactent presque perpétuellement. Dans ce contexte, les réglementations sur la protection des données, qui fixent pour la première fois des limites au profilage, nécessitent une analyse approfondie. Au sein de l'Union européenne, le Règlement européen sur la protection des données ("RGPD") et la Directive 2016/680 constituent les principales réglementations en matière de profilage. S'agissant de la Turquie, la loi sur la protection des données personnelles ("KVKK") contient des réglementations importantes concernant le processus de profilage et le traitement des données en général. Compte tenu de ces réglementations, afin de bénéficier des garanties de protection des données, tout d'abord, les technologies concernées doivent traiter les données personnelles. Cependant, la définition des données personnelles doit être reconsidérée, car les nouvelles technologies remettent

en cause la dichotomie entre données anonymes et données identifiables, alors qu'elles rendent presque tout le monde identifiable en combinant et en analysant différents ensembles de données. De plus, ils provoquent des effets juridiques sur certaines personnes. Par conséquent, à la lumière de la jurisprudence, des recommandations et des rapports du groupe de travail sur l'article 29 au sein de l'UE, les données à caractère personnel devraient être considérées de manière plus large. D'autre part, il convient de noter que même dans le cadre des procédures pénales, le règlement général sur la protection des données pourrait s'appliquer. Dans la plupart des cas, les processus de collecte et d'analyse des données sont initiés par des entreprises privées. Par conséquent, au sein de l'UE, pour le profilage dans le contexte de la justice pénale, les dispositions du RGPD peuvent être directement applicables. Dans les cas où les autorités répressives ou judiciaires traitent des données pour détecter et poursuivre des infractions, le règlement plus spécifique, la directive 2016/680, s'appliquera. Comme les deux réglementations étant pertinentes en matière de profilage, elles sont toutes deux analysées de manière approfondie. La thèse démontre que l'utilisation de technologies de profilage telles que COMPAS, SyRI, PSA, Static 99 dans de nombreux pays ne suit pas les principes de limitation des finalités, de minimisation des données et de proportionnalité. En outre, la thèse traite du droit de ne pas faire l'objet d'une décision fondée exclusivement sur un procédé automatisé. Au sein de la Turquie, les réglementations concernant le profilage dans le cadre du KVKK sont évaluées par rapport à l'acquis de l'UE. KVKK prévoit de nombreuses limitations et exceptions pour le traitement des données via les autorités judiciaires, la police et les procureurs. La thèse vise à souligner les lacunes juridiques au sein du KVKK et souligne l'absence d'une réglementation distincte telle que la directive 2016/680.

Les lois sur la protection des données personnelles prévoient de nombreux principes, obligations et droits importants. Cependant, ces technologies limitent les droits et libertés fondamentaux et doivent être explicitement réglementées par la loi pour être utilisées dans le cadre des procédures pénales. Ainsi, avant d'évaluer s'il existe ou non une norme prévisible pour ces technologies, la deuxième partie de la thèse analyse leur statut juridique. Dans ce contexte, des mesures préventives similaires au profilage telles que la recherche et l'identification physique sont évaluées. Ensuite, les objectifs et les caractéristiques des mesures préventives sont expliqués. Enfin, les différences entre les technologies de profilage et les mesures préventives

sont signalées. De plus, la thèse se demande si les technologies de profilage peuvent être considérées comme des mesures de sécurité. En fait, les mesures de sécurité, comme les technologies de profilage, se concentrent sur le danger de l'auteur et visent à protéger la société contre de futurs crimes. À cette fin, les mesures de sécurité se concentrent sur la réhabilitation de l'auteur et sa réinsertion dans la société. Puisqu'elles restreignent les droits de l'auteur, ces mesures sont limitées par des réglementations prévisibles. La thèse conclut que les technologies de profilage contredisent les finalités et les règles des mesures de sécurité.

Enfin, la nature probante des scores de risque est évaluée. Les juridictions étrangères arrivent à des conclusions incompatibles sur leur évaluation. De plus, ils ne précisent pas quel type de preuve ils constituent. Pour cette raison, tout d'abord, les caractéristiques communes des preuves ont été discutées, puis les types de preuves pertinents tels que les déclarations de témoins sont évalués. Des ressemblances entre les témoins de personnalité et les résultats de profilage sont établies. Ensuite, les scores de risque sont évalués à la lumière de preuves scientifiques et d'opinions d'experts. Enfin, la légalité de ces preuves est remise en question. Les preuves illégales constituent une intersection importante entre la législation sur la protection des données personnelles et les règles de procédure pénale, car les tribunaux doivent évaluer la conformité avec les deux réglementations pour s'assurer que les preuves sont collectées ou évaluées légalement. Par conséquent, l'évaluation de la légalité des scores de risque rassemble tous les principes et règles discutés dans la thèse.

En conclusion, parmi toutes les technologies d'intelligence artificielle, les technologies de profilage sont celles qui transforment le plus radicalement les procédures pénales. Les groupes à risque créés via le profilage et les scores qui leur sont attribués créent un impact à vie sur les individus. Ces scores ne conduisent pas seulement à l'imposition de sanctions contre des individus en Europe et aux États-Unis, mais obligent également les gens à se confronter constamment à ces étiquettes, car elles sont en outre partagées avec des institutions telles que les banques, les compagnies d'assurance, les employeurs et les administrations de l'immigration. Elle conduit à un isolement permanent des groupes dits à risque de la société. Ainsi, à la fin de la thèse, une nouvelle norme a été proposée concernant l'utilisation du profilage,

pour renforcer les droits et libertés des individus et pour rétablir les principes des droits de l'homme dans les procédures pénales.

ABSTRACT

Artificial intelligence technologies enabled the collection and analysis of unlimited amounts of data. Profiling technologies are frequently used for data analysis. These technologies infer general character traits of individuals from several databases which give away their class, economical and social status. Then they determine whether these features pose a risk to society. Their use in criminal procedures transforms the prosecution into a tool to combat the allegedly risky people and inevitably menaces many rights and freedoms. Nevertheless, this thesis addresses primarily the threats towards personal data protection.

The thesis evaluates the risk analysis technologies, which have become increasingly complicated, due to the advancement in machine learning. The main concern of the thesis is to answer whether it is possible to benefit from personal data protection norms in criminal procedures when profiling technologies are enforced in criminal procedures.

The use of profiling during criminal proceedings requires examining the personal data regulations, yet it is also necessary to evaluate the basic principles and measures of criminal procedures. Thus, the thesis seeks to further question the compliance of profiling tools with the principles and rules of criminal procedures. It evaluates the legal nature of profiling technologies and examines the evidential value of the results obtained by profiling.

The research mainly consists of desk research scrutinizing data protection and criminal procedure regulations within a comparative perspective. Thus, relevant books, articles, and publications, as well as the decisions of the Supreme Court, Constitutional Court, and European Court of Human Rights are evaluated. Furthermore, different foreign jurisprudence on the evidential value of profiling technologies is elaborated in detail. Finally, the European Union acquis and non-governmental organizations' reports are examined to show the current applications of AI technologies and the best practices.

Risk analysis tools require knowledge of both technology and law. It is not possible to regulate these technologies without understanding the basic models and concepts of profiling. Therefore, within the thesis, first, the terms such as artificial intelligence, algorithm, machine learning, rule-based learning are introduced. Then the learning models which comply with the principles of the criminal procedures and data protection law have been underlined. Afterward, profiling technologies in criminal justice are introduced. These technologies aim either to detect potential perpetrators or the potential crime scenes. In order to explain their functioning, the underlying criminological theories such as "the theory of broken windows" and "the near-repeat theory" are discussed. Furthermore, the types of data which lead to the profiling outputs are exposed. This chapter is crucial to show that the tools which are already in use in Europe and the US have resulted in identifying people with a certain class, lifestyle, and worldview as risk groups or in marking minority neighborhoods as risky areas.

Profiling technologies assign risk scores to individuals based on their identity and personality, yet they are not based on the criminal act in question. It is very crucial to set limits on them, as the risk scores label people and impact them almost perpetually based on their character. In this context, data protection regulations, which have set limits to profiling for the first time, require a thorough analysis. Within the European Union, the European Data Protection Regulation ("GDPR") and the Law Enforcement Directive 2016/680 constitute the main regulations on profiling. As per Turkey, the Personal Data Protection Law ("KVKK") contains important regulations regarding the profiling process and data processing in general. Considering these regulations, in order to benefit from data protection safeguards, first of all, the relevant technologies must process personal data. However, the definition of personal data must be reconsidered, as the new technologies challenge the dichotomy between anonymous data and identifiable data, while they render almost everyone identifiable via combining and analyzing different datasets. Moreover, they eventually cause legal effects on certain people. Therefore, in the light of the case law, recommendations, and reports of the Article 29 Working Group within the EU, personal data should be considered more broadly. On the other hand, it should be noted that even within context of the criminal procedures, the General Data Protection Regulation might

apply. In most cases, the data collection and analysis processes are initiated by private companies. Therefore, within the EU, for profiling within the criminal justice context, the GDPR provisions may directly be applicable. In cases where law enforcement or judicial authorities process data for detecting and prosecuting crimes, the more specific regulation, the Directive 2016/680, will apply. As both regulations are relevant with regard to profiling, they are both analyzed thoroughly. The thesis demonstrates that the use of profiling technologies such as COMPAS, SyRI, PSA, Static 99 in many countries is not following the principles of purpose limitation, data minimization, and proportionality. Furthermore, the thesis discusses the right not to be subject to automated decisions based solely on automated processing. As per Turkey, the regulations regarding profiling within the scope of KVKK are evaluated in comparison with the EU acquis. KVKK foresees many limitations and exceptions for data processing via judicial authorities, law enforcement, and prosecutors. The thesis aims to point of legal loopholes within KVKK and emphazises the lack of a separate regulation such as Directive 2016/680.

Personal data protection laws foresee many important principles, obligations, and rights. However, these technologies limit fundamental rights and freedoms and must be explicitly regulated by law to be used within criminal procedures. Therefore before evaluating whether a foreseeable norm exists for these technologies or not, the second part of the thesis analyzes their legal status. In this context, preventive measures similar to profiling such as search and physical identification are evaluated. Then, the purposes and basic characteristics of protection measures are explained. Finally, the differences between profiling technologies and preventive measures are pointed out. Furthermore, the thesis questions if profiling technologies can be considered as security measures. As a matter of fact, security measures, like profiling technologies, focus on the danger of the perpetrator and aim to protect society against future crimes. For this purpose, security measures concentrate on rehabilitating the perpetrator and reintegrating them into society. Since they restrict the perpetrator's rights, these measures are limited via foreseeable regulations. The thesis concludes that the profiling technologies contradict the purposes and the rules for security measures.

Finally, the evidential nature of the risk scores is evaluated. Foreign jurisdictions come up with incompatible conclusions on their assessment. Moreover, they do not clarify what type of evidence they constitute. For this reason, firstly, the common features of the evidence were discussed, then relevant types of evidence such as witness statements are evaluated. Similarities between personality witnesses and profiling results are drawn. Then risk scores are assessed in light of scientific evidence and expert opinions. Finally, lawfullness of such evidence is questioned. Illegal evidence constitutes an important intersection between personal data protection legislation and criminal procedure rules since the courts must evaluate the compliance with both regulations to make sure that the evidence is legally collected or assessed. Therefore, assessing the legality of risk scores brings together all the principles and rules discussed within the thesis.

In conclusion, among all artificial intelligence technologies, profiling technologies are the ones that transform criminal procedures most drastically. Risk groups created via profiling and their assigned scores create a lifetime impact on individuals. These scores do not only lead to the imposition of sanctions against individuals in Europe and the US, but also force people to confront these labels constantly, as they are further shared with institutions such as banks, insurance companies, employers, and immigration administrations. It leads to permanent isolation of so-called risky groups from society. Therefore, at the end of the thesis, a new norm has been proposed concerning the use of profiling, to strengthen the rights and freedoms of individuals and to re-establish the human rights principles within criminal procedures.

ÖZET

Günümüzde yapay zekâ teknolojileri ile sınırsız veri toplama ve bu verileri analiz etme mümkün hale gelmiştir. Profilleme teknolojileri veri analizinde en sık kullanılan teknolojilerdir. Profilleme ile farklı veri tabanlarından süzülen sınıfsal, ekonomik ve sosyal veriler ile kişilere ilişkin karakter özellikleri değerlendirilmekte, bu özelliklerin toplum için risk teşkil edip etmediği belirlenmektedir. Bu teknolojilerin ceza muhakemesinde kullanımı, ceza muhakemesini adeta "riskli kişilere" karşı mücadele aracına dönüştürmüştür. Bu durum kuşkusuz ki pek çok hak ve özgürlüğü aşındırma ihtimali barındırır. Tez kapsamında öncelikli olarak profillemeye karşı kişisel verilerin korunması boyutu ele alınmıştır.

Tezin kapsamı, özellikle makine öğrenmesi ile gittikçe karmaşık bir yapıya kavuşan risk analiz teknolojileri ile sınırlanmıştır. Bu tür profilleme yöntemlerine ilişkin çeşitli hak ve düzenlemeler ilk olarak kişisel verileri koruma kanunlarında yapılmıştır. Tezin temel sorunsalı, profilleme teknolojilerinin ceza muhakemesinde kullanılması halinde, muhakeme sürecinde kişisel verileri koruma normlarından yararlanmanın mümkün olup olmadığıdır.

Elbette ceza muhakemesi alanında bu teknolojilerin kullanılması, muhakemenin temel ilkeleri ve mevcut tedbirlerin niteliklerini incelemeyi gerektirir. Bu nedenle profilleme teknolojileri kişisel verileri koruma normlarının yanı sıra ceza muhakemesi ilke ve kuralları çerçevesinde de incelenmiştir. Profilleme teknolojilerinin hukuki niteliği ve bu teknolojiler ile varılan sonuçların delil değeri üzerinde durulmuştur.

Tezde araştırma yöntemi olarak kişisel verileri koruma mevzuatı ve bunun yanı sıra ceza muhakemesi düzenlemeleri, farklı hukuk sistemlerindeki örnekleriyle birlikte ele alınmıştır. Bu hususta temel makale ve kitaplar taranmış, ardından ilgili Yargıtay kararları, Anayasa Mahkemesi kararları ve Avrupa İnsan Hakları Mahkemesi kararları incelenmiştir. Bunun yanı sıra profilleme teknolojileri ve bunların delil değeri ile ilişkilendirilebilecek çeşitli ülkelerdeki içtihatlar da ayrıntılı şekilde incelenmiştir. Son olarak bu teknolojilerin nasıl kullanıldığı ve ne şekilde uygulanması gerektiğini gösteren sivil toplum örgütleri raporları ve AB bünyesindeki tavsiye kararları incelenmiştir.

Risk analizi yapan profilleme uygulamaları, teknoloji ile hukuku birleştiren bir alandır. Temel kavramlar ve profilleme teknolojilerinin çalışma şekli anlaşılmaksızın bunlara ilişkin hukuki düzenleme yapılması mümkün değildir. Bu nedenle ilk bölümde öncelikle yapay zekâ, algoritma ve makinelerin öğrenme süreci üzerinde durulmuş, hangi öğrenme yöntemlerinin ceza muhakemesi ve kişisel verilerin korunması mevzuatı ile uyumlu olacağına ışık tutulmuştur. Ardından ceza adaletinde kullanılan profilleme teknolojileri ayrıca ele alınmıştır. Bunlar suç işlenecek yeri ve suç işleyecek kişileri tespit eden profilleme teknolojileri olarak ikiye ayrılmış, dayandıkları modellere ilham veren "kırık camlar teorisi" ve "suç mahalline dönüş teorisi" gibi kriminolojik teoriler açıklanmıştır. Ayrıca bu teknolojilerin hangi verilere dayanarak risk analizi yaptıkları irdelenmiştir. Tartışılan bu hususlar, ceza muhakemesinde Avrupa ve Amerika'da kullanılmakta olan profilleme teknolojilerinin, dolaylı olarak belirli bir sınıfa, yaşam tarzına, hayat görüşüne sahip kişileri ve bu kişilerin yoğunlukla yaşadığı mahalleleri risk grubu olarak tespit ettiğine işaret etmektedir.

Profilleme teknolojileri, kişinin suç teşkil eden davranışlarından değil bizzat kişiliğinden yola çıkmaktadır. Bu durum, kişiler üzerinde daimi etkiler doğurabilmektedir. İlgili teknolojilerin sınırlandırılması bu nedenle büyük önem taşımaktadır. Sınırlandırma rejimi açısından öncelikle, profilleme teknolojilerinin işleyiş şekline ilişkin kurallar getiren kişisel verileri koruma düzenlemeleri dikkate alınmıştır. Bu bağlamda, Avrupa Birliği bünyesinde Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR") ve 2016/680 sayılı Kolluk Direktifi öncül düzenlemeleri oluşturmaktadır. Türkiye'de ise Kişisel Verileri Koruma Kanunu ("KVKK") kapsamında profilleme sürecine ve genel olarak tüm veri işleme süreçlerine ilişkin önemli düzenlemeler bulunmaktadır. Bu düzenlemelerin kapsam alanına girebilmek için kuşkusuz ki öncelikle kişisel veri işlenmesi söz konusu olmalıdır. Tez kapsamında, günümüzde anonim veri ve belirli bir kişiye işaret eden veri şeklinde ayrımın geçersiz hale geldiği vurgulanmıştır. Profilleme sürecinin en başında, henüz belirli bir kişiye işaret etmeyen pek çok veri, farklı veri tabanlarındaki verilerin birleştirilmesi ve analiz edilmesi ile kişileri belirlenebilir kılmakta veya üzerlerinde hukuki sonuçlar doğurmaktadır. Bu nedenle, AB bünyesindeki içtihatlar, tavsiye kararları ve 29. Çalışma grubu raporları da dikkate alınarak kişisel veri kavramı, günümüzdeki teknolojiler kapsamında daha geniş şekilde değerlendirilmiştir.

Ardından ceza muhakemesi sürecinde dahi profillemenin çoğunlukla özel şirketler tarafından gerçekleştirildiği vurgulanmıştır. Bu nedenle AB kapsamında GDPR hükümleri önem taşımaktadır. Ancak kolluğun veya adli mercilerin, ceza muhakemesi sırasında adli amaçla veri işlediği durumlarda, özel bir düzenleme olan 2016/680 sayılı Direktif uygulanacaktır. İlgili mevzuatların profilleme ile ilişkilendirilebilecek düzenlemeleri detaylı şekilde ele alınmış, pek çok ülkede ceza muhakemesi alanında sevk edilen COMPAS, SyRI, PSA, Static 99 gibi uygulamaların, bu mevzuatlarda yer alan amaç sınırı, asgari düzeyde veri işleme ve orantılılık gibi ilkelere aykırılıkları tespit edilmiştir. Ayrıca kişilerin münhasıran otomatik şekilde alınan kararlara tabi tutulmama hakkı masaya yatırılmıştır. Türkiye özelinde ise KVKK kapsamında profillemeye ilişkin düzenlemeler AB bünyesindeki düzenlemelerle karşılaştırmalı şekilde ele alınmıştır. KVKK ile öngörülen yargı mercileri, kolluk ve savcılar tarafından veri işlenmesi halinde uygulanacak sınırlamalar ve istisnalar açıklanmış, Kanun'da bırakılan boşlukların AB mevzuatında olduğu gibi ayrı bir düzenleme ile doldurulmadığı vurgulanmıştır.

Kişisel verileri koruma kanunları kuşkusuz ki önemli ilkeleri, yükümlülük ve hakları düzenlemektedir. Ancak profilleme teknolojilerinin ceza muhakemesinde kullanımı için, temel hak ve özgürlükleri sınırlayan bu teknolojiler mutlaka kanunla düzenlenmelidir. Bu hususta öngörülebilir bir kanuni düzenleme bulunup bulunmadığı değerlendirilmeden önce, profillemenin ceza muhakemesindeki yeri tespit edilmeye çalışılmıştır. İkinci bölümde ilkin bu teknolojilerin koruma tedbiri olarak kabul edilip edilemeyeceği değerlendirilmiştir. Bu bağlamda profilleme ile benzerlik gösteren adli arama, önleme araması, fizik kimlik tespiti gibi tedbirler üzerinde durulmuştur. Ardından koruma tedbirlerinin amaçları ve temel nitelikleri açıklanmış, profilleme teknolojilerinin koruma tedbirlerinden nasıl farklılaştığı vurgulanmıştır. Bu bölümde ayrıca profilleme teknolojileri ile güvenlik tedbirleri arasındaki benzerlik ve farklılıklar değerlendirilmiştir. Nitekim güvenlik tedbirleri de profilleme teknolojileri gibi failin tehlikeliliğine yoğunlaşır, gelecekte işlenebilecek suçlara karşı toplumu koruma amacı güder. Bu amaçla faili topluma yeniden kazandırmaya yoğunlaşır. Bu sırada failin hakları kısıtlandığından, güvenlik tedbirlerine ilişkin sınırlar, kanun ile öngörülmüştür. Profilleme teknolojileri ise amaçları ve uygulanma usulleri yönünden güvenlik tedbirlerinden uzaklaşmaktadır.

Son olarak profilleme ile ulaşılan sonuçların delil niteliği üzerinde durulmuştur. Pek çok yabancı içtihat profilleme teknolojilerinin hükme esas alınıp alınamayacağı konusunda farklı sonuçlara ulaşmaktadır. Ayrıca henüz profilleme teknolojilerinin belirlediği risk puanlarının hangi delil türü kapsamında ele alınması gerektiği açıklık kazanmamıştır. Bu nedenle tez kapsamında delillerin müşterek özellikleri ele alınmış, ardından delil türlerinden profilleme ile ilişkilendirilebilecek olanlar irdelenmiştir. Bu bağlamda profilleme teknolojileri tanık beyanları ile karşılaştırılmış, profillemenin daha ziyade kişilik tanıklığı ile benzeştiği gözlemlenmiştir. Ardından profilleme teknolojileri ile varılan sonuçların bilimsel delil veya bilirkişi görüşü olarak ele alınıp alınamayacağı tartışmaya açılmıştır. Bu tür teknolojiler ile varılan sonuçlar açısından en önemli husus bunların hukuka uygunluğunun incelenmesidir. Nitekim bu inceleme, verilerin toplanmasından analiz edilmesine kadar tüm aşamaları kapsamakta, kişisel verileri koruma mevzuatı ile ceza muhakemesi kuralları arasında bir kesişim noktası oluşturmaktadır. Başka bir deyişle, hukuka uygun delil incelemesi, ceza hâkimlerinin delillerin kişisel verilerin korunması mevzuatına uygun elde edilip edilmediğini değerlendirmesini gerektirmekte, tez kapsamında ele alınan tüm ilke ve kuralları bir araya getirmektedir.

Sonuç olarak yapay zekâ teknolojileri arasında ceza muhakemesi üzerinde en fazla dönüştürücü etkiye sahip profilleme teknolojileri farklı boyutlarıyla ele alınmıştır. Profilleme ile oluşturulan gruplamalar ve verilen risk puanları, Avrupa ve Amerika'da kişilere ceza hukuku yaptırımlarının uygulanmasına yol açmakta, ayrıca bankalar, sigorta şirketleri, işverenler, göç idareleri gibi pek çok kurumla paylaşılarak ömür boyu damgalayıcı bir etki doğurmaktadır. Kişilerin toplumdan tecritine yol açan bu uygulamalara ilişkin tüm önemli hususlar sonuç bölümünde yeniden vurgulanmıştır. Bu bölümde son olarak, fiilden yola çıkan ve insan haklarına saygılı şekilde maddi gerçeği arayan hümanist bir ceza muhakemesini yeniden tesis etmek adına profilleme teknolojilerinin kullanımına ilişkin yeni bir norm önerilmiştir.

GİRİŞ

Yeni teknolojiler, şüpheli olan ve olmayan kişiler arasında ayrım yapmaksızın sınırsızca veriye erişimi ve bu verilerin ilişkilendirilerek analiz edilmesini mümkün hale getirmiştir. Öngörülebilirlik adına, tüm bireylerin yaşamının panaromik fotoğrafı çekilmekte, düşünce, eğilim ve alışkanlıkları takip edilmektedir.

Ekonomik, politik ve sosyal kırılmaların gittikçe keskinleştiği çağımızda, devletler bu müdahaleleri olası riskleri henüz doğmadan ortadan kaldırmak amacıyla gerçekleştirmektedir. Bu durum ilkin kamu düzenini ihlal eden hareketlerden, kamu düzenini "tehlikeye" sokan hareketlere yoğunlaşılması ile kendini göstermiş, bugün gelinen noktada ise artık hareketlerden yola çıkan "tehlikelilik" algısı, yerini daha da soyut olan risk kavramına bırakmıştır. Risk retoriği kişilerin karakterlerinden yola çıkarak sürülen izlerle, belirli kişilik özelliklerine sahip olan kişi ve grupların, belirsiz bir gelecekte toplum düzenine karşı doğuracakları risklerin olasılıksal olarak hesaplanabileceğini iddia eder. Bu kişilerin hareketleri ile tehlike veya zarar doğurmasını beklemeden, bugünden müdahale edilebileceğini savunur[1]. Bu anlayış, kuşkusuz ki Ceza Muhakemesi Hukukunun dayandığı geleneksel zemini alt üst edecek niteliktedir. Nitekim ceza muhakemesi evleviyetle suç teşkil eden hareketlerin gerçekleştirilmesi üzerine devreye girer, belirli sayıda şüphelinin, belirli zaman kesitindeki hareketlerini hedef alır. Oysa artık geçmişteki suçun aydınlatılması ve suç oluşturan fiilleri sebebiyle faillerin cezalandırılması yetersiz bulunmaktadır. Bunun yerine herkesin suç işleme potansiyeli bulunduğuna inançla, her anın gözetlenmesi ve kaydedilmesi ve risklerin bugünden önlenmesi amaçlanır. MOBESE kamera görüntüleri, biyometrik veri tabanları, plaka numaraları, gecikmiş ödemeler, ani hesap hareketleri, takip edilen internet siteleri, katılınan etkinlikler ve iletişim kurulan kişiler toplanan bilgilerin yalnızca bir kısmını oluşturmaktadır. İnternet alt yapısı ile birlikte, online dünyada bıraktığımız izler de takip edilebilir hale gelmiş, evlerden ve iş yerlerinden tüm dünyaya açılan bu kapı ile mahremiyet kavramı yeni bir boyut kazanmıştır. Böylelikle verileri işlenen, analiz edilen kişilerden "uyumsuz" özellikler

[1] Maria Laura Böhm, "Endanger Law: War on Risks in German Criminal Law", **İçinde The Law in the Information and Risk Society**, Ed: Gunnar Duttge/Sang Won Lee, Universitätsverlag Göttingen, 2011, s.145-164, s.151.

gösterenlerin hedef alınması oldukça kolaylaşmıştır. Bu kişiler gelecekte işleyecekleri iddia edilen suçlar için bugünden "kusursuz bir sorumlulukla" cezalandırılmaktadır[2].

Bu durum, ceza muhakemesinde yer alan tedbirlerin dayandığı şüphe olgusunu köklü bir şekilde dönüştürmektedir. Klasik anlamda şüphenin oluşmasına temel teşkil eden, kişinin suç teşkil eden fiiline ilişkin somut olgular, tanık beyanları ve sınırlı sayıda delildir. Bu usül, yerini sınırsız dijital veriden yola çıkan, otomatikleşmiş, gayrişahsi bir şüpheye bırakmıştır[3]. Artık kişinin suç teşkil eden hareketi ile korunan hukuksal bir değeri ihlal etmesi gerekmemektedir. Yine kişinin üzerinde yoğunlaşmış, kişiselleştirilmiş bir şüphe üzerine soruşturulması söz konusu değildir. Aksine şüpheli sıfatı kazanmamış her vatandaş, "dijital profiller"i çıkartılarak izlenmektedir. Bu koşullar için sıklıkla Orwell'in "Büyük Ağabey'in gözetimi" ifadesi kullanılmakla birlikte bugünü nitelendirmek için Kafka'nın Dava benzetmesi daha isabetli olacaktır. Nitekim Dava kitabı, kişilerin ne ile suçlandıklarını bilmeksizin, kendilerini sürekli bir soruşturma sürecinde buldukları bir sistemin ağırlığını resmektedir.

Elbette kişilerin tüm verilerinin ve yaşam biçimlerinin izinin sürüldüğü bir düzen, ifade özgürlüğü, toplanma özgürlüğü gibi pek çok hak açısından caydırıcı etki doğuracak ve kişilerin geleceğini serbestçe tayin ettiği, insan onuruna uygun yaşama hakkını sarsar hale gelecektir. Ceza muhakemesi özelinde bu etki "suçluluk karinesi" şeklinde ifade edilebilecek bir noktaya erişmiş, adil yargılanma ilkeleri pek çok yönüyle müdahaleye uğramıştır.

Yeni risk analiz teknolojilerinin ceza muhakemesi sürecine dâhil edilmesi, sınırları gittikçe kaybolan hak ve güvencelerin sağlamlaştırılmasını zorunlu hale getirmiştir. Nitekim bu tezin amacı, muhakeme sürecinde mevcut düzenlemeleri ve kişisel verilerin korunması mevzuatını, karşılaştırmalı hukuktan da yararlanarak ele almak ve söz konusu düzenlemelerin yeni teknolojiler karşısında gerçek bir koruma kalkanı oluşturup oluşturmadığını tartışmaya açmaktır.

---

[2] **Ibid.**

[3] Elisabeth E Joh, "The New Surveillance Discretion: Automated Suspicion, Big Data and Policing", **Harvard Law & Policy Review**, Cilt: 10, Sayı:1, 15-42, s.15,17.

Tez kapsamında öncelikle yeni teknolojiler arasından yapay zekâ teknolojileri irdelenecektir. Popüler kültürde ve bilim kurgu kitaplarında yer alan, kendi kendine düşünebilen, insan zekâsını birebir taklit edebilen, hatta onu alt eden yapay zekâ seviyesine henüz ulaşılamamıştır. Bu nedenle tez kapsamı, ilk bölümde ayrıntılarıyla tanımlanacak olan öğrenme aşamasındaki dar yapay zekâ teknolojilerinin kullanılması ile sınırlandırılmıştır. Elbette bu tür yapay zekâ teknolojilerinin tamamının bir tezin kapsamında incelenmesi mümkün değildir. Bu nedenle, risk kavramını ceza muhakemesi sürecine dâhil eden ve temel hak ve özgürlüklere yönelik çok daha yoğun bir müdahale içeren profilleme teknolojileri incelenecektir. Profilleme teknolojileri, farklı veri tabanlarından süzdükleri sınıf, mahalle, kültürel ve sosyal çevre, karakter özellikleri ve tercihlere ilişkin verileri gruplandırarak, bu gruplar üzerinden risk faktörlerini belirlemektedir. Ceza muhakemesinin bu riskleri ortadan kaldırmak üzere kullanılan bir mücadele aracına dönüşmemesi için bu teknolojilerin dikkatle ele alınması gerekmektedir. Bununla birlikte profilleme teknolojileri, yalnızca ceza muhakemesi sürecinde değil, suç öncesi alanda ve ayrıca suçun tespitinin ardından infaz aşamasında kullanılabilmektedir. Tezin konusu, risk analizi yapan profilleme teknolojilerinin yalnızca ceza muhakemesi sürecinde kullanılmasıyla sınırlanmıştır. Dolayısıyla, ceza muhakemesi sürecinde şüphe tespiti, failin duruşmalara katılmama ihtimali veya failin yeniden suç işleme riski gibi farklı amaçlarla risk analizi yapan profilleme teknolojileri ele alınacaktır.

Kuşkusuz profilleme teknolojilerinin kulllanımı pek çok farklı hakka müdahale içermektedir. Adil yargılanma hakkının görünümü olan masumiyet karinesi, susma hakkı, savunma hakkı gibi ceza muhakemesinin temel hak ve prensiplerinin yanı sıra ifade özgürlüğü, kişisel güvenlik ve seyahat etme özgürlüğü gibi özgürlükler bugün söz konusu teknolojilerin müdahalesi altındadır. Çalışmanın kapsamı yapay zekâ teknolojileri eliyle ceza muhakemesinde veri işlenmesi, dolayısıyla kişisel verilerin korunması boyutuyla ele alınacaktır. Dolayısıyla tez kapsamında ceza muhakemesi ile kişisel verilerin korunması hukukunun kesişim noktası üzerinde durulacaktır.

Profilleme teknolojilerinin ceza muhakemesi alanında sevk edilmesi, kişisel veriler mevzuatı ile ceza muhakemesi ilkelerini birlikte değerlendirmeyi gerektirmektedir. Bu bağlamda tezin cevap vermeye çalıştığı temel soru şu şekildedir:

Profilleme teknolojileri ceza muhakemesinde kullanıldığı takdirde, kişisel verileri koruma normlarından, ceza muhakemesi sürecinde yararlanmak mümkün müdür?

Bu soruya yanıt verebilmek adına hem Avrupa Birliği hem Türkiye'de yer alan kişisel verileri koruma mevzuatları değerlendirilecek, bu mevzuatların uygulama alanı, sınırları ve profilleme sürecine dair öngördükleri ilke ve kurallar incelenecektir. Bu düzenlemelerin ceza muhakemesinde veri işlenmesine uygulanıp uygulanamayacağı tespit edilecektir. Bu soru profilleme teknolojileri ile varılan sonuçların delil değeri incelenirken tekrar ele alınacaktır. Nitekim bir delilin hukuka uygunluğunun tespiti, tüm hukuk düzenine uygun şekilde delil toplanması ve değerlendirilmesini gerektirdiğinden, hukuka aykırı delil kavramı kişisel verileri koruma ve ceza muhakemesi mevzuatları arasında bir köprü kurmaktadır.

Günümüzde, kişisel verileri koruma mevzuatlarının, ceza muhakemesi hükümlerine ek güvenceler sağlamasına rağmen, profilleme teknolojilerine karşı yeterli bir koruma sağlanıp sağlanmadığı mutlaka ele alınmalıdır. Aksi halde, mevcut teknolojiler ve bunların yol açtığı bilgi asimetrisi sonucu yerinden oynayan birey-devlet terazisinde, bireyler güçsüz bir konuma terk edilmiş olacaktır. Bu nedenle tez kapsamında ikincil bir soru ele alınacaktır:

Ceza muhakemesi ve kişisel veriler mevzuatlarındaki mevcut düzenlemeler, profilleme teknolojilerine karşı yeterli koruma sağlamakta mıdır?

Tezde bu soruya yanıt ararken kişisel verilerin korunması mevzuatının yanı sıra, ceza muhakemesi ilkeleri ve kuralları incelenecek, profilleme teknolojilerinin amacı, niteliği ve işleyişlerinin, ceza muhakemesi bünyesindeki tedbirler ile uyum gösterip göstermediği değerlendirilecektir. Böylelikle, mevcut düzenlemelerin profilleme teknolojilerine yanıt vermesinin mümkün olup olmadığı ele alınacaktır. Çalışma kapsamında ele alınan ikincil soruya verilecek menfi cevap, profilleme teknolojilerini yeterince sınırlayan hükümler yoksa alınması gereken önlemleri araştırmayı içerir. Nitekim tezin son bölümünde, bu teknolojilerle elde edilen sonuçların delil değeri bu anlayışla incelenecek ve sonuç bölümünde profilleme teknolojilerini sınırlayan bir norm önerilecektir.

Tez kapsamında ele alınan bu soru ve sorunlara cevap ararken, ilk bölümde öncelikle yapay zekâ ve makine öğrenmesi kavramları, bu kavramlara ilişkin tartışmalar ve güncel gelişmeler değerlendirilecektir.

Ardından kişisel verilerin ne olduğu açıklanacak, kişisel veri - anonim veri ayrımının, teknolojilerinin bugün vardığı aşamada geçerli bir ikilem olup olmadığı tartışmaya açılacaktır. Avrupa'da büyük tartışma yaratan Avrupa Birliği Genel Veri Koruma Tüzüğü ve Türkiye'de Kişisel Verilerin Korunması Kanunu ile gündem olan bu yeni alanın sınırları ve temel prensipleri ele alınacak, söz konusu kavram ve ilkelerin profilleme teknolojileri karşısında kişilerin haklarını korumada yeterli olup olmadığı tartışmaya açılacaktır.

Tezin ikinci bölümünde profilleme teknolojilerinin yargılama sürecinde kullanılması üzerinde durulacaktır. Bu bölümde öncelikle karşılaştırmalı hukukta yer alan düzenlemeler ve yargı kararları dikkate alınacaktır. Ardından profillemenin geleneksel koruma tedbirlerindeki ortak ilkeler olan kanunilik, geçici olma, hâkim denetimine tabii olma niteliklerini karşılayıp karşılamadığı değerlendirilecek, suç şüphesi ve özel olarak makul şüphe kavramını dönüştürücü etkileri tartışılacaktır. Kalıcı olan etkileri, kişileri toplumdan ayrıştırmaları ve failin tehlikeliliğine yoğunlaşmaları nedeniyle güvenlik tedbirleri ile de benzerlikler barındıran profilleme teknolojileri, güvenlik tedbirleri kapsamında da değerlendirilecektir. Son olarak bu teknolojilere dayanılarak varılan sonuçların delillerin taşıması gereken niteliklere sahip olup olmadıkları ve hukuka uygunlukları tartışılacaktır.

BİRİNCİ BÖLÜM:

YAPAY ZEKÂ, PROFİLLEME TEKNOLOJİLERİ VE KİŞİSEL VERİLERİN KORUNMASI

I. YAPAY ZEKÂ TEKNOLOJİLERİNDE ÖNEMLİ KAVRAMLAR

Teknolojik gelişmelerin ivme kazanmasıyla yapay zekâya ilişkin eski tanımlar bugün gelinen aşamayı açıklamakta yetersiz kalmaktadır. Bu nedenle aşağıda yapay zekâ alanındaki kavramlar değişim ve dönüşüm içerisinde, özellikle bugüne ışık tutan ve ceza muhakemesi üzerinde etki doğuran boyutuyla ele alınacaktır. Bu amaçla öncelikle yapay zekânın ne olduğuna dair genel bir tartışmanın ardından, ceza muhakemesi alanında hangi tür akıllı risk analiz teknolojilerinin kullanıldığı üzerinde durulacaktır.

Her ne kadar yeni teknolojilere ilişkin tartışmalarda, bunların özerkleşerek doğurabileceği sıkıntılar üzerinde durulsa da bugün gelinen aşamada, bu teknolojilerin hangi amaçlarla kullanılacağını tayin etmek hâlâ insanın elindedir. Dolayısıyla bu bölümde, mevcut teknolojilerin resmi çizilirken, bir yandan şu sorulara cevap aranmaktadır: "Tüm bu gelişmeler, hangi amaçla kullanılmakta ve kimin lehine sonuç doğurmaktadır? Bunların ceza muhakemesinde kullanılması vatandaşlık hakları ve sanık/şüphelinin hakları açısından ne ifade etmektedir? Süreçte şirketler ve hükümetlere karşı vatandaşlar için hukuk eliyle daha fazla korunma sağlanması gerekmekte midir?"

Bu sorulara verilecek yanıt, tez kapsamında ele alınacak teknolojilerin kullanılmasına ilişkin düşünsel alt yapıyı oluşturacaktır.

A. Zekâ ve Yapay Zekâ Kavramı

Yapay zekâyı, kodlar veya algoritmalar aracılığıyla insan zekâsını yapay olarak yeniden yaratma çabası olarak tanımlamak mümkündür. Nitekim yapay zekâ ile insan kapasitesine sahip, insanlar gibi düşünen ve davranan yapay bir makinenin yaratılışına

gayret edilmektedir. İnsan zekâsını taklit edebilme iddiası, öncelikle insan zekâsının ne olduğunu tarif etmeyi gerektirir. Ayrıca bu amacın gerçekçi olması için, insan zekâsının indirgenebilir ve yapay olarak programlanabilir olup olmadığı gündeme getirilmelidir.

İnsana has zekânın nasıl işlediği biyoloji, psikoloji, nöroloji, felsefe gibi pek çok farklı alanda ele alınsa da hâlâ gizemini korumaktadır. Ancak günümüzde makinelere kazandırılmak istenen zekânın fonksiyonlarını öğrenme, algılama, dili işlevsel şekilde kullanabilme, mantık yürütme, karar alma ve sorun çözme gibi belirli bilişsel yetilerle tanımlamak mümkündür[4]. Kuşkusuz ki zekâ, tek boyutlu bir şekilde tanımlanması mümkün olmayan, pek çok farklı bilgi ve işlem kapasitesini barındırır. Oysa yapay zekâ için bu denli sınırsız bir işlem kapasitesinin oluşturulması henüz mümkün olmamıştır. Bu nedenle, makinelere, öngörülen görevleri yerine getirebilmelerini mümkün kılacak daha sınırlı yetiler kazandırılmaya çalışılmaktadır. Bu tür fonksiyonel bir yaklaşımla, yapay zekânın insan zekâsını taklit edebilmesinden ziyade, tarif edilen görevi yerine getirmeye elverişli kapasiteye ulaşması yeterli olacaktır[5].

Geçmişten bugüne insan, kendisine benzer ve hatta kendisini de aşan bir varlık yaratma arayışını sürdürmüş, zeki ve otonom varlıklar üretmeyi istikrarlı bir şekilde kurgulamıştır. Bu kurgunun ürünü olarak yapay zekâ, doğada kendiliğinden var olmadığından, her halükarda yapay veya taklit olarak adlandırılmaya mahkûmdur. Ancak henüz insan zekâsının tüm boyutlarıyla tanımlanamadığı düşünüldüğünde, bu zekânın yapay olarak birebir üretimi oldukça güçtür[6]. Bununla birlikte zekânın tüm boyutlarını açıklamak mümkün olmasa da pek çok boyutu soyut bir modelleme ile açıklanmaya çalışılmaktadır. Bu bağlamda yapay sinir ağları ve genetik algoritmaları geliştirilerek, dış dünyayı algılayan, çevresine uyum sağlayan ve fiziksel dünya ile etkileşime geçen bir yapay zekâ modeli oluşturulmaya çalışılmaktadır. Yine bu amaçla, Aristoteles'in izinden gidilerek tümevarım, tümden gelim gibi pek çok mantıksal çıkarım yöntemi makinelere aktarılmıştır[7].

---

[4] Mark Coeckelbergh, **AI Ethics**, The MIT Press: Cambridge, Nisan 2020, s. 64, 65.
[5] Margaret A. Boden, **AI: Its Nature and Future**, Oxford University Press: Oxford, Temmuz 2016, s.121.
[6] Stuart J Russel/Peter Norvig, **Artificial Intelligence: A Modern Approach**, Pearson: Edinburgh, Mayıs 2016, p. 1, 7.
[7]George F, Lugar, **Artificial Intelligence: Structures and Strategies for Complex Problem Solving**, Addison Wesley Yayınları: Edinburgh, Ocak 2005, s.VIII-IX.

Zekâ, bireysel bir yeti olarak algılansa da kolektif boyutu göz ardı edilmemelidir. Sosyal sistem içinde var olan insan, bu sistemde öğrendiği derslerle hayatta kalmak ve kendini gerçekleştirmek için yeni çözüm yollarını benimsemiştir. Bu nedenle, akıllı addettiğimiz davranışlar, sınırlı sayıda bilgi ve tecrübeye sahip bireylerin, toplumsal olarak geliştirdikleri ortak bir üretimin ürünüdür. Topluluk içinde yaşayan canlıları, bir nevi topluluğun nöronları olarak kabul etmek ve zekâyı kolektif etkileşimin ürünü olarak ele almak gerekir. Dolayısıyla, zekâyı salt bir bireyin sinir ağlarına borçlu olduğumuzu söylemek güçtür. Bu nedenle bir makinenin zeki olup olmadığını değerlendirirken, kendi kendine karar alabilme yetisi kadar, bu kararı alırken diğer birimlerle veya bireylerle ne şekilde iletişim kurduğu da değerlendirilmelidir. Nitekim zekâ otonom olma yetisinin yanı sıra, iletişimsel ve diğerleriyle "yarı otonom" bir bağ kurabilme yetisini de içerir. Doğa ve diğer bileşenler gözetilmeden alınan kararlar "akıllı kararlar" olarak nitelendirilemeyecektir. Bu nedenle gözleme dayalı dinamik veri toplama, zekânın gelişimi açısından büyük önem taşır. Zekâ, bireysel ve sınırlı gözlem yeteneğinin dışına çıkarak, farklı bilgi ve gözleme sahip kişilerle koordine olmayı ve eldeki kaynakları birleştirebilmeyi mümkün kılar. Bu bağlamda zekâ, sürekli öğrenme ve yeni koşullara uyum sağlayabilmeyi, bu uğurda toplulukla ilişki kurabilmeyi içerir[8]. Nitekim yapay zekânın işleyişi için makineler çeşitli sensörlerle donatılarak "gözlem" yapabilir hale getirilmekte, yine nesnelerin interneti aracılığıyla örneğin akıllı evlerdeki araçlar, ev içindeki ve hatta internete bağlanabilen ev dışındaki diğer araçlarla iletişim kurabilecek şekilde evrimleştirilmektedir. Bununla birlikte, günümüzde hâlâ yapay zekâyı besleyen öncelikli kaynak, gözlemleri ve etkileşimleri değil, insan eliyle üretilmiş dijital verilerdir.

Yapay zekâ modellerinin gerçekten insan zekâsının farklı boyutlarını barındırıp barındırmadığını, başka bir deyişle insandan ayırt edilemeyecek noktaya ulaşıp ulaşmadığını ölçen en önemli testlerden biri Turing testidir. Bu test, yapay zekânın insanı iyi taklit edip edemediği üzerine inşa edilmiştir. Testin yaratıcısı olan Turing, makinelere insan zekâsını taklit edebilme yetisi kazandırabilmek için öncelikle insanların her türlü eylemi nasıl ve neden yaptığını tespit etmenin zorunlu olduğunu ve dahası bunları "matematiksel komutlar" haline getirilmesi gerektiğini belirtmiştir. Söz konusu matematiksel komutlar, "programlama" şeklinde ifade edilebilecek ve

[8] Lugar, s.17-19.

makinelere bu yolla aktarılabilecektir. Turing'in etkisiyle yapay zekânın ün kazandığı yıllarda cevabı aranan soru "yapay makineler düşünebilir mi" den ziyade, "bir gün insanı kusursuz taklit edebilen programlar yazılabilir mi" sorusu olmuş ve alandaki gelişmeler yıllarca bu soru etrafında şekillenmiştir[9].

Yapay sistemler günümüzde sınırlı nitelikte görevleri yerine getirebilecek şekilde programlanabilmektedir. Bununla birlikte yapay zekânın insan zekâsına oranla daha kısa bir süreçte evrilmesi beklenmektedir. Nitekim "en güçlü olanın hayatta kaldığı" binlerce yılda bugünkü halini almış insan zekâsına nazaran, yapay zekânın, çok daha kısa sürede geliştirilmesi mümkündür[10]. İnsan zekâsından farklı olarak yapay zekâ, yıllar içerisinde elenen tesadüfi gen mutasyonları veya hayatta kalmayı güçleştiren zayıflıkları barındırmamakta, aksine geçmişten bugüne insan emeğiyle üretilen tüm bilgi ve verilerin üzerine hızla inşa edilmektedir. Bu nedenle AlphaGo yapay zekâ uygulaması, Asya'nın en köklü zekâ oyunlarından Go oyunu şampiyonunu yenebilmiş, otonom araçlar sürücü koltuğunu insanların elinden almaya başlamış, hastalıkların teşhisinde akıllı yardımcılar kullanılmaya başlanmış ve daha pek çok yapay zekâ uygulaması hayatımızda hızla yerini almıştır. Dolayısıyla yapay zekâ, a priori şekilde öğrenmekten ziyade, kendisine nakledilen büyük veri mirası üzerinden hızla gelişmektedir[11]. Hesaplama, hafıza, öğrenme, planlama, yaratma gibi pek çok alanda makineler insanın düşünme kapasitesini aşabilmekte, bu alanlarda öğrendiklerini sonraki "makine nesillerine" aktarabilmektedir. Makineler, dışsal araçlarla öğrenen, bilgi ve tecrübelerinin yalnızca bir kısmını sonraki nesillere iletebilen insanlara nazaran evrimsel bir üstünlüğe sahiptir. Bu tür bir zekâ aktarımı gittikçe genişleyen bir düşünme pratiğini mümkün kılmaktadır. Belki de ileride doğal insan zekâsı ile yapay zekâ arasındaki keskin ayrım ortadan kalkabilecektir.

Bununla birlikte, bir programın zekâsı, yukarıda ele alındığı üzere sosyal ortamdaki performansı da dikkate alınarak değerlendirilmelidir. Bu nedenle toplumda etkisi gittikçe görünür olan yapay zekânın toplumsal ve çevresel etkileriyle ele

[9] Turing, 438
[10]Turing, 456.
[11]Cathy O'Neil, **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**, Crown Publishers: New York, Eylül 2016, s.33.

alınması gerekir[12]. Aşağıda yapay zekânın, nasıl öğrendiği ve öğrendikleriyle ne tür bir etki yarattığı değerlendirilecek, ardından ceza muhakemesinde kullanılan yeni risk analiz teknolojileri açıklanırken, nasıl bir toplumun tahayyül edildiği üzerinde durulacaktır. Bu tahayyül, kuşkusuz yapay zekâ teknolojilerinin kullanılma şeklini de etkilemektedir.

B. Günümüzde Yapay Zekâ Teknolojileri

Alan Turing 20. yüzyılda makinelerin geldiği aşamayı sınayabilmek adına ürettiği test sırasında, bir araştırmacı, görmediği bir makine ve bir kadına yazılı olarak soru yöneltmektedir. Eğer bilgisayar, soru soran kişiyi aslında kadın olanın kendisi olduğuna ikna edebilirse testi geçebilecek ve böylelikle dış görünüşün herhangi bir etki doğurmadığı ortamda salt zekâsını kanıtlayabilecektir[13]. Bu testi geçebilmek için bilgisayarın öncelikle dili taklit etmesi, dolayısıyla doğal dil işleme yetisine sahip olması gerekir. Bunun yanı sıra bilgisayar sisteminin veri deposu bulunmalı ve sistem bu depoda kayıtlı veriler arasında bağlantı kurarak bilgi üretebilmelidir. Otomatik mantık yürütme süreci, bilgisayar sisteminin soruya uygun yanıt verilebilmesini sağlayan son gerekli aşamadır[14]. Elbette bu test, makinenin birebir insan gibi düşünebildiğini kanıtlamak açısından yeterli değildir. Hazırlanan soruların niteliği dikkate alındığında, klişeleşmiş toplumsal kadın-erkek rollerine sıkışarak "kadın taklidi" yapmaya çalışan bir makinenin gerçek hayattaki insanın karmaşıklığını yansıtabildiğini söylemek mümkün olmayacaktır[15].

Görüldüğü üzere yapay zekâ için ilkin insana benzer düşünsel yetilere sahip olması amaçlanmıştır. Bu amacın yansımaları, Robokop ve Terminatör filmlerinden çok daha önce Antik Yunan döneminde dahi görülmektedir. İnsanoğlu kendisine benzer makinelerin üretimini her dönemde hayal etmiş, Talos mitinde yer alan "yapay askerler", doğumla değil insan eliyle yaratılan otonom zekânın ilk örneklerini

---

[12]Çağatay Topal, "Alan Turing'in Toplumbilimsel Düşünü: Toplumsal Bir Düş Olarak Yapay Zekâ", **Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi**, Cilt:57, Sayı: 2, 2017, 1340-1364, s. 1355-1357.

[13] Cem Say, **50 Soruda Yapay Zekâ**, 7 Renk Basım Yayınevi: İstanbul, Nisan 2020, İstanbul, s. 34.

[14] Russell/Norwig, s.2

[15]Huma Shah/Kevin Warwick, "Imitating Gender as a Measure for Artificial Intelligence: Is It Necessary?" In **Proceedings of the 8th International Conference on Agents and Artificial Intelligence**, Roma, 2016, ss. 126-131, s.130.

oluşturmuştur[16]. "Yapay genel zekâ" olarak adlandırılan bu zekâ, insan sinir sisteminden esinlenmekte, bu tür bir zekâ ile birebir insana benzer şekilde algılayan, konuşan, muhakeme yapabilen yazılım ve donanıma sahip bir sistemin kurulması amaçlanmaktadır. Antik dönemden bu yana aynı düşün peşinden koşulmakta, bugün derin öğrenme, yapay sinir ağları gibi modeller bu amaçla oluşturulmaktadır[17]. Düşünen, öz bilince ve duygulara sahip yapay genel zekânın yaratılma çabasından hiç vazgeçilmemiş, Turing testini başarıyla geçen bir yazılımın üretilmesi için pek çok yöntem denenmeye devam edilmiştir. Dolayısıyla, biyolojik olmayan bir donanım içinde dünyayı algılayan, nasıl düşündüğü üzerine düşünebilen ve fonksiyonel olarak yeni soru ve sorunlara yanıt verme yetisine sahip bir beynin üretilmesi olarak ifade edilen "genel yapay zekâ" çalışmaları hızla devam etmektedir[18].

Ancak günümüzde varılan aşamada, bu tür bir zekânın yapay olarak üretilebildiğini söylemek mümkün değildir. Yapay zekâ, henüz yazılımcılar tarafından öngörülen programın dışına çıkamamaktadır[19]. Kendi kararlarını alan ve en önemlisi kendisi ve aldığı kararlar üzerine düşünebilen bir yapay zekâ üretilememiştir. Yine de bu durum ileride bu tür bir yapay zekânın üretilemeyeceği anlamına gelmemektedir[20].

Bugünkü yapay zekâ modelleri, yalnızca belirli bir problemin çözümü için geliştirilen ve veriden öğrenen yapay dar zekâ olarak adlandırılan sistemlerdir[21]. Başka bir deyişle, henüz çok boyutlu şekilde düşünebilecek kadar zeki olmayan yazılımları "yapay zekâ" olarak adlandırdığımız bu dönemde, tek bir alanda kendisine verilen görevi ifa etmeye elverişli yazılımlar, henüz bir çocuğun bilişsel zekâsına bile sahip değildir. Örneğin bir çocuk, yerdeki oyuncaklara takılmadan yürümeyi becerebilecekken, temizleme görevini yerine getirmek üzerine programlanmış bir robot, boyut ve alan hesaplaması yetisine sahip değil ise en ufak bir engelde yere

[16]Adrienne Mayor, **Gods and Robots: Myths, Machines, and Ancient Dreams of Technology**, Princeton University Yayınevi: Princeton, Kasım 2018, s.28, 29.
[17]Merve Ayyüce Kızrak/Bülent Bolat, "Derin Öğrenme ile Kalabalık Analizi Üzerine Detaylı Bir Araştırma", **Bilişim Teknolojileri Dergisi**, Cilt: 11, Sayı: 3, Temmuz 2018, ss.263-286, s.266.
[18]John R. Searle, "Minds, Brains, and Programs", İçinde, **Foundations of Cognitive Pscyhology: Core Readings**, Ed: Levitin, Daniel J. Levitin, MIT Press: Cambridge, Ekim 2002, ss. 95-113, s.95.
[19] Zeynel Kangal, **Yapay Zekâ ve Ceza Hukuku**, On İki Levha Yayıncılık: İstanbul, Mayıs 2021, s. 27.
[20] Turing, 450.
[21] Ayyüce Kızrak/Bolat, s. 266

devrilmeye mahkûmdur[22]. Bugün AlphaGo oyunu şampiyonunu yenen DeepMind tarafından üretilmiş zekâdan, kanser teşhisinde yararlanılan IBM üretimi yapay zekâ teknolojilerine, hikâye yazabilen, haber üretebilen, interaktif şekilde insanlarla konuşabilen, sosyal medya hesapları üzerinden profil çıkartarak hedeflenmiş reklamları gösteren, Predpol gibi suç işleme potansiyeli barındıran kişileri listeleyen tüm yapay zekâ modelleri, bir alanda kendilerine verilen komutları insan kapasitesinin üstünde bir hızla yerine getirebilirken, diğer alanlarda zeki niteliğini taşımaktan oldukça uzaktır. Dahası bu zekâ modeli, işlediği verileri anlamlandırmadan otomatik olarak sonuçlara varmakta, karar almak üzere kullanıldıklarında etik ve vicdan gibi süzgeçler barındırmamaktadırlar.

Bu nedenle günümüzde asıl korkulması gereken, insan zekâsını aşacak ve insanı hâkimiyet altına alacak, adeta bir distopya senaryosu haline gelmiş yapay zekâ değildir. Tehlikenin kaynağı, yapay zekâ teknolojilerini yaratanların onları ne amaçla ve nasıl kullandığıdır. Mevcut durumda, henüz zeki olmayan ve adalet körü bir teknolojinin, her alanda kullanılması, kontrol edilmesi güç sonuçlar doğuracaktır. Nitekim bir klasik olmuş Frankenstein kitabında da verilen öğüt aynıdır: Yapay bir şekilde üretilen Frankenstein, yapay ve zeki olduğu için değil sahibi tarafından terk edildiği için kontrolden çıkmıştır[23].

Yapay zekânın işleyiş modelini gözlemlemek, teknolojik gelişme sürecini kontrol altında tutabilmek adına büyük önem taşımaktadır. Bu amaçla aşağıda kısaca makine öğrenmesi, derin öğrenme, gözetimli-yarı gözetimli öğrenme gibi öğrenme türleri incelenecektir. Öğrenme modellerini anlayabilmek adına "algoritma" gibi önemli bazı kavramlar üzerinde durulacaktır. Ardından işleyiş modelleri tarif edilen yazılımların ceza muhakemesi alanında ne şekilde kullanıldığı üzerinde durulacaktır.

C. Algoritma Kavramı

Algoritma, 9. yüzyılda "Cebir ve Denklem Hesabı Üzerine Özet Kitap" isimli kitabı yazarak cebirin temelini oluşturan ünlü İranlı matematikçi Al Khwarizmi'nin

[22]Broussard, Meredith, **Artificial Unintelligence: How Computers Misunderstand the World**, MIT Press: Cambridge, Mayıs 2018, s.87, 88.
[23] Coeckelbergh, s.19.

isminden üretilmiş bir kelimedir[24]. Günümüzde yeni bir zekâ türünün doğumuna olanak veren algoritmalar olmuştur.

Algoritmayı belirli bir problemin çözüm yolunu gösteren sıralı komutlar olarak tarif etmek mümkündür. Nitekim insanların zihni de algoritmalara benzer şekilde çalışmaktadır. Buna en basit örnek olarak yemeğin nasıl pişirileceğini gösteren tarifler verilebilir[25]. Örneğin dört kişilik bir ailede yemek hazırlarken eldeki malzemelerle en etkin sonuca ulaşmak için dikkate alınması gerekenler sanıldığı kadar basit değildir. Bunun için öncelikle evde olan veya o sırada ulaşılabilen malzemeler bilinmeli, ne kadar zamana ve enerjiye sahip olunduğu gözetilmeli, hangi aile bireyinin hangi yemeği en çok sevdiği, hangi bireyin ne kadar yediğinde doyduğu ve en sağlıklı yemeğin bu şartlar altında hangisi olabileceği gözetilmelidir. Basit bir yemekten diğer tüm faaliyetlere, gündelik hayatımızda sürekli dinamik ve değişken modeller kurmamız gerekir. Matematiksel ve öngörülebilir modeller, fikrimizi başkasına aktarabilmemizi, dolayısıyla yokluğumuzda başka birinin aynı modelleri kullanarak yaptığımız işlemleri tekrarlayabilmesini mümkün kılar. Başka bir deyişle, bu modeller hareketlerimizin otomasyonunu, öngörülebilirliğini ve taklit edilebilmesini sağlar. Ancak oldukça kolay gözüken yemek pişirme faaliyetinin dahi, her somut olaya uyarlanabilir şekilde komutlara dökülemeyeceğini, yani, gerçek hayatın karmaşıklığının algoritmalara indirgenemeyeceğini söylemek mümkündür. Nitekim sıradan bir gün için oluşturduğumuz yemek modeli, yalnızca doğum günlerinde çocukların fast food yemesine izin verilmesi gibi pek çok ince detayı ve istisnayı barındırmamakta, sadece genellemeler içermektedir. Dolayısıyla insan davranışına ilişkin tüm modeller, kişisel detaylara ve yaşamın karmaşıklığına karşı kör denebilecek basite indirgemelerden ibarettir[26].

Algoritmalar, insanlardan farklı olarak dünyayı ancak kendilerine sunulan veriler üzerinden yorumlayabilmektedir. Ayrıca verileri bağlamı içinde anlama, sezgi, idrak gibi kabiliyetlerden yoksundurlar. Karmaşık veya yeni bir durumla karşılaştıklarında, öngörüde bulunmaları ve kendi başlarına karar almaları mümkün olmamaktadır. Bu nedenle, dünyayı bütüncül bir şekilde kavramayı gerektiren sosyal

[24] Fernando Iafrate, **Artificial Intelligence and Big Data: The Birth of a New Intelligence**, Wiley Publications: London, Mart 2018, s.34.
[25] O'Neil, s.34
[26] O'Neil, s. 18, 19.

bilimler ve özellikle hukuk alanında kullanıldıkları takdirde eksik veya hatalı sonuçlara varmaları kaçınılmazdır[27]. Daha da önemlisi, algoritmalar, insan zihnine benzer şekilde verileri bilişsel bir süzgeçten geçirmekten yoksundur, aksine veriler arasında bağ kurarak yalnızca istatistiksel sonuçlar çıkartmaktadırlar. İnsanlarca öngörülen amaçlar içerisinde hareket etmeleri ve kendilerine sunulan verilerle sınırlı işlemeleri nedeniyle dünyayı otonom bir şekilde yorumlamaktan uzaktırlar. Dolayısıyla algoritmalar programcıların yazdığı adımları takip eder, ancak tamamen özerk bir bilinç geliştiremezler[28].

Sonuç olarak algoritma kavramını izlenmesi gereken yöntemi gösteren, etkin, sayısal bir kural dizisi olarak tanımlamak mümkündür[29]. Bu kurallar belirli özellikleri barındırmaktadır. Öncelikle insan eliyle yaratılmış ve sonlu sayıdadırlar ve gerçek hayatı matematiksel bir kesinliğe indirgeyerek çalışırlar. Algoritmayı teşkil eden adımların mutlaka önceden tanımlanmış olması gereklidir ve programlama dili sayesinde bu kesinlik tesis edilir. Algoritma uygulanmaya başlamadan önce sisteme girdi veriler sunulur. Girdileri süreç içerisinde dinamik olarak sunmak da mümkündür. Bunun yanı sıra, algoritmalar girdilerle belirli bir ilişkisi olduğu düşünülen çıktılar üzerinde çalışır, bunlar arasında istatistiksel bağlar kurarlar[30]. Milyonlarca veri arasında insanlar tarafından tespit edilmesi mümkün olmayan tekrarları ve örüntüleri tespit ettikleri ve ilgili verileri gruplandırdıkları için önemli bir kolaylaştırıcıdırlar. Bununla birlikte algoritmaların vardıkları sonuç herhangi bir yargı içermemektedir[31]. Yalnızca verilerin mekanik bir şekilde ele alınıp gruplandırılmasından ibarettir. Bu bağlamda algoritmalarla varılan sonuç, adalet, eşitlik, vicdan gibi kavramlardan yoksundur.

---

[27] **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, Erişim Tarihi: 30.12.2020, s.34.

[28] **European Commisson**, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-65-F1-EN-MAIN-PART-1.PDF, Erişim Tarihi: 31.12.2020, s.16.

[29] Marvin Minsky, **Computation: Finite and Infinite Machines**, Prentice Hall: London, Ocak 1967, s. 106.

[30] Donald E. Knuth, **The Art of Computer Programming: Fundamental Algorithms**, Adison Wesley Publications, Massachusettes, Cilt: 1, Ocak 1938, s.5, 6.

[31] Roben K. Hill, "What an Algorithm is", **Philosophy and Technology Journal**, Cilt: 29, 2016, ss. 35–59, s. 45.

Algoritmaların çalışma şeklini etkin kılan husus, sunulan veriler arasında bağ ("correlation") kurabilmeleri ve bu bağları hatırlayarak kendi kendilerine öğrenebilir hale gelmeleridir. Nitekim yapay zekâ dediğimiz husus da bu öğrenme sistemi üzerine inşa edilmiştir[32]. Dolayısıyla aşağıda ele alınacak olan öğrenme modelleri algoritmalar aracılığıyla tesis edilmektedir.

D. Yapay Zekâ Kapsamında Öğrenme Kavramı

Öğrenme, kişinin tecrübeleri, eğitimi, başkalarından gözlemledikleri ile şekillenen bir süreçtir. Öğrenme, bir bakıma "ders çıkararak" kişiyi daha farklı ve daha iyi sonuçlar alacak şekilde davranmaya yöneltir. Bu süreç, sosyal ve mesleki davranış kalıplarına sirayet eder, kişinin sosyal çevresine ve gündelik hayata uyum sağlamasını mümkün kılar. Bununla birlikte doğal uyum sağlama, öğrenme ile ilişkili değildir, doğal seleksiyon sonucu tesadüfi bir nitelik gösterir. Sosyal ve ticari hayata uyum sağlama ise bu şekilde tesadüfen gerçekleşmez, zaman içerisinde, kişinin hareketleri sonucu aldığı tepkiler ve edindiği bilgiler ile şekillenir. Nitekim bu sayede insan, çok küçük yaştan itibaren, tanıdık yüzleri seçme, kendisine aktarılan dili anlama, yürüme, konuşma yetilerini kazanabilir. Her kuşak, diğer kuşağın bilgi ve tecrübelerine yenisini eklemekte, böylelikle düzenli bilgi birikimi aktarımı insanlık tarihini şekillendirmektedir. Her ne kadar internet çağında öğrenme kavramı, yeterli veriye erişme ile eş tutulsa da eğitim ve deneyimin olmadığı bir öğrenme tanımı eksik olacaktır[33].

Yapay zekâ öğrenmesi ise bu tür "sosyal seleksiyondan" geçmemektedir. Algoritmaların insanlar gibi öğrenebilmesi için, çeşitli seçenekler arasında tercih yapmaları, hata yaptıkları takdirde reaksiyon görmeleri gerekir. Nitekim yapılan tercihlerin hatalı ya da doğru olması tecrübelere dönüşecek ve bu tecrübeler öğrenmenin ilk adımını teşkil edecektir. Oysa algoritmanın varmak istediği amaç baştan tanımlıdır. Yine kendisine sunulan veriler ile bağlı olan algoritmaya, yalnızca en baştan tarif edilmiş çözüm önerileri arasından en etkin olanı seçme yetisi kazandırılmaya çalışılmaktadır[34]. Öğrenme algoritmaları, günümüzde tecrübe

[32] Iafrate, s.33.
[33] Iafrate, s.33, 34.
[34] Iafrate, s.13, 14.

biriktirmemekte, yalnızca sunulan veriler arasındaki benzerlik ve döngüleri tespit etmekte, bu dağınık veri kümesini insanlar tarafından kullanılabilir hale getirmek üzere hazırlanmaktadır.

Bununla birlikte insan öğrenmesine benzer şekilde "yapay zekâ da tecrübelerinden yola çıkarak kendi kendine öğrenebilir mi?" sorusu hala ucu açık bir sorudur. Bilgisayar programcısının hiçbir müdahalesi olmadan, kendi kendine işlemlerini düzelten ve geçmiş hatalarından öğrenen bir yazılımın mümkün olup olmadığı tartışılmalıdır[35]. Bu noktaya ulaşabilmek için yürütülen denetimli ve denetimsiz makine öğrenmesine çalışmaları devrimci bir nitelik barındırmaktadır. Bu nedenle aşağıda bu çalışmalar dikkate alınarak yapay zekâ çalışmalarında gelinen nokta üzerinde durulacaktır.

1. Eski Model Öğrenme Teknikleri

Yapay zekâ çalışmaları, 1980'li yıllara kadar "simgeci öğrenme metodu"na dayanmıştır. Bu yöntem, zekânın bir simge işleme süreci olduğuna, dolayısıyla bilgiyi işlemek ve aktarmak için, mantık kuralları çerçevesinde matematiksel kurallar dizini oluşturulmasının yeterli olduğuna dayanmaktadır. Bu görüşe göre, bilişsel süreç de aynı programlama gibi başlangıç ve sonuç dizilimi olan bir hesaplama zincirinden ibarettir. Örneğin basit bir programla ile aile bireyleri arasındaki "A, B'nin babasıdır", "C, A'nın kardeşidir", "dolayısıyla C, B'nin amcasıdır" sonucuna varılabilecek şekilde mantık zincirleri kurularak makinenin aile ağacını öğrenmesi sağlanabilir. Aile ağacının öğrenilmesinin ardından, genlerin yüzde kaç oranında paylaşıldığı, mirasın yüzde kaç oranında aktarılacağı gibi hesaplar da kolaylıkla bir dizi simge zincirinin kurulmasıyla otomatik olarak yapılabilecektir[36]. Bununla birlikte, bu şekilde yazılan program, insan tarafından belirlenen kuralların dışına çıkamaz. Dahası bu program işlediği verilerin neye dair olduğunu, bağlamını ve sembollerin ötesinde nasıl bir anlamı olduğunu bilmemektedir. Oysa A ve B şeklinde semboller haline getirilmiş bu kişileri tanıyan biri, bu kişilerin yüzlerini, seslerini, karakterlerini de bilmektedir. Dolayısıyla bir insanın zihninde, bu kişileri gösteren simge, o kişilerin isimleri ve akrabalık derecelerinin çok ötesinde, çok daha karmaşık ve çetrefilli bir bilgi ağını

[35] Iafrate, s.22.
[36] Say, s. 93, 94.

içermektedir. İnsanlar, simgelerle birlikte duyu organları ve diğer yetilerinden gelen bilgileri birleştirmektedir. Bu nedenle yalnızca matematiksel simgeler ve mantık kuralları ile öğrenen yapay zekâ, hayatın karmaşıklığını anlamlandırma yetisinden yoksun kalmaya mahkûmdur[37]. Bu tür bir yapay zekâ, hatasız, istisnasız bir mantık zincirinden oluşmayan şartlarla karşılaştığında bu şartlara uyum sağlayamayacaktır[38].

Ancak tüm bunlar, simgesel öğrenme metodunun tamamen başarısız olduğu ve günümüzde artık bu metoda ihtiyaç duyulmadığı anlamına gelmemektedir. Örneğin bugün karar ağacı denilen ve simgesel öğrenmeye dayanan yöntem çeşitli alanlarda uygulanmaktadır. Bu yöntemde, bir listede toplanmış tüm veriler ve olası sonuçlar kümeler halinde sıralanır. Örneğin yaş, cinsiyet, iş, sigara kullanımı, kilo, ailede daha önce bulunan hastalıklar gibi pek çok veri kümesinin yanı sıra kalp hastalığı, soğuk algınlığı, kanser, egzama gibi olası sonuçlar kümesi de oluşturulur. İşte karar ağaçları, tüm bu veri ve sonuçları tarayarak istatistiksel olarak ilişkili gördüğü veriler arasında "eğer…ise, o zaman…" şeklinde kurallar oluşturur. Örneğin eğer kişi 50 yaş üzerinde ise kalp hastalığı ihtimali bulunmaktadır şeklinde bir kural oluşturabileceği gibi farklı bağlantılar kurarak kişi spor yapıyor ve yabancı dil biliyor ise egzama hastalığına yakalanma ihtimalinin düşük olacağı gibi insan gözüyle hemen öngörülmeyen bağlantılar da üretebilecektir. Nitekim karar ağacı yöntemiyle öğrenme, günümüzde hastalık teşhislerinde kullanılmakta ve bu tür bağlantıları gözden kaçırmamak adına bu algoritmalara hastaların tedavisinde uzman görüşü olarak başvurulmaktadır. Karar ağaçları, zorlu ve farklı problemlere otonom şekilde cevap verememekle birlikte, şeffaf ve anlaşılabilir adımlar sunmaları nedeniyle, takibi, kontrol edilebilirliği ve hesap verilebilirliği en kolay yöntemlerden biridir[39].

Simgesel yöntemler, örneğin ceza muhakemesinde iddia, savunma ve yargılamanın bir yapay zekâ programı tarafından varılan sonuca giden her adımı izleyebilmesini mümkün kılar. Nitekim bu yöntemde, hangi veriden hangi sonuca ulaşıldığı, sonuca ulaşırken hangi verilerin yüzde kaç etkili olduğu kurallar halinde gösterilmektedir. Ancak elbette, bir davanın somut koşullarının değerlendirilmesi,

[37] Say, s. 95,96.
[38] Say, s. 96.
[39] Coeckelbergh, s. 71, 72.

fiilin niteliği, failin saiki gibi pek çok hususta tüm ihtimallerin öngörülerek veri kümesi olarak belirtilmesi ve sürecin tamamen sembollerle ifade edilmesi mümkün değildir.

Simgesel öğrenmeye farklı alanlarda başvurulmakla birlikte, günümüzde yapay zekâ alanında aşağıda incelenecek farklı öğrenme modelleri ortaya çıkmış, yeni yöntemlerle yapay zekâ, çok boyutlu düşünebilen bir zekâ modeline yaklaştırılmaya çalışılmıştır.

2. Makine Öğrenmesi

Makine öğrenmesi, makinelerin programlanmış, rutin ve otomatikleşmiş görevleri ifa etme yöntemlerini geliştirebilmeleridir. Bu bağlamda makineler kendileri için öngörülen amaca en hızlı ve doğru şekilde ulaşmaya çalışırlar, ancak bu tür bir öğrenme yoluyla "bilgelik" kazandıklarını ileri sürmek mümkün değildir[40].

Öğrenme geçmiş tecrübelerden sonuç çıkarma şeklinde olabileceği gibi, deneysel şekilde veya analojiye başvurma şeklinde de gerçekleşebilir. Makine öğrenmesi aslında makinenin kendisi için öngörülmüş sınırlı görevi ifa etmede gittikçe daha fazla yetkinlik kazanmasıdır[41].

Makine öğrenmesi ile programlama alanında önemli bir atılım yapılmıştır. Geleneksel olarak bir programcı program için kullanılacak girdi veriler, sonuç verilerini ve hatta bunlar arasındaki işlemleri sürecin en başında belirlemektedir. Makine öğrenmesi yönteminde ise veri setleri hazır verilmekle birlikte, bunlar arasında bağ ve kuralları bulma görevi programa bırakılır[42]. Programın bizzat kuralları üretmesi, aslında insan benzeri otonom bir yapı kazanmaya yönelik önemli bir adımdır. Bu bağlamda uygulayacağı her kural baştan öngörülen bir sistem yerine, kendi kendini geliştiren ve öğrenen bir sistem kurulmaya çalışılmaktadır.

---

[40] Broussard, s.89.
[41] Broussard, s. 91, 92.
[42] Kangal, s. 25, Eylem Aksoy Retornaz/Osman Gazi Güçlütürk, "Yapay Zekânın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi", İçinde**: Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ**, Ed. Eylem Aksoy Retornaz/Osman Gazi Güçlütürk, On İki Levha Yayınevi: İstanbul, 2021, ss.275-302, s.279.

Bununla birlikte makine öğrenmesi, sunulan veriler üzerinden gerçekleşmekte, hangi verilerin kullanılacağı ve dolaylı olarak öğrenme süreci yine insan tarafından tayin edilmektedir. Örneğin eski usul yapay zekâ öğrenme modellerinde, yapay zekânın bir fotoğraftaki kedi, köpek ve diğer hayvanları tespit etmesi için yazılımcı bir kediyi "dört patili, iki gözlü, keskin çeneli ve tüylü" gibi sıfatlarla formüllere dökmektedir. Günümüzde ise makine öğrenmesi için milyonlarca hayvan fotoğrafı girdi olarak kullanılmakta, makine bu örnekleri süzerek hangi hayvanın hangi ayırt edici özelliği olduğunu öğrenmekte ve bu yolla hayvanları gruplara ayrıştırabilmektedir. Ancak yetersiz veya hatalı veriler sunulduğunda, makine elbette bu veriler üzerinden eğitildiğinden hatalı bir şekilde öğrenmektedir.

Kimi zaman algoritmaların simgeci öğrenmede olduğu gibi keskin formüllerle sınırlı kalmaması, milyonlarca veri akışı içerisinde daha esnek ve sürekli kendini güncelleyen bir şekilde çalışması gerekir. Bu durum örneğin yol tarifi veren algoritmalar için geçerlidir. Böyle bir yazılım, gidilecek güzergâhı farklı kişiler, farklı telaffuz şekilleri ile söylediğinde dahi tespit edebilecek kadar fazla veri ile beslenmiş olmalıdır[43]. Nitekim Facebook, Google, akıllı telefonlar gibi pek çok kaynaktan toplanan verilerin çeşitliliği, makine öğrenmesine ivme kazandırmıştır. Ancak başarılı bir öğrenme için, insanlar tarafından veri girdi ve çıktılarının düzenli denetimi ve hatalı verilerin ayıklanması zorunludur.

Makine öğrenmesinde makine, yalnızca farklı veriler arasındaki bağlantıları tespit etmekte ama verilerin anlamını, bağlamını ve yaptığı işlemin içeriğini idrak edememektedir. Bu nedenle öğrenme şekli bir nevi "otomatlaşmış" istatistiksel öğrenmedir.

Geleneksel makine öğrenme yöntemlerinde, makinenin öğrenme kapasitesi yine programcının fikirleri ve öngörüsü ile sınırlı kalmaktadır. Bununla birlikte, yeni makine öğrenme modelleri, veriler arası bağ kurarken önceden öngörülmüş formülleri izlemek zorunda kalmazlar. Verileri eşleştirme ve gruplama sonucu kendi kendilerine sonuca varırlar. Kimi zaman bu sonuçları başka ve yeni bir veri setinin girdisi olarak kullanmak üzere aktarırlar, böylelikle sürekli değişen ve dönüşen bir model

[43] Peter Buxmann/Holger Schmidt, **Künstliche Intelligenz mit Algorithmen zum Wirtschaftlichen Erfolg**, Springer Yayınları, 2019, https://doi.org/10.1007/978-3-662-57568-0, s.8.

oluşturulur. Dolayısıyla makinelerin kendi kendine öğrenebilmesi ve yazılımcılar tarafından öngörülmeyen, bağımsız türetilmiş veri yaratmaları mümkün olmaktadır[44]. Böylelikle dış bir müdahale ile kendilerine yeni komut verilmesi gerekmeksizin makinelerin kendi kendini geliştirmesi söz konusudur. Nitekim makineler, günlük hayatın çetrefilliği karşısında, farklı değişkenleri kendiliğinden dikkate aldığı ve yeni koşullara uyum sağlayabildikleri ölçüde gerçek anlamda öğrenmeden bahsetmek mümkün olacaktır.

Bu nedenle günümüzde, sınırsız sayıda veri ile eğitilen algoritmaların, kendi kendine kurallar belirlemeleri ve yazılımcı tarafından öngörülmemiş problemlerle karşılaştıklarında dahi çözüm üretebilmeleri amaçlanmaktadır. Bir adım daha öteye gidilerek, bilgisayarların insan tarafından incelenmesi ve analiz edilmesi mümkün olmayan veri yığını üzerinden bağımsız modeller üretebilmeleri ve geçmiş verilerden yola çıkarak gelecekte ortaya çıkabilecek senaryoları öngörmeleri beklenmektedir. Bu durum, özellikle geleceğe yönelik potansiyel suç ve suçlunun tespiti için ceza hukuku alanında da başvurulan bir yöntem haline gelmiştir[45].

Makine öğrenmesinde Naive Bayes sistemi, destek rektör makineleri, yapay sinir ağları gibi farklı yöntemlere başvurulduğu görülmektedir. Yine başka bir yöntem olan "derin öğrenme" metodu, çok katmanlı yapay sinir ağları aracılığıyla yapay zekânın "düşünme" şeklini, insan zihni gibi karmaşıklaştırmak amacıyla kullanılmaktadır. Bununla birlikte söz konusu yöntemler, makinenin öğrenme sürecinin takibini ve kontrolünü güçleştirmekte, kişisel veriler kısmında hukuki sonuçları tartışılacağı üzere, yazılımın "kara kutu" haline gelmesine ve yazılımı üreten kişinin bile kimi zaman açıklayamadığı bağlantıların kurulabilmesine yol açabilmektedir[46].

Tez kapsamında üzerinde sıklıkla durulacak kara kutu problemini basit bir şekilde anlatmak adına otonom araç kullanımının temellerinin atıldığı ve Dean Pomerlau tarafından 1991 yılında gerçekleştirilen araştırma örnek verilebilir.

---

[44] Nico Lück, **Lernende Künstliche Intelligenz in der Rüstungskontrolle**, PRIF Report 4/2019, https://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/prif0419.pdf, s.5, 6.
[45] Johannes Graf Ballestrem/Ulrike Bär/Tina Gausling/Sebastian Hack/Sabine von Oelffen, **Künstliche Intelligenz Rechtsgrundlagen und Strategien in der Praxis**, Springer Gabler Yayınları, 2020, https://doi.org/10.1007/978-3-658-30506-2, s.15
[46] Coeckelbergh, s.71, 72.

Pomerlau geçtiği yollarda, bilgisayarını kameradan görüntü alacak şekilde programlamış, böylelikle sokağı, trafiği ve kendisinin trafikteki tepkilerini kaydeden programın, yapay nöron ağları ile kaydettiği tüm verilerden bir sonuç çıkarmasını beklemiştir. Pomerleau ayrıca yola her çıktığında sistemi eğitimden geçirmiş, ardından programın sürücülüğü devralmasına izin vermiştir. Ancak bir gün bir köprü yakınında otonom şekilde ilerlemekte olan araç yoldan çıkınca bunun sebebini keşfetmek oldukça güç olmuştur. Bunun nedeni bu tür öğrenme modellerinde, makinenin tüm öğrendiklerini belirli bir dijital hafıza bölgesinde kaydetmemeleri, dolayısıyla salt bir bölgedeki verilerin incelenmesinin sürece dair fikir vermemesidir. Aynı insan beyninde olduğu gibi, özellikle yapay nöronların kullanıldığı derin öğrenme yöntemlerinde, öğrenme sırasında ve sonucunda edinilen bilgiler tüm sisteme yayılmakta ve sürecin deşifre edilmesi insan beynini deşifre etmek kadar güç olmaktadır. Pomerlau'nun bu deneyi 1991 yılında gerçekleştirdiği göz önüne alınmalıdır; bu güçlük çok fazla katmanı olmayan yapay nöronlar ve oldukça sınırlı sayıda veri kullanılmasına rağmen yaşanmıştır. Pomerlau pek çok kez programa farklı görseller tanıttıktan ve yazılımın tek tek bu görsellere tepkisini ölçtükten sonra sorunu tespit edebilmiştir. Yazılım, insanların hayatın olağan akışında araç sürerken vardıkları sonuçlardan oldukça farklı şekilde, yakınında yeşillik bulunan yol kenarlarını kendisine hareket noktası olarak sabitlemiştir. Bununla çelişen köprü görüntüsü ise karışıklığa yol açmış ve aracın yoldan sapmasıyla sonuçlanmıştır[47].

Bugün milyonlarca veri üzerinden eğitilen yazılımın ne şekilde işlediği, bu nedenle "kara kutu" şeklinde ifade edilmektedir. Veriler arasında kurulan bağlantılar, çok katmanlı nöron sistemleri veya diğer karmaşık yöntemlere dağıtılmakta ve bunları tespit edip incelemek mümkün olmamaktadır. Makineler adeta insanların görmediği yeni bir renk keşfetmiş ve dünyayı insanın göremediği şekilde yorumlar hale gelmiştir. İnsanlar için başta ilgisiz gözüken veriler arasında bağlantılar tespit etmekte, ancak bu bağlantıları insanların anlayacağı nedenler ve sonuçlarla açıklayamamaktadırlar[48]. Bu nedenle kara kutu modeli, kural bazlı eski usul öğrenmeden farklı olarak çok daha kapsamlı sonuçlara vararak insanları uyarabilir, örneğin hiç dikkat edilmeyen bir belirtinin kansere yol açtığını tespit edebilir. Bununla birlikte bu sonuca nasıl

[47] Davide Castelvecchi, "Can We Open the Black Box of AI?", **Nature Journal**, Cilt: 538, Ekim 2016, s.20-23, s.21.

[48] Bu durum, öğrenilen verilerin önem ve değerinin anlaşılmaksızın adeta "ezberlenmesine" benzetilebilir, Kangal, s. 26.

vardığının insan tarafından anlaşılamaması, farklı sorunlar doğuracaktır. Örneğin risk faktörünün ne olduğunu açıklayamayan bir doktorun hangi temellerle önleyici tedaviye başlayabileceği, somut bir neden-sonuç ilişkisi kurmaksızın bunu hastaya nasıl açıklayabileceği sağlık alanında karşılaşılabilecek bir dilemmadır. Hukuk alanında, özellikle ceza hukuku alanında ise usul varsayımlar değil, gerekçe ve deliller üzerinden işlemek zorundadır. Bir sanığa neyle suçlandığının açıklanamaması, onun savunma yapmasını ve adil bir yargılamayı imkânsız kılacak, varılan sonucun meşruiyetini kabul etmek mümkün olmayacaktır.

Bununla birlikte makine öğrenmesi yöntemleri, sürekli gelişmekte ve Ceza Muhakamesi dahil pek çok farklı alanda kullanılmaktadır. Bu nedenle bu yöntemlerin üzerinde durulmalıdır. Aşağıda makine öğrenmesi denetimli, denetimsiz ve pekiştirmeli (takviyeli) öğrenme olmak üzere üç gruba ayırarak incelenecektir[49].

a) Denetimli Öğrenme

Denetimli öğrenme modelinde, yazılıma bir takım veri girdi olarak sunulduktan sonra erişilmesi beklenen sonuçlar da gösterilir. Dolayısıyla varılmak istenen amaç ve doğru sonuçlar sürecin en başında sunulur. Amaç yapay zekânın bu iki veri kümesini birbirine bağlayan genel geçer kuralları öğrenmesidir. Bu bağlamda denetimli öğrenme daha doğrudan ve takip edilebilir bir öğrenme modeli sunar. Bilgisayar, bu süreçte yalnızca veri kümesiyle baş başa bırakılmaz, ulaşması beklenen sonuçlara varana kadar "eğitimden" geçirilir[50]. Öğrenmenin sonucunda, artık sistem kendiliğinden bir sesi, görüntüyü tanımlayabilir veya istenilen bir görevi yerine getirebilir hale gelmiştir. Bu süreçte dışardan bir kontrol mekanizmasıyla varılan sonuçların kontrol edilmesi ve sistem hatalı işlem yaptığında düzeltilmesi gerekir. Sistem, eldeki veriler arasından görüntü seçme, yüz tanıma veya diğer işlemleri yerine getirebilir hale geldiğinde, yeni veriler sunularak öğrenmenin tamamlanıp tamamlanmadığı test edilir. Bugün büyük veri ve yeni teknolojik gelişmeler sayesinde denetimli öğrenme algoritmaları çok daha etkin hale gelmiştir. Pek çok yapay zekâ uygulamasında başvurulan denetimli öğrenmenin en bilinen örneği, çevrimiçi tercüme

[49]Muhammet Atalay, "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt: 9, Sayı: 22, 2017, s.155-172, s.161.
[50] Broussard, s. 93.

araçlarıdır. Milyonlarca metinden yola çıkan bu programlar, kendilerine gösterilen sonuçlarla istatistiksel bağlar kurmakta, yanlış tercüme yaptıklarında müdahaleye uğramaktadır. Sonuç olarak istenilen metin ile en bağlantılı olabilecek çeviri metnini sunmayı denetimli öğrenme sonucunda gerçekleştirebilmektedirler[51].

Dolayısıyla denetimli öğrenme dört adımda gerçekleşir. Öncelikle yazılımcı hangi sonuçlara varılması gerektiğine dair tasavvurda bulunur. Ardından makineye model olarak ne tür sonuçlara varması gerektiğini etiketlenmiş verilerle sunar. Üçüncü adım olarak hiç işlenmemiş veri kategorize edilmek üzere sisteme sunulur ve son olarak sistemin "çıktı" olarak vardığı sonuç denetlenir[52] ve sistem en baştan varılması istenen sonuca ulaşıncaya kadar eğitime devam edilir. En eski ve yaygın sistem olan denetimli öğrenme aslında takibi en kolay ve kontrol edilebilir olan öğrenme modelidir.

b) Denetimsiz Öğrenme

İnsan öğrenme modeline en yakın olan bu modelde yalnızca veri üzerinden değil, ayrıca tecrübe üzerinden öğrenme de devreye girer. Denetimsiz öğrenme aslında doğa içerisinde canlıların koşullara uyum sağlamalarını ve dolayısıyla hayatta kalmalarını sağlayan öğrenme modelidir. Algoritmalar açısından ise bu öğrenme modeli, algoritmaların kendi kendilerine sonuç üretmelerini ifade eder. Programcının önceden sonucu öngördüğü ve makine öğrenmesi ile programı bu sonuca ulaşana dek eğittiği denetimli öğrenme modelinden farklı olarak, denetimsiz öğrenmede varılacak sonuca dair önceden bir tahayyül söz konusu değildir.

Aslında insan denetimi ve bilgisinin sınırlarını aşan dijital bir düzende, yapay zekânın sınırlandırılmaksızın çıkarımlarda bulunabilmesi, insana daha çok katkı sunabilme potansiyeli barındırmaktadır[53]. Böylelikle veri yığını ardında, insan idrakinin ötesinde kalan bilgiler makineler eliyle ortaya çıkartılabilecektir. Bu öğrenme şeklinde, artık makine kendisinin öğretmenidir, ele aldığı verilere ve "tecrübelerine" dayanarak çıkarım yapabilir hale gelmesi beklenmektedir.

---

[51] Iafrate, s. 22, 23.
[52] Iafrate, s. 24.
[53] Iafrate, s. 28, 29.

Örneğin denetimli öğrenme modelinde, önce havaalanında suç işleyen insan görüntüleri bir veri kümesi olarak sisteme girilir. Ardından diğer bir veri kümesi olarak suç teşkil etmeyen hareketler sunulur. Böylelikle hangi hareketlerin suç teşkil ettiğine dair çıkarım yapmayı öğrenme sağlanacak, genelleme yapma yetisi kazanan sistemin yeni bir görüntü ile karşılaştığında suçu tespit etmesi mümkün kılınacaktır.

Denetimsiz öğrenme modelinde farklı olan sisteme hangi unsurların suç teşkil eden hareketi oluşturduğu kodlarla tarif edilmez. Algoritmaların kendi kategorilerini oluşturması beklenir. Bu durumda algoritmalar şüpheli hareketi tespit etmede kullanacağı kıstasları kendi seçecek, buna göre güvenlik kümeleri oluşturacaktır. Dolayısıyla, denetimsiz öğrenmeyi asıl ayırt eden, algoritmalara varacakları sonuç hakkında otonom karar verme alanı bırakılmasıdır[54]. Elbette algoritmaların vardığı sonuçlar, insanlar için her zaman anlam ifade etmeyebilir. Başka bir deyişle girdi olarak sunulan verilerden nasıl ilgili sonuca varıldığını açıklamak her zaman mümkün olmayabilir. Bu nedenle denetimsiz öğrenme modeli, sınırsız sayıda veriyi eşleştirerek insanlar için yeni kapılar aralama potansiyeline sahip olsa da şeffaf ve açıklanabilir olma açısından sorunlar barındırmaktadır.

c) Pekiştirmeli Öğrenme

Yukarıda tartışılan iki öğrenme modeli arasında kalan bu modelde, program denetimsiz öğrenmeye benzer şekilde girdi verilerinden sonuç verilerine nasıl ulaşacağını kendi tayin etmekte, ancak doğru sonuçlara vardığında ödüllendirilmektedir. Dolayısıyla öğrenme süreci bir nevi ödül-ceza mekanizması ile desteklenir. Böylelikle yapay zekâ, hatalı işlemleri sonucu farklı yöntemler denemeye yönlendirilir. Pekiştirmeli öğrenme, zaman içerisinde kişilerin davranışlarının sonuçlarından yola çıkarak öğrenme metoduna benzemektedir[55].

Havaalanında suç teşkil eden davranışları tespit etmeyi öğrenen yapay zekâ örneğinden devam edilirse, pekiştirmeli öğrenme için yazılım tarafından varılan sonuçların güvenlik görevlileri tarafından doğrulanması ve sisteme olumlu geri

[54] Coeckelbergh, s. 84, 85.
[55] Norvig/ Russell, s. 830.

bildirim sunulması gerekir. Böylelikle sistem, sonuçları olumlu bildirimlere uyarlayacak şekilde optimize edecektir[56].

Pekiştirmeli öğrenme örneğin satranç, Süper Mario gibi farklı oyun kategorilerinde de sıklıkla kullanılmaktadır. Yenildiğinde geri bildirim alan yapay zekâ, zaman içerisinde insanı yenebilecek kapasiteye ulaşabilmektedir[57]. Bu tür alanlarda, satranç gibi karmaşık yapıda bir oyun öğretilmek istendiğinde, yapılan her hamle için bu hamle ile kazanma oranını hesaplayan bir değerlendirme algoritması da kullanılabilir. Böylelikle bir yazılım, diğer yazılımın öğrenmesini bildirimleriyle destekleyerek kolaylaştıracaktır[58].

Pek çok durumda, pekiştirmeli öğrenmede, öğrenmeyi destekleyen yapay sinir ağları kullanılmaktadır. Yapay sinir ağları, öğrenme aşamasındaki yazılımın oluşturduğu serileri incelemekte, bunlardan en optimum olanını seçmektedir. Böylelikle, sonuçlar gözden geçirilmekte, öğrenme geçmişindeki verilere dayanılarak en etkin sonuçlar benimsenmektedir. Pekiştirmeli öğrenme ve yapay sinir ağları birlikte kullanıldığında, örneğin bir grup zanlının belli kişileri rehin aldığı senaryoda, geçmişte benzer durumlara ilişkin verilerden yola çıkılır, böylelikle en doğru hamlenin ne olacağı hesaplanabilir. Aynı şekilde yüz tanıma algoritmaları açısından da pekiştirmeli öğrenme aşamasında yapay sinir ağları ile denetimin uygulandığı görülmektedir[59]. Buna rağmen makine öğrenmesi ile varılan sonuçlarda hata payı hâlâ sıfıra indirilememektedir.

E. Değerlendirme

Yapay zekâda öğrenmenin amacı ve ne şekilde gerçekleşeceği insan eliyle tanımlanmıştır. Bugün insan müdahalesinin tamamen yokluğunda yapay zekânın var olması mümkün değildir. Yapay zekânın, hangi yöntemlerin daha yararlı olduğunu doğal ve sosyal bir seçilimle kazanması söz konusu değildir. Nitekim yapay zekâ henüz insan müdahalesi ile dahi "kendisini çevresiyle diyalektik ilişkiler kuran bir

[56] Coeckelbergh, s.86.
[57] Richard Berk, **Machine Learning Risk Assessments in Criminal Justice Settings**, Springer Nature Yayınevi, https://doi.org/10.1007/978-3-030-02272-3, 2019, s.170.
[58] Norvig/Russell, s.831.
[59] Berk, s.113, 114.

özne”[60] olarak algılayamamaktadır. Bu durum, yapay zekânın bilinç sahibi olmadığını gösterir ki bilinçsiz oluşu yapay zekâ ile işleyen makineleri insandan ayıran temel özelliktir. Matematiksel formüllerden yola çıkan ve gerçek hayata dair verileri istatistikler halinde yorumlayan bir zekânın, toplumsal bağlamı ve bu bağlamda vardığı sonuçların neye tekabül ettiğini algılaması mümkün değildir. Dolayısıyla bu teknolojilerinin yaptıkları çıkarımlar ve bunlara nasıl ulaştıkları, özellikle insanları doğrudan etkileyen kararların alınması sırasında mutlaka kontrol edilmelidir. Ancak bugün varılan noktada, derin öğrenme ve benzeri yeni yöntemler, öğrenme sürecini insan zihninde olduğu gibi açıklanması zor bir aşamaya ulaştırmıştır. Bu yöntemlerde, basit bir hafıza deposu veya belirli bir yapay nöronu analiz ederek tüm sürecin nasıl gerçekleştiğini tespit etmek mümkün değildir. Bu durum varılan sonucun açıklanmasını ve dolayısıyla gerekçelendirilmesini engellemektedir. Bu nedenlerle, bizatihi kendisi diyalektik bir yöntem olan ve maddi gerçeğe nedenleriyle birlikte ulaşmaya çalışan ceza muhakemesinde yapay zekâ teknolojileri kullanılırken bu tartışmalar mutlaka gözetilmelidir.

[60] Yavuz Köroğlu, **Yapay Zeka'nın Teorik ve Pratik Sınırları**, Boğaziçi Üniversitesi Yayınevi: İstanbul, 2017, s.3, 4.

II. YAPAY ZEKÂ TEKNOLOJİLERİNİN CEZA MUHAKEMESİ ALANINDA KULLANILMASI

Yapay zekâ alanındaki gelişmelerin, sosyal medya, akıllı telefonlar ve dört bir koldan akan veri trafiği ile birleşmesi algoritmaların öğrenme sürecinde büyük bir evrimsel sıçrayış yaratmış, böylelikle yapay zekâ bilim, eğitim, çalışma hayatında olduğu kadar ceza hukuku alanında da kullanılır hale gelmiştir.

Ceza Hukuku alanında, bu sıçrayış sonucunda klasik ceza teorisinin yapay zekâya sahip varlıklara nasıl uygulanacağı ve cezai sorumluluğun yeni zeminleri tartışmaya açılmıştır. Ancak tartışma yalnızca maddi ceza hukuku ile sınırlı değildir. Tüm bu gelişmelerin ceza yargılaması ve daha da geniş bir perspektifle ceza adaletini etkileyen bir boyutu bulunmaktadır. Teknoloji ile ceza hukukunu buluşturmaya çalışan ve Budapeşte Sözleşmesi olarak tanınan Avrupa Konseyi Siber Suç Sözleşmesi bu gelişmelere karşılık vermede oldukça eksik kalmıştır[61].

Yapay zekâ sistemlerindeki gelişim ile öncelikle delil toplama yöntemleri kişisel haklara daha fazla müdahale içeren bir nitelik kazanmış, kolluk görevlileri "hackleme", veri madenciliği, profilleme pek çok yönteme başvurabilir hale gelmiştir. Bunun sonucu olarak toplanan delillerin niteliği de değişmiş, dijital deliller ve adli bilişim gittikçe önem kazanır hale gelmiştir.

Ceza muhakemesinin işlevinde asıl dönüm noktasını oluşturan, artık şüpheli veya sanığa karşı "gözü bağlı" şekilde yaklaşan ve yalnızca fiillerinden yola çıkarak değerlendirme yapan yargılama anlayışı yerine, pozitivistlerden bu güne miras kalan "failin tehlikeliliği" kavramının yeniden ağırlık kazanmasıdır. Klasik görüş üzerine inşa edilen ceza muhakemesi, kişinin yalnızca kendi fiilinden dolayı sorumlu olması ve aynı zamanda suç teşkil eden fiili ile arasında sübjektif bir bağın kurularak kusurluluğunun tespit edilmesine dayanır[62]. Oysa günümüzde, özellikle risk analizi yapan profilleme teknolojileri ile fiillerden yola çıkan ve faile eşit mesafede duran bir

[61] Serena Quattrocolo, **Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion**, Springer: Cham, Ağustos 2020, s.5.
[62] Vesile Sonay Daragenli, **Tehlike Suçları**, İstanbul Üniversitesi Kamu Hukuku Bölümü, Yüksek Lisans Tezi, 1998, s. 100.

sistemden, kişiler daha suç işlemeden onları tüm kişilik özellikleri, hayat tarzları ve "topluma uyumlulukları" üzerinden değerlendiren bir sisteme geçilmiştir. Bu teknolojiler ile kişiler, milyonlarca verinin istatistiksel şekilde analiz edildiği bir sistemde, "suç işleme riski" barındıran gruplar altında toplanarak kimi zaman suç işlemeden önce ceza muhakemesi çerçevesinde kalan yaptırımlara uğrayabilmektedir. Bir nevi kolektif sorumluluk ve suçluluk karinesine dayanan yeni devlet-vatandaş ilişkisinde, sosyo-ekonomik aidiyet, politik eğilim ve yaşam tarzından yola çıkarak oluşturulan "riskli kişi" listeleri gittikçe kabarmaktadır.

Topluma uyum sağlama yetisi olmadığı düşünülen failin "anormalliği" ile "tehlikeliliği" arasında ilişki kuran bu anlayış[63], fiilden değil "failin kişiliğinden" yola çıkarak onu toplum dışına itmektedir. Ceza muhakemesinin suça dair maddi gerçeğe ulaşma amacından saptırılması, adeta "riskli" kişilerle bir mücadele aracı olarak kullanılması, elbette uygulanacak tedbirlerin ve verilecek cezanın amacını da farklılaştırmaktadır. Bunun ilk etkisi, kişinin suç teşkil eden bir fiili işlemesi ve klasik anlamda başlangıç şüphesiyle başlayan soruşturma sürecinin, suç öncesi alana çekilmesidir. "Kişinin işlemeye niyet ettiği suçun sonuçları toplum bakımından çok ağırsa, cezalandırmak için suçun işlenmesi beklenmeli midir?"[64] retoriği, yalnız Türkiye'de değil, tüm dünyada toplumu ikna sürecine sızmıştır. Ancak bu süreçte yalnız ağır suçlarla sınırlı kalınmamış, pek çok suçta hazırlık hareketlerine ilişkin yaptırımlar öngörülmüştür. Ceza hukuku kurumlarını suç öncesi alanda seferber eden bu anlayış, faili işlediği bir fiilden dolayı sorumlu tutmayı, kefaret ödetmeyi ve ardından topluma yeniden kazandırmayı amaçlamamaktadır. Aksine "riskli" kişilerin toplumdan tecrit edilmesi ve böylelikle toplumun savunulması temel amaçtır. Bu durum "suçu önleme" şeklinde masum gözüken bir ifadeyle meşrulaştırılsa da aslında şüpheli olan-olmayan ayrımının kaldırıldığı, tüm vatandaşların her hareketinin ve dışa yansımayan düşüncelerinin teknoloji eliyle analiz ve kontrol edildiği yeni bir ceza muhakemesi sisteminin inşası söz konusudur[65].

---

[63] Somay Tümerkan, "Klasik, Pozitivist Okullarda Ve Toplumsal Savunma Hareketinde Ceza Sorumluluğunun Esası", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt:48, Sayı:1-4, 1983, ss. 51-71, s.55-57.

[64] Nuran Haydar, "Düşman Ceza Hukuku ve Uygulamaları", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Yıl: 2019, Cilt: 16, Sayı: 2, ss. 281 – 320, s. 283.

[65] Eckert, s. 13

Bu durum kolluk kuvvetlerinin faaliyetlerini de suçu bastırıcı faaliyetlerden, suçu "tahmin edici" faaliyetlere yöneltmiş, pek çok koldan gelen veriyi kullanan algoritmalar aracılığıyla suçun nerede ve kim tarafından işlendiğini öngören yazılımlar artık bir distopya olmaktan çıkarak gerçek hayatta kullanılır hale gelmiştir. Aşağıda ele alınacak olan ve Amerika'da Kaliforniya polisi tarafından kullanılan PredPol yazılımı ve bazı Avrupa ülkelerinde kullanılan Precobs yazılımı bu tür potansiyel suç mahallini ve faili tespit etmeye çalışan yapay zekâ teknolojilerine örnektir[66].

Bugün gelinen aşamada, veri toplayan, analiz eden ve potansiyel şüpheli profili çıkartan algoritmalar yalnızca kolluk kuvvetleri tarafından kullanılmamakta, Avrupa ve Amerika'da hâkim ve mahkeme kararları sırasında da risk analizi yapan yapay zekâ teknolojilerine başvurulmaktadır. Ayrıca bu teknolojilerin infaz aşamasında hükümlünün tabi olacağı rejimi belirlerken de sevk edildiği görülmektedir.

Risk analizi yapan profilleme teknolojileri, ceza muhakemesinin zeminini en derinden sarsan teknolojilerdir. Bunların ne şekilde kullanıldığının daha detaylı şekilde ele alınması, ceza muhakemesine etkilerini tespit edebilmek ve bir sonraki bölümde ele alınacak kişisel verilerin korunması hakkı bağlamında bu teknolojileri değerlendirebilmek için oldukça önemlidir. Her ne kadar tez kapsamı yalnız ceza muhakemesi süreciyle sınırlı tutulsa da kimi zaman önleyici amaçla yapılan analizlerin ceza muhakemesine de sirayet etmesi söz konusu olduğundan risk analizi teknolojileri aşağıdaki şekilde iki gruba ayrılarak incelenecektir:

- Suç işlenmesini önleme amacıyla suçun işleneceği zaman ve yeri tahmin etme, gelecekte suç işleme potansiyeli bulunduğu düşünülen kişileri belirleme amacıyla kullanılan yapay zekâ teknolojileri

- Suç işlendikten sonra ara ve nihai kararlarda kullanılmak üzere şüpheli ve sanığa dair risk analizi yapan yapay zekâ teknolojileri

[66] Katalin Ligeti/Fabio Giuffrida, "Artificial Intelligence and Criminal Justice", http://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf, Erişim Tarihi: 01.01.2021, s.7.

A. Suç İşlenmeden Önce Profilleme Teknolojilerinin Kullanılması ve Tahmine Dayalı Kolluk Faaliyetleri ("Predictive Policing")

Suç işlenmeden önceki alanda "etkin müdahale" gerekçesiyle kolluğun uyması gereken kurallar, ceza muhakemesi sürecine göre daha esnek tutulmuş, kişilerin temel hak ve özgürlükleri daha güvencesiz bırakılmıştır. Bu durum yapay zekâ teknolojilerinin uygulanması açısından boş bir alan bırakarak, müdahalelerin daha gözetimsiz yapılmasını mümkün kılmaktadır[67].

Failin tehlikeliliğinin ön plana çıktığı ve potansiyel şüphelilerin tayini açısından tüm teknolojik gelişmelerin deneysel denebilecek şekilde kullanıldığı bu alanda, artık kolluğun bastırıcı işlevi ve önleyici görevlerinden ziyade "tahmin etme" faaliyetlerinde bulunduğu görülmektedir. Bu tür teknolojileri ilk olarak seferber eden Anglosakson ülkelerinde kolluğun yürüttüğü algoritmik ve otomatik tahmine dayalı faaliyetler "Predictive Policing" adı ile ifade edilmektedir. Ancak bu kavram henüz Kıta Avrupası'nda ve Türkiye'de tam karşılığını bulamamıştır. Policing ifadesi Avrupa'da genel olarak gözetim şeklinde tercüme edilmekle birlikte aslında, istihbarat faaliyetlerini, önleyici kolluk faaliyetlerini, bunun yanı sıra soruşturma yürütme ve kovuşturma alanındaki tüm faaliyetleri kapsayan daha geniş bir anlama sahiptir[68]. Bu faaliyetler arasında "predictive policing" ile kast edilen ise kolluğun suç öncesi alanda veya suç işlendikten sonra özellikle veri analizine dayanan teknolojileri kullanarak, müdahale etmesi gereken bölgeleri ve kişileri tespit etmesini ifade eder. Kimi zaman geçmiş ve bugünkü izlerdeki benzerlikler, daha önce işlenmiş bir suçu aydınlatmak üzere tahminlerde bulunmayı da mümkün kılmaktadır. Bu faaliyetler, suçların temelde tesadüfi olmadığı, bu nedenle veriler ve izlerden yola çıkarak tespit edilen örüntülerle hem geçmişin hem geleceğin tahayyül edilebileceği iddiası üzerine inşa edilmiştir[69]. Türkiye'de ise bu tür faaliyetler için doktrinde "proaktif polislik"[70], "öngörüye dayalı kolluk"[71] terimlerinin kullanıldığı görülmektedir. Ancak bu ifadeler, kolluğun yeni

---

[67] Quattrocolo, s.38
[68] Ibid s.37.
[69] Mohammad A. Tayebi/Uwe Glässer, **Social Network Analysis in Predictive Policing: Concepts, Models and Methods**, Springer Yayınevi: Londra, Ekim 2016, s. 9.
[70] Turan Atlı, "Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 2, Sayı: 1, 2019, ss.4-22, s. 12.
[71] Nurettin Alkan/Yunus Emre Karamanoğlu, "Öngörüye Dayalı Kolluk Temelinde Önleyici Kolluk: Rusya Federasyonu'ndan Örnekler", **Güvenlik Bilimleri Dergisi**, Kasım 2020, Cilt:9, Sayı:2, s.388-412, s. 388.

faaliyetlerini, geleneksel anlamda önleyici görevleri ile ayırt etmede yetersiz kalmaktadır. Teknoloji ile kolluk faaliyetlerinin iç içe geçtiği predictive policing modelini asıl ayırt eden husus, hem geçmiş hem gelecekteki suçları veri madenciliğine dayalı istatistiksel tahminler yoluyla çözmek için analitik tekniklerin kullanılmasıdır. Bu nedenle tez kapsamında "tahmine dayalı kolluk faaliyetleri" ifadesi tercih edilecektir. Bu başlık altında incelenecek olan ise tahmine dayalı kolluk faaliyetlerinin suç işlenmeden önceki alanda nasıl kullanıldığıdır.

Suçla mücadelenin konusu suç işlenmeden önce tehlike barındıran faaliyetleri tespit etmektir. Ancak yapay zekâ teknolojilerinin bu süreçte itici gücü, kolluk kuvvetlerine daha az çaba ve kaynak ile tüm vatandaşları kategorize etme, takip etme ve potansiyel şüphelileri tespit etme imkânı tanımasıdır. Bu şekilde risk analizi yapan teknolojiler ile henüz bir fiil ile tehlike dışarı vurulmadan, kişilere müdahale etmek ve gelecekte yol açacakları riskleri bugünden engelleyebilmek amaçlanır. Nitekim sınırsız veri toplama ve saklamanın mümkün olması ile artık yalnızca suç işlemiş kişilerin kayıtları değil tüm vatandaşların ikametgâhı, aile bilgileri, eğilimleri, görüştükleri çevreler ve yaşam şekilleri hakkında istihbarat edinmek mümkün olmuştur. Artık kolluğun öncelikli görevi, suç işlendikten sonra soruşturma yürütmek, faili tespit etmek ve delillerin ortadan kaldırılmasını önlemek değil, evleviyetle kamu düzenine aykırı hareketlerin doğmasını engellemek şeklinde tanımlanmıştır. Ancak söz konusu teknolojiler kullanılırken bunlar ile ulaşılmak istenen amaç daha mühimdir. Toplum içerisinde farklılıklar ve eşitsizlikler tespit edilerek sosyal devlet kurumlarının sevk edilmesi amacı bu teknolojilerin kullanılmasına farklı bir yön verebilir. Ancak bunun yerine bu eşitsizliklerin suçu doğurduğu ve bunun yalnızca kolluk eliyle alınan bastırıcı ve önleyici tedbirlerle engellenebileceği iddiası, doğru ve bilimsel olduğuna inanılan teknolojiler aracılığıyla geçmişteki ayrımcı ve tek tipçi uygulamaları tekrar etmeye yol açacaktır[72].

Suçu önleme amaçlı kullanılan yapay zekâ teknolojileri incelendiğinde, ilk olarak geliştirilen PredPoL, Hunchlab gibi yazılımların amacının suçun nerede ve ne zaman işleneceğinin haritasını çıkarmak olduğu görülmektedir. Bölge risk analizi veya "tehlikeli alan analizi" olarak adlandırılan bu modeller, kişilere değil coğrafi bölgelere

[72] Andrew Ashworth, Andrew/Lucia Zedner, **Preventive Justice**, Oxford University Press: Oxford, Nisan 2015, s.49-50.

yoğunlaşmaktadır. Bu modeller bir bölgede daha önce hangi tip suçların ne zaman işlendiği gibi görünürde objektif olan verileri dikkate almaktadır[73]. İlkin Anglosakson ülkelerinde başvurulan bu uygulamalar, hızla Kıta Avrupası'nda da yaygınlaşmıştır. Örneğin İtalya'nın Trento şehrindeki E-güvenlik sistemi, polise gelen suç ihbarlarını, bir bölgede yeniden mağdur olma oranını, bölgede sokak aydınlatması, MOBESE sistemi bulunması gibi değişken koşulları ve yaşayanların güvende hissetmesi gibi sübjektif verileri de hesaba katarak kolluk faaliyetlerine yön vermek üzere kullanılmıştır[74]. Almanya ve İsviçre'nin çeşitli bölgelerinde kullanılan Precobs yazılımı ise hırsızlık, ateşli yaralama gibi kimi suçların zaman ve mekân açısından suç mahalline yakın yerlerde yeniden işleneceği varsayımına dayanmakta[75], ayrıca suçun işlenme zamanı ve şekli, yine hangi tür eşyaların çalındığı gibi verilere dayalı analizler yaparak suçun yeniden işleneceği yeri öngörmeye çalışmaktadır[76].

Bu tür yazılımlarda, geliştirilen algoritmalara hangi verilerin sunulacağı belirlenirken kriminolojik teorilerden yola çıkılmaktadır. Bu teorilere örnek olarak suç mahalline dönüş teorisi ("near repeat theory") ve kırık camlar teorisi ("broken windows theory") verilebilir[77]. Bunlardan ilki hırsızlık ve silahlı yaralama gibi belli suç tipleri açısından failin aynı bölgeye yeniden suç işlemek üzere döndüğü varsayımına dayanmaktadır. Bunun nedeni bölgedeki güvenlik zafiyeti veya mağdurların kırılganlığı sebebiyle suç işlemenin kolay olduğu algısının oluşmasıdır. Bu teori Precobs yazılımına da ilham vermiş ve mükerrer suç işlenen yerler, yapılan modellemede önemli bir veri kaynağı olarak ele alınmıştır[78]. Kırık camlar teorisi ise**,** sosyal düzensizliğin suçun oluşmasında önemli etkisi olduğunu ileri sürmekte ve adını bilinçli olarak dikiz aynası ve anteni kırık şekilde park edilmiş bir arabanın terk edildiği bir sosyal deneyden almaktadır. Bu aracın terk edildiği mahallede insanlar önce araca zarar vermeye başlamış, ardından aracın çevresinde işlenen kabahatler

---

[73] O'Neil, s.85.

[74] Andrea di Nikola/Serena Bressan, **E-Security and the New Horizon of Urban Security, An Information System for Police Forces and Local Administrations**, http://www.esecurity.trento.it/report/eCrime-eSecurity-Guidelines.pdf, Erişim Tarihi: 01.01.2021, s.7-10.

[75] Lukas Staffler/Oliver Jany, "Künstliche Intelligenz und Strafrechtspflege: Eine Orientierung", **Zeitschrift für Internationale Strafrechtsdogmatik**, Sayı:4, 2020, s.164-177, s. 168.

[76] Sylvia Lundschien, "Predictive Policing: Wie Algorithmen bei der Verbrechensbekämpfung Helfen",14.01.2021, https://www.goethe.de/prj/jad/de/the/ari/22082332.html, Erişim Tarihi: 01.07.2021.

[77] Tayebi/Glässer, s.116.

[78] Staffler/Jany, s. 167.

gittikçe yayılmıştır. Dolayısıyla sahipsiz araçlar, terk edilmiş mallar, toplanmamış çöpler, aydınlatılmayan sokaklar, suçun daha rahat işlenebileceği bir düzensizlik ve sahipsizlik ortamı doğurmaktadır[79]. Bu nedenle bu tür unsurlar suç işlenecek yeri ve zamanı tespit etmeye çalışan risk profilleme yazılımları oluşturulurken dikkate alınmaktadır.

Her ne kadar bu tür yazılımların dayandığı geçmişte işlenen suç sayısı ve aydınlatma, günün saati gibi faktörler objektif veriler gibi görünse de bu verilerin tamamen tarafsız olduğunu iddia etmek imkânsızdır. Öncelikle bu sistemler, zaten kolluğun geçmişten bugüne özellikle yoğunlaştığı mahallelerden topladığı verilere dayanmaktadır. Zaten sıklıkla kolluk müdahalesi altında olan mahallelerden yola çıkan profilleme teknolojileri kuşkusuz ki ilgili bölgeleri kırmızı bölge ilan etmekte ve bunun sonucu olarak bu bölgeye daha çok devriye aracı gönderilmektedir. Bu durum bölgede çok daha fazla kişinin ve aracın durdurulmasına, arama ve gözaltı tedbirlerinin çok daha sık uygulanmasına yol açmaktadır. Uygulanan tedbir sayısı, negatif bir veri olarak sisteme işlenmekte, sonuç olarak bölgenin risk oranı daha da yüksek gözükmektedir. Bu durum kendi kendini sürekli doğrulayan bir kısır döngü yaratmaktadır. Öte yandan, "nezih semtler" ve beyaz yaka suçları karanlık sayılar olarak kalmakta ve belli bölgeler aldatıcı şekilde risksiz bölge olarak gözükerek kolluk müdahalesi ile hiç karşılaşmamaktadır. Amerika özelinde, bu tür uygulamalar Hispanik ve siyahi kökenlilerin oturduğu mahallelere sürekli devriye polisinin sevk edilmesi ile sonuçlanmış[80], kolluğun yoksul mahallelerde sıfır tolerans politikası renk ve sınıf körü olduğu iddia edilen bu algoritmalar aracılığıyla meşrulaşmıştır.

Suç öncesi alanda uygulanan ve ayrımcılığı daha da körükleyen asıl tehlikeli model ise gelecekte suçun kim tarafından işleneceğini tespit etme iddiasındaki yazılımlardır. Bu tür yapay zekâ uygulamalarına örnek olarak İtalya'da Milano Polisi tarafından kullanılan ve soygunların "aynı tip" insanlar tarafından işlendiği varsayımına dayanan KeyCrime yazılımı verilebilir. Belli kişilerin veya grupların suça daha eğilimli olduğu iddiasındaki bu yazılımlar, yaş, cinsiyet, posta kodu, kişi hakkında polis veya istihbarat veri tabanında bulunan kayıtlar gibi çeşitli verilerden

[79] Hakan İnankul, "Suçun Önlenmesinde Polisin Rolü", **Turkish Studies**, Cilt:11, Sayı:2, 2016, ss.567-582, s.572, 573.
[80] O'Neil, s.85, 86.

beslenmektedir. Şikago örneğinde benzer yazılımlara dayanarak oluşturulan "tehlikeli kişiler" listesine giren kişiler, kolluk tarafından uyarı mektubu almakta, herhangi bir suç işledikleri takdirde karışılacakları yaptırımlar kendilerine hatırlatılmaktadır[81]. Söz konusu uygulamalar, kişilerin kimi zaman kredi almasını, işe alınmasını[82] kimi zaman seyahat etmesini engellemekte[83], idari yaptırımlarla karşılaşmalarına yol açmakta, hatta kişiler hakkında soruşturma açılması için başlangıç şüphesi teşkil edebilmektedir.

Bu yazılımlar ile riskli gruplar listesinde olduğu belirlenen kişiler açısından bir nevi suçluluk karinesi oluşmakta, tehlikeli olmadığını kanıtlama yükü bu kişilere yüklenmektedir. Ancak hükümetler ve güvenlik birimleri, bu tür "kara listelere" girme kriterlerini ve bu listeler oluşturulurken hangi verilerin ne şekilde işlendiğini açıkça paylaşmamaktadır. Bu nedenle hatalı veri girişini düzeltmek mümkün olmadığı gibi varılan sonuçlara anlamlı bir itiraz hakkından bahsetmek de mümkün olmamaktadır[84].

Hükümetlerin günümüzde suçu önleme amacıyla profilleme teknolojilerini sevk ederken, suçun nedenlerini ortadan kaldırmak yerine "tehlikeli kişileri tespit etme" ve korunan hukuksal değerlere yönelik bir zarar ve tehlike oluşmaksızın özgürlükleri kısıtlama yolunu seçtiğini söylemek mümkündür[85].

---

[81] Orla Lynskey, "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection From Predictive Policing", **International Journal of Law in Context**, Sayı:15, 2019, s.162-176, s. 167, 168.

[82] Bu duruma örnek olarak Amerika'da işe alımlarda başvurulan E-Verify sistemi verilebilir. Bu sistem, kişi hakkında tüm verileri birleştirmekte, işe alımının yasal olarak mümkün olup olmadığına karar vermektedir. Ancak dayanılan verilerde en ufak hata, kişilerin iş görüşmesine davet edilmeden elenmesine yol açmaktadır, bkz. Juliet P. Stumpf, "Getting to Work: Why Nobody Cares About e-verify (and Why They Should)", **UC Irvine Law Review**, Cilt:2, Sayı 1, 2012, ss 381-414, s.388, 389.

[83] Örneğin NSA ve FBI arasında hukuka uygunluğu tartışmalı şekilde paylaşılan veriler ve CAPPS II (Computer Assisted Passenger Pre-screening System) isimli sisteme dayanılarak oluşturulan "Uçuş Yasağı Listesi" seyahat özgürlüğüne doğrudan müdahale teşkil etmektedir, ayrıntı için bkz. Justin Florence, "Making the No Fly List Fly: Due Process Model for Terrorist Watchlists", **Yale Law Journal**, Cilt:115, Sayı: 8, 2006, ss. 2148-2182, s. 2156.

[84]Margaret Hu, "Big Data Blacklisting", **Florida Law Review**, Cilt: 67, Sayı:5, 2016, ss. 1735-1809, s.1759, 1760.

[85] Ashworth/Zedner, s.10.

B. Soruşturma ve Kovuşturma Aşamalarında Yapay Zekâ Teknolojilerinin Kullanımı

Yukarıdaki bölümde tartışılan tahmin odaklı kolluk faaliyetleri, kitlesel olmaları ve suç tipine göre ayrıma gitmeksizin sınırsızca uygulanmaları nedeniyle klasik anlamda önleyici kolluk faaliyetleri kapsamındaki düzenlemelerin dışına taşmaktadır. Benzer faaliyetlerin soruşturma sırasında yürütülmesi de kuşkusuz ki Ceza Muhakemesi sistematiği ile çatışmaktadır.

Ceza Hukukunun sınırları, son yıllarda zarar yerine hukuksal değere yönelik tehlikeleri de içerecek şekilde gittikçe genişlemiştir. Tehlikeden daha da soyut olan risk kavramı ise bu sınırların daha kontrolsüzce genişlemesine ve bulanıklaşmasına yol açmaktadır. Nitekim failin geçmişi, sosyal yaşamı, etnik kökeni ve ekonomik durumuna dayanarak geleceğini tahmine yönelen risk kavramı, failin iç dünyası ve dışa yansıyan fiilleri arasında yapılan ayrımı ortadan kaldırmaktadır. Artık failin fiilinin bir hukuksal değeri ne ölçüde ihlal ettiği ile ilgilenilmemekte, failin kamu düzenini ne ölçüde ihlale hazırlıklı olduğunu tespit edilmeye çalışılmaktadır[86]. Bu belirsiz amaç, kişileri sınırsızca hedef haline getirmeyi mümkün kılmış, "objektif ve bilimsel" teknolojiler kolluk tedbirleri ve hâkim kararlarına yeni bir "meşru" zemini hazırlamıştır.

Soruşturma ve kovuşturma sırasında risk analizi yapan profilleme teknolojilerinde kullanılan veriler aşağıda ele alınacaktır. Ancak genel bir değerlendirmeyle bunlar tarafından hedeflenen kişinin yaşı, doğduğu yer, milliyeti, aile bilgileri gibi veriler, kişinin seçme ve değiştirme ihtimali olmayan verilerdir. Bu verilerin doğrudan veya dolaylı şekilde risk analizine konu edilmesi kişinin adeta kendisi olmaktan ötürü cezalandırılması anlamına gelmektedir. Medeni durum, iş koşulları, alkol ve benzeri bağımlılıkları gösteren veriler ise statik veriler değildir. Bu veriler adeta değişme ihtimalleri yokmuşçasına risk gruplarını indirgemeci ve dondurulmuş bir şekilde çizmektedir[87].

---

[86] Barış Erman, "Ceza Hukukunun Dönüşümü", Yeditepe Üniversitesi Hukuk Fakültesi, Cilt:9, Sayı:2, 2012, ss.447-480, s. 451.
[87] Ashworth/ Zedner, s. 124.

1. Soruşturma Aşamasında Yapay Zekâ Teknolojilerinin Kullanımı

Günümüzde yapay zekâ teknolojileri yalnızca suç öncesi alanda değil, soruşturma sürecinde de kullanılmaktadır. Ancak bu yöntemlerin kişisel haklara müdahale oranı çok daha fazla olup söz konusu teknolojiler özellikle özel hayatın ve kişisel verilerin korunması bakımından ağır ihlal potansiyeli barındırmaktadır[88]. Bugün risk analizi yapan profilleme teknolojileri özel hayatın çekirdek alanını tamamen göz ardı etmekte, artık ev içerisi dahi nesnelerin interneti ile sınırsız bir veri toplama alanı haline evrilmektedir. Dolayısıyla klasik anlamda arama, el koyma gibi tedbirlerine başvurmadan veriye ulaşabilmek mümkün hale gelmiştir. Bilgisayarda arama gibi özel düzenlemeler, pek çok ülkede kolluk görevlilerinin kullandığı casus yazılımlara ve Truva atlarına karşı yeterli koruma sağlamamakta, kişilerin internetteki tüm hareketlerini, mikrofon ve kamera karşısındaki görüntülerini takip etmek mümkün hale gelmektedir[89]. Dolayısıyla belirli kişi hakkında koruma tedbirleri sevk edilerek delil elde edilmesi, yerini herkes hakkında sınırsız veriye erişime bırakmıştır. Bu durum genellemeler üzerine kurulu "suçlu profilleri"nin inşasını mümkün kılmaktadır.

Bu profilleme teknolojilerinden çok azı suç teşkil eden fiiller üzerine yoğunlaşmaktadır. Bunlardan biri olan G.I.A.N.O.S Avrupa'da çeşitli bankalar tarafından kullanılmakta, örneğin 15 000 Euro'dan fazla miktarda para transferlerinde, banka müşterisinin tüm hesap hareketlerini, bu hareketlerin gerekçesini ve sıklığını takip ederek "anomali" tespit etmekte, böylelikle kara para aklama ile mücadele edilmeye çalışılmaktadır. Benzer şekilde işleyen MENTAS ve NORCOM yazılımları, kara para aklamanın yanı sıra dolandırıcılık suçunun tespitinde de kullanılmakta, ancak işlevli olmak adına müşterilerle ilgili tüm veri tabanlarını seferber ederek kişisel veri toplamaktadır[90].

Bunun yanı sıra sosyal bağlantı analizi algoritmaları, internet üzerinden toplanan veriler arasında karar ağaçları veya yapay sinir ağları aracılığıyla bağlantı kurmakta, bu yazılımlar özellikle örgütlü suçlarda birbiriyle bağlantılı kişileri tespit edebilmek adına kullanılmaktadır. Böylelikle kolluk kuvvetleri tarafından kişilerin örgüt bağı ve

---

[88] Quattrocolo, s.41
[89] Marco Torre, **Il Captatore Informatico: Nuove Tecnologie Investigative e Rispetto delle Regole Processuali**, Guiffre Editore: Milano, Haziran 2017, s. 13-18.
[90] Qauttrocolo, s. 65.

örgüt içerisindeki konumları tespit edilmeye çalışılmaktadır. Bu algoritmalar email içeriği, internette paylaşılan içerikler gibi pek çok veriye erişerek, farklı sosyal platformlardan edinilen verileri birbirine bağlamaktadır[91].

Failin suç işleme ve itiyadı suçlu olma ihtimalini değerlendiren, böylelikle kimi zaman hakkında soruşturma açılması veya aleyhine karar alınmasına yol açan Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) ise "belli bir gruba aidiyeti"[92] tespit etmek üzere kullanılmaktadır. COMPAS ilk bölümde ele alınan kara kutu şeklinde çalışan uygulamalara örnektir. Hangi verileri ne şekilde kullandığı, vardığı sonuca nasıl ulaştığı açıkça belirlenememektedir. Kuşkusuz ki bu durum kişisel verilerin korunması hakkı kadar, masumiyet karinesi, savunma hakkı ve daha genel anlamıyla adil yargılanma hakkı açısından da pek çok sorun teşkil etmektedir.

2. Ara Karar ve Hükümlerde Yapay Zekâ Teknolojilerinin Kullanımı

Karşılaştırmalı hukukta, ceza muhakemesi sürecinde hâkim ve mahkemeler tarafından verilen ara ve nihai kararlarda çeşitli profilleme teknolojilerine başvurulduğu görülmektedir. Mevcut muhakeme sisteminde, "sanığın kişilik özellikleri ile duruşmadaki tutum ve davranışları göz önünde bulundurularak yeniden suç işlemeyeceği hususunda kanaate varılması", "kaçma şüphesi", "delilleri karartma şüphesi" gibi unsurların değerlendirilmesi, aslında bir nevi hâkim tarafından yürütülen bir risk analizidir.

Bununla birlikte hâkim ara ve nihai karar verirken somut olayın koşullarını ve mevcut delilleri incelemeli, bunları mantık süzgecinden geçirerek kendi vicdanına göre değerlendirmelidir. Hâkimin sübjektif algısı, "objektif gerçeklik" olan delillerden yola çıkmaktadır. Yine hâkimin vardığı neticenin yalnızca varsayım ya da tahminlere değil, somut şekilde fiil ve fail arasındaki ilişkiye dayandığını kanıtlayan gerekçe

[91] Hossein Hassani/Hu Huang/ Emmanuel Silva/Mansi Ghodsi, "A Review of Data Mining Applications in Crime", **Statistical Analyses and Data Mining**, Cilt:9, Sayı:3, ss.139-154, s.145, 146.
[92] Liu Han-Wei/Lin Ching-Fu/Chen Yu-Jie, "Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability", **International Journal of Law and Information Technology**, Cilt:27, Sayı: 2, 2019, ss. 122-141, s.130.

gösterme zorunluluğu bulunmaktadır[93]. Dolayısıyla hâkim yalnızca yazılı kuralları olaya uygulamamakta, ayrıca sınırları çizilmiş bir akıl yürütme faaliyeti gerçekleştirmektedir[94]. Profilleme teknolojileri ise somut bir davada işlendiği iddia edilen fiili göstermekten ziyade, kişilere ait geçmiş verilerden yola çıkar ve "risk" teşkil eden belirli nitelikleri istatistiksel olarak tespit ederek gruplandırırlar. Bu tespiti neden sonuç ilişkisinde gerekçelendirmez, yalnızca matematiksel olasılıklar üzerinden ilerlerler.

Ara kararlarda kullanılan bu tür risk analiz teknolojilerine örnek olarak Kamu Güvenliği Değerlendirme Yazılımı şeklinde ifade edilen PSA gösterilebilir. Bir milyon beş yüz bin örnek dava verisi ile geliştirilmiş PSA günümüzde Amerika'nın üç eyaletinde kullanılmakta, sanığın yaş ve sabıka kaydı verilerinden yola çıkarak hakkında tehlike puanı öngörmekte, bu yolla hâkimlerin kişinin tutuklanması veya serbest bırakılması yönündeki kararlarına yol gösterici olmaktadır[95]. Hem suç öncesi hem suç işlendikten sonra yaygın şekilde kullanılan COMPAS yazılımı ise yalnız sabıka geçmişini değil, kişinin ailevi durumu, ekonomik koşulları, eğitim durumu, hayat tarzı, topluma bakışı, boş zamanlarını nasıl geçirdiği, özel hayatı, sosyal çevresine ilişkin verilere dayanarak çıkarımlarda bulunmakta ve tekrar suç işleme potansiyelini puanlarla değerlendirmektedir[96]. Yine Static-99 adlı uygulama Amerika ve Avrupa'da cinsel suçluların tekrar suç işleme riskini değerlendirmek üzere şüphelilerin yaşı, uzun süreli ilişkileri olup olmadığı, daha önce cinsel suç işleyip işlemediği, en son suç işlediği tarih, suçu tanıdık bir kişiye karşı mı yoksa bir yabancıya karşıya mı işlediği gibi kriterleri dikkate almaktadır[97].

---

[93] Veli Özer Özbek, "Ceza Muhakemesinde Hâkimin Vicdani Kanaati", **Hukuk Felsefesi ve Sosyoloji Arkivi,** Cilt:16, 2007, ss.282-287, s. 286-286.

[94] Balkan M. Demirdal, "Ceza Hâkiminin Vicdani Kanaati Üzerine Bir Değerlendirme", **Çankaya Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:5, Sayı:1,2020, ss. 1021-1042, s.1026.

[95] Danielle Kehl/Guo Priscilla/Samuel Kessler, **Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing**, Responsive Communities Initiative, Berkman Klein Center for Internet and Society, Harvard Law School, 2017, https://dash.harvard.edu/handle/1/33746041, Erişim Tarihi: 03.01.2020, s.10.

[96] Staffler/ Jany, s.172, Eleftherios Chelioudakis, "Risk Assessment Tools in Criminal Justice: Is There a Need for Such Tools in Europe and Would Their Use Comply with European Data Protection Law?", **Australian National University Journal of Law and Technology**, Cilt: 2, Sayı:1, Eylül 2020, ss.72-96, s.89

[97] Martin Rettenberger/Reinhard Eher,"Die deutsche Übersetzung des Static 99 zur aktuarischen Kriminalprognose verurteilter Sexualstraftäter Monatsschrift für Kriminologie und Strafrechtsreform", **Monatsschrift für Kriminologie und Strafrechtsreform**, Cilt: 89, Sayı: 5, Ekim 2006, ss.352-365, s.356, 357.

Bu tür yapay zekâ teknolojilerinin öğrenme sürecinde, farklı davalardan ve veri tabanlarından yola çıkarak öncelikle "benzer özellikler gösteren fail profili" çıkartılır. Ardından bu profille benzerlikler gösteren kimseler aynı grup altına toplanır ve bunlar için ortak bir tehlike puanı öngörülür. Bu durum ceza sorumluluğunun şahsiliği, cezanın bireyselleştirilmesi gibi yerleşik ilkelerin uygulanmaması, belli kişilerin otomatik olarak belirlenen bir gruba aidiyeti nedeniyle cezalandırılması anlamına gelmektedir[98].

Diğer bir sorun ise, bu yazılımları üreten firmaların tehlikelilik sonucuna varırken hangi verilere ağırlık verildiğini "fikri mülkiyet hakları" çerçevesinde paylaşmamasıdır[99]. Oysa ceza muhakemesinde ithamın ve kararların şeffaflığı, adil yargılanma açısından vazgeçilmezdir. Fikri mülkiyet gerekçesiyle sürecin paylaşılmaması, ilgili verilere ve yazılım modeline itiraz ve dolayısıyla savunma hakkının kullanımına engel teşkil etmektedir. Bir nevi "gizli bilirkişi"[100] haline gelen bu yazılımların esas alınarak karar verilmesi halinde, adil yargılanma hakkı ihlal edilmiş olacaktır.

Nitekim bu nedenle, COMPAS yazılımının kullanımını konu alan State v. Loomis davasında, mahkeme, tutuklamaya ilişkin kararlarda veya cezanın tayininde salt bu tür yazılımların vardığı sonuçlara dayanılmaması gerektiğini vurgulamıştır. Failin gelecekte suç işleyip işlemeyeceğine ilişkin risk değerlendirmesi yapan yazılımlar, ex ante şekilde suç teşkil eden fiili değerlendirme amacına hizmet etmemektedir[101].

Adalet, vicdan, eşitlik gibi ceza muhakemesinin merkezinde bulunan değerler formüle indirgenemez ve dolayısıyla matematiksel olarak aktarılamaz kavramlardır. Buna rağmen bugün en azından Avrupa'da belli tür davalarda yapay zekânın hâkimlerin yerini almaya başladığı pilot uygulamaların varlığından bahsetmek

---

[98] Leah Wisser, "Pandora's Algorithmic Black Box: The Challenges of Using Algorithmic Risk Assessments in Sentencing", **American Criminal Law Review**, Cilt:56, Sayı:4, 2019, ss. 1811-1832, s.1815.

[99] Fikri mülkiyet haklarının şeffaflık hakkına etkileri üzerine bkz. Sandra Wachter/Brendt Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", **Columbia Business Law Review**, Cilt:2019, Sayı: 2, ss. 494-620, s. 604 vd.

[100] Wisser, s. 1824.

[101] State v. Loomis.14 881 N.W.2d 749 (Wis. 2016), https://www.courts.ca.gov/documents/BTB24-2L-3.pdf, para 93-97, Erişim Tarihi: 03.03.2021.

mümkündür. Örneğin Estonya'da 7000 Euro'nun altındaki hukuki tazminat talepleri için akıllı algoritmaların karar alması uygulaması yakın zamanda kullanılmaya başlanılacaktır[102]. Yine benzer şekilde, Avrupa İnsan Hakları Mahkemesi'nin ("AİHM") HUDOC veri tabanından yola çıkarak öğrenen yazılımlar, şu an ortalama %79 oranda doğruluk payı ile Mahkemenin bir olay karşısında nasıl karar vereceğini tahmin etmekte, gerekçeli kararları taklit edebilmektedir[103]. Bu örnekler gelecekte yapay zekâ uygulamaları tarafından doğrudan hüküm kurmasına ilişkin denemelerin çoğalacağını göstermektedir. Ancak hukuk mahkemeleri ve ikincil nitelikte yargı organı olan AİHM'ye nazaran, ceza hukukunun kendine has ilkeleri ve prensipleri göze alındığında, henüz yapay zekâ teknolojileri açısından gelinen noktada bu teknolojilerin hüküm kurmada esas alınmasının mümkün olmadığı anlaşılmaktadır.

Özet olarak profilleme teknolojilerinin ceza muhakemesinde kullanılması, belirli risk gruplarını ceza muhakemesinin konusu haline getirmiştir. Bu risk grupları kişinin değiştirmesi mümkün olmayan ailesi, milliyeti, dini, bunun yanı sıra arkadaş seçimi, zevkleri gibi verilerden yola çıkmakta[104], bu veriler üzerine anti sosyal veya riskli kişi grupları oluşturmaktadır. Bu durum ceza muhakemesini suçu aydınlatma ve faili tespit etme ödevinden uzaklaştırarak adeta "normatif insan yaratma" hususunda bir araç haline getirmektedir. Her ne kadar bu yazılımların oluşturulmasında kriminolojik teoriler dikkate alınsa da profilleme teknolojilerinde hangi verilerin hangi oranlarda dikkate alındığı, bilimsel teorilere sadık kalınıp kalınmadığı ve varılan sonuçların temelleri mahkemelerle fikri mülkiyet hakları veya "kara kutu" modellerindeki teknik imkânsızlıklar nedeniyle paylaşılmamaktadır. Bu durum hem kişisel verilerin korunması hem ceza muhakemesi ilkeleri açısından pek çok hakkı aşındırmaktadır. Bir sonraki bölümde, kişisel verileri koruma mevzuatlarında bu tür profilleme teknolojileri açısından sınırlar öngören düzenlemeler ele alınacak, ceza muhakemesi sürecinde bunlardan ne şekilde yararlanılabileceği üzerinde durulacaktır.

---

[102] Der Standard, "Estland will Richter durch Künstliche Intelligenz Ersetzen", 3 Nisan 2019, https://www.derstandard.at/story/2000100613536/justiz-estland-will-richter-durch-kuenstliche-intelligenz-ersetzen, Erişim Tarihi: 03.03.2021.

[103] Nikolaos Aletras/Dimitrios Tsarapatsanis/Daniel Preoţiuc-Pietro/Vasileios Lampos, "Predicting Judicial Decisions of the European Court of Human Rights: a Natural Language Processing Perspective", **PeerJ Computer Science**, 2016, https://doi.org/10.7717/peerj-cs.93, s.2.

[104] Böhm, s. 151.

III. KİŞİSEL VERİLERİN KORUNMASI MEVZUATI KAPSAMINDA PROFİLLEME TEKNOLOJİLERİ

Kişisel verilerin korunması, mahremiyet hakkı, özel hayatın gizliliği, kişisel bütünlüğün korunması gibi pek çok kavramla birlikte anılmakta[105], bununla birlikte, bu kavramlardan sıyrılan yeni ve önemli bir alanı kapsamaktadır.

Tarihsel olarak kişisel verilerin korunması hakkı, çoğunlukla özel hayatın gizliliği hakkı içerisinde ele alınmıştır. Nitekim Türkiye Anayasası başta olmak üzere pek çok ülkede ilkin kişisel verilerin korunması hakkının özel hayatın gizliliği ile birlikte ele alındığı görülmektedir. Ancak bu hakkın ayrı bir hak olarak kanunlara yansıması 1970'li yılları bulmuştur[106]. Ana hatlarıyla, kişilerin toplumdan, sosyal yargılardan, devlet kurumlarından ve çoğunluğun baskısından koruyan bir kalkan olan özel hayatın gizliliği, kişilere özerk bir alan tesis etmeyi amaçlamaktadır. "Yalnız bırakılma hakkı" olarak da nitelendirilen bu hak ile kişilerin devlet ve çoğunluktan ayrılarak bağımsız bir birey olarak kişiliğini tesis etmesi amacıyla bir nevi görünmezlik ve dokunulmazlık kazanması sağlanmıştır[107]. Nitekim konutun ve aile yaşamının dokunulmazlığı da bu önemli kalkanın bir parçasıdır. Bu bağlamda, kişinin özel yaşamının gizliliği, demokratik anayasal devletin temelini oluşturan değerlerden biri olup, bireylere farklı olma, farklı düşünme, ilişkilerini istediği biçimde şekillendirme, serbestçe kişiliğini oluşturma[108] ve kendisinden beklenen rollerden sıyrılmak için gizli ve özel bir alan tesis etmektedir. Avrupa İnsan Hakları Mahkemesi de geleneksel olarak kararlarında özel hayatın gizliliğini "kişilik hakkı" ile birlikte ele almakta, bu bağlantı ile birlikte özel hayatın gizliliğini, kişiliğe ve kimliğine sahip çıkma, otosansüre başvurmak zorunda kalmama, otomatik karar alma mekanizmaları ve özellikle profilleme sonucu kendi tercihlerini belirleme otonomisini yitirmeme ve kendisi hakkında toplanan bilgilere dayanılarak yapılan çıkarımları kontrol edebilmeyi kapsayacak şekilde ele almıştır[109].

---

[105] Kama Işık, Sezen, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış**, On İki Levha Yayıncılık: İstanbul, Ocak 2020, s. 55.
[106] Işık, s.58.
[107] Güçlü Akyürek, **Özel Hayatın Gizliliğini İhlal Suçu**, Seçkin Yayıncılık: Ankara, Ocak 2014, ss. 29, 32.
[108] Paul de Hert/Serge Gurtwith,"Privacy, Data Protection and Law Enforcement: Opacity of the individual and Transparency of Power", İçinde: **Privacy and Criminal Law**, Ed: Erik Claes, Antony Duff, Serge Gutwirth), Intersentia: Antwerpen, 2007, ss.61-104, s.72
[109] Wachter/Mittelstadt, s.512.

Bununla birlikte gelişen teknoloji ile yalnızca belirli kişilerin hayatına müdahale içeren bilgi ve veri toplama, yerini sınırsız sayıda kişinin hayatına sürekli müdahale içeren büyük veriye bırakmıştır. Bu durum, verilerinin ne şekilde toplandığı ve kullanıldığından habersiz bireyleri veri işleme sürecinin dışına itmiştir. Kişiler kimi zaman başka bireyler, kimi zaman ise şirketler ve devletler tarafından toplanan verileri üzerindeki hâkimiyetlerini yitirmişlerdir. Sürecin görünmez bir şekilde işlemesi, bireylerin kendi verilerinin işlenme şekline dair itiraz etme haklarını da ellerinden almış, bu görünmez müdahale sürecinde zarara uğradıklarını iddia etmeleri imkânsız hale gelmiştir[110]. Bu durum, salt özel alanının gizliliğinin tesisi ile korunamayacak bir boyuta ulaşmıştır. Özel hayatın korunması, kişilere görünmezlik sağlarken, veriler üzerinde gerçek anlamda bir koruma sağlanması için kişisel verilerin "şeffaflık" içeren normlarla korunması ve sürecin görünür hale gelmesi gerekmektedir. Nitekim bu nedenle, ayrıca kişisel verileri koruyan bağımsız düzenlemeler doğmuş, kişilere işaret eden verilerin ne şekilde işlenebileceği kanun eliyle düzenlenmiştir. Böylelikle, veri sahibinin bu süreci takip edebilmesi sağlanarak, gizlilikten ziyade şeffaflık tesis edilmiştir. Ancak kişisel verilerin korunması hakkı, özel hayatın gizliliğine nazaran çok daha fazla aktörün uzlaşmasını gerektiren pragmatik bir yapıya sahiptir[111]. Kişisel verilerin korunması dikkate alınırken, kişilerin mahremiyetinin korunması kadar, toplumda kamu düzeninin sağlanması, haber ve bilgi akışının devamlılığı, ticari hayatın gereklilikleri gibi farklı nedenlerle özel şirketlerin, kamu kurum ve kuruluşlarının, güvenlik örgütlerinin, medya kurumlarının ve daha pek çok aktörün uzlaştırılması gerekmektedir. Bir uzlaşmanın sonucu olarak ortaya çıkan kanunlar, kural olarak veri işlenmesini yasaklamaktan ziyade veri işleme sürecini düzenleyen ve sınırlayan normları içermektedir. Bu normlar, veri işleyişinin hukuki zeminini sağlamak, aynı zamanda bu işleyiş sırasında vatandaşların iddia ve itirazlarını mümkün kılmak, böylelikle kişilerin verilerini tayin hakkı kadar, "hesap verebilirlik" ve "güvenilirliği" tesis etmeyi amaçlamaktadır. Böylelikle, "bırakınız yapsınlar" anlayışı yerine, şirketlerin ve hükümetlerin, bireylerin özerkliği, onuru ve mahremiyetlerine saygılı şekilde veri işlemesi amaçlanmıştır.

---

[110] Bart van der Sloot, "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data' ", **Utrecht Journal of International and European Law**, Cilt: 31, Sayıt: 80, 2015, s.25-50, s.46.

[111] De Hert/ Gutwirth, s.77.

Dolayısıyla kişisel verilerin korunmasına ilişkin normlar, özel hayatın gizliliğine gerçekleştirilen müdahalenin sınırlarını çizen normlardan farklı bir koruma alanı tesis etmektedir[112]. Nitekim veri işlemenin hukukiliği, kişilerin haklarında toplanan verilere erişim ve itiraz hakları, bu verilerin düzeltilmesini veya silinmesini talep etme hakları gibi pek çok husus, diğer kanunlar kapsamında korunmamaktadır[113]. Yine verilerin düzenli kontrolünü sağlayan veya vatandaşlar adına veri işleme süreçlerinin hukukiliğini denetleyen Kişisel Verileri Koruma Kurulları ancak özel verileri koruma kanunları ile birlikte gündeme gelmiştir.

Günümüzde büyük veri ve bu verinin analizini mümkün kılan algoritmaların kullanılması, kuşkusuz ki hem özel sektörde hem kamu sektöründe karar alma sürecini dönüşüme uğratmıştır. Artık belirli bir kişinin verilerinin tek bir tüzel kişi tarafından toplanması söz konusu değildir, aksine bu veriler zaman içerisinde sürekli hareket etmekte, farklı veri tabanları ve kişiler arasında el değiştirmektedir. Bu durum kişinin verilerinden yola çıkarak hakkında bir kimlik yaratılmasına yol açmakta, ancak ilgili kişiler hakkında "peşin hükümler" verirken onlara söz hakkı tanımamaktadır. Kuşkusuz ki devletlerin ve şirketlerin elindeki bu imkân, kişilerin "sıfırdan başlama", "fişlenmeden kendi kimliğini oluşturma" hakkını da elinden almaktadır[114].

Bu bağlamıyla verilerin çift fonksiyonu bulunmaktadır. Artık kitlesel şekilde toplanan veriler belirli bir kişi hakkında bilgi verirken, genel olarak toplum ve toplumu oluşturan belli bir grubun resmini de çizmektedir. Öte yandan belli bir profil altında toplanan kişileri, bu gruba dair yöneltilen reklamlar, öneriler, kimi zaman gruba yönelik tedbirler ile sınırlayarak bu kişilerin, kendi geleceklerini serbestçe ve etki altında kalmadan oluşturma olanaklarını ellerinden almaktadır[115]. Bu nedenle verilerin işleniş şeklinin hukuki bir zemine çekilmesi, insan onuru ve özerkliğini zedelemeyecek şekilde saklanması ve sürecin görünür ve denetlenebilir olması büyük önem taşımaktadır. Bu bağlamda kişisel verilerin korunmasına ilişkin normlar, yürütmenin meşruiyeti için bir zorunluluk haline gelmiştir. Bu haklar aracılığıyla insan

---

[112] Bu yönde bkz. Pınar Memiş Kartal, "Özel Hayatın Gizliliği Kapsamında Kişisel Verilerin Korunmasının Sınırları", Sanal Dünya'da Adalet, Tebliğ, **9. Uluslararası Suç ve Ceza Film Festivali**, 27.11.2019, https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=9uscff-teblig.pdf, Erişim Tarihi: 10.02.2021.

[113] De Hert/ Gutwirth, s.81.

[114] Wachter/Mittelstadt, s.513.

[115] Andreas Busch/Yana Breindl/Tobias Jakobi, **Netzpolitik: Ein einführender Überblick**, Springer: Weisbaden, Ekim 2019, s.50.

haklarını gözeten bir veri işleyişi tesis edilmektedir. Özellikle kolluk ve ceza muhakemesi sürecinde kişisel verilerin korunması, muhakeme taraflarının kişilik haklarının koruma altına alınmasını temin etmektedir. Adalete güven ve kamu otoriteleri ile vatandaşın arasındaki ilişkinin güçlendirilmesi açısından, görünürlük ve hesap verilebilirlik sağlayan bu normların varlığı elzemdir. Bu nedenle muhakeme sürecinde kişisel verilere ilişkin normlar bir kısıtlama değil, hukuk devletinin ve kişisel hakların güvencesi olarak görülmelidir[116].

Günümüzde şirketlerin ve hükümetlerin çok farklı veri kaynaklarından sınırsızca beslenebilmesi ile kişisel verilerin korunması açısından farklı bir döneme girilmiştir. Yalnız sınırsız veri toplanması ile değil, aynı zamanda bu verilerin yapay zekâ içeren algoritmalar tarafından ilişkilendirilmesi ile hak ve özgürlüklere müdahale alanı genişlemiştir. Nitekim yukarıda bahsedildiği üzere kişiler hakkında farklı veri tabanları arası bağlantı kurularak çizilen profiller, çağımızda otomatikleşmiş bir gözetim toplumunu mümkün kılmaktadır. Bu bağlamda, profilleme teknolojileri kişisel veriler ile ceza muhakemesi arasında bir bağ kurmakta, ceza muhakemesinin işleyişinde adil yargılanma, susma hakkı, aleyhe delil göstermeye zorlanmama hakkı gibi temel pek çok ilkenin etrafından dolaşılmasına izin vermektedir. Bunun yanı sıra, eski usul delil toplama modelleri üzerinden tahayyül edilmiş koruma tedbirleri, vatandaş-devlet arasında alt üst olan bilgi hâkimiyeti dengesini yeniden tesis etmek için yeterli olamamaktadır. Nitekim kişiler suç yoluna girmese dahi haklarında hazırlanmış olan bu profillere ilişkin bilgi edinememekte, dolayısıyla hatalı ya da haksız çıkarımlara karşı haklarını arayamamaktadırlar[117]. Kimi zaman ayrımcılık yasağı ihlali teşkil eden uygulamalar, otomatik karar alma mekanizmalarıyla meşrulaştırılarak, kapalı kapılar ardında kalmakta, teknoloji eliyle üstü örtülen bu süreç sonucunda pek çok ülkede kişiler idari ve cezai yaptırıma uğramaktadır.

Profilleme teknolojilerinin insan haklarına müdahale boyutunun artması ile öncelikle Avrupa Birliği ülkelerinde kişisel verileri koruyan düzenlemeler yapılmıştır. Profilleme algoritmalarının kimi zaman verileri bağlamından kopardığı, internette

---

[116] Thomas Marquenie, "The Police and Criminal Justice Authorities Directive: Data protection standards and Impact on the Legal Framework", **Computer, Law and Security Review**, Cilt: 33, 2017, ss. 324 – 340,s 327, 328.

[117] Serge Gutwirth/Mireille Hildebrandt, "Some Caveats on Profiling", İçinde: **Data Protection in a Profiled World**, Ed. Serge Gutwirth/Yves Poullet/Paul de Hert, Springer: Dordrecht, Ağustos 2010, s. 31-41, s. 34.

gerçekleştirilen basit bir aramanın, evdeki akıllı cihazlara takılan konuşmanın bir bölümünün veya sosyal medyadaki bir beğeninin bile potansiyel şüpheli hedef listesine düşmeye yol açtığı günümüzde[118], yapay zekâ teknolojilerinin topladıkları verileri değerlendirme kapasitesinin, hâlâ insan muhakemesi seviyesine ulaşmadığı görülmektedir. Bu nedenle profilleme teknolojilerinin şeffaf şekilde ve herkes tarafından anlaşılabilir hale getirilmesi kadar, bu teknolojilerle varılan sonuçların insan eliyle denetlenmesi, bu düzenlenmelerin odak noktasındadır.

Bugün kabarık veri tabanları içerisinde eriyen insan, en fazla mahremiyete sahip olduğu evi içerisinde bile, telefonu, akıllı televizyonu, interneti ve bilgisayarı ile takip edilebilir konumdadır. Mahrem ve dokunulmaz alan olan ev içinin dönüştüğü ve herkese açılabilen alan olarak evrildiği günümüzde[119], kişisel verileri koruyan kanunlar, kişileri görmedikleri, nasıl ve ne amaçla veri topladıklarını bilmedikleri veri işleyen kurumlara ve idareye karşı koruyarak yeni duvarlar örmeye çalışmaktadır. Ancak makine öğrenmesinin kazandığı hız ile verilerin ne şekilde işlendiği ve profillendiğine dair bilgi edinme oldukça güçleşmiş, toplanan verilerin el değiştirmesi ve kimi zaman kolaylıkla idare ve adli birimler tarafından erişilebilmesi, kimi zaman veri koruma mevzuatının amaçladığı korumanın işlevsiz kalmasına yol açmıştır.

Bu nedenle aşağıda öncelikle hangi verilerin kişisel veri sayılması gerektiği ve özellikle gelişen profilleme teknolojileri karşısında ceza muhakemesi süreci ile de ilişkilendirilebilecek veri işleme sürecine ilişin ilke ve haklar ele alınacaktır. Bu değerlendirmeler yapılırken öncelikle Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR"), ardından yine Avrupa Birliği çerçevesinde ceza muhakemesi sürecinde veri toplanması ile doğrudan ilişkili olan 2016/680 sayılı Gerçek Kişilere Ait Kişisel Verilerin Yetkili Merciler Tarafından Adli Suçların Önlenmesi, Araştırılması, Tespit Edilmesi veya Kovuşturulması ya da Mahkûmiyetlerin İnfazı Amacıyla İşlenmesi ve Bu Verilerin Serbest Dolaşımı Hakkında, 2008/977/JHA Çerçeve Kararını İlga Eden Direktif ("2016/680 sayılı Direktif")[120] ele alınacaktır. Ardından Türk mevzuatı

[118] Poullet, Yves, "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?", İçinde: **Data Protection in a Profiled World**, Ed: Serge Gutwirth/Yves Poullet/Paul de Hert, Springer: Dordrecht, Ağustos 2010, s.3-30, s.7.
[119] Yves, s.8.
[120] Direktifin orijinal adı Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data,

değerlendirilerek, Kişisel Verilerin Korunması Kanunu'ndaki profillemeye ilişkin hak ve yükümlülükler karşılaştırmalı şekilde incelenecektir. Bu bölümde yapılan incelemeler, profilleme teknolojilerinin kullanımı sırasında uyulması gereken kuralların tespiti açısından büyük önem taşımaktadır. Nitekim bu düzenlemelere aykırı şekilde veri işlendiği ve profilleme yapıldığı takdirde, bu durum ceza muhakemesi sürecine de yansıyacaktır. Bu tartışma son bölümde ceza muhakemesinde profilleme teknolojileri ile varılan sonuçların, hukuka uygun delil olarak kabul edilip edilemeyeceği hususunda yeniden ele alınacaktır.

A. Avrupa Birliği Kişisel Verilerin Korunması Mevzuatında Profilleme Teknolojilerine İlişkin Düzenlemeler

1. Giriş

Tarihin hiçbir döneminde olmadığı kadar fazla kişisel verinin işlendiği, özel sektörün ve hükümetlerin büyük veri analizlerini büyük bir iştahla kullanmak istediği günümüzde teknolojik gelişmeler veri üretimini ve saklanmasını oldukça kolaylaştırmıştır. Bu durum Facebook, Google başta olmak üzere pek çok firmanın hizmet ücreti yerine veri ticareti üzerinden zenginleşmesini sağlarken, kişiler, verilerinin kimlerin elinde ne şekilde işlendiği, el değiştirdiği ve analiz edildiğinin kontrolünü yitiren, nesneleştirilen ürünler haline gelmiştir. Avrupa'da teknolojik gelişmeler karşısında kişisel verileri korumaya yönelik ilk atılım 1970'li yılların ortasında, Avrupa Konseyi Bakanlar Komitesi tarafından elektronik veri tabanlarında işlenen kişisel bilgilerine ilişkin (73)/22 sayılı[121] ve (74)/22 sayılı[122] ilke kararları ile gerçekleştirmiştir. Bu kararlardan ilkinde özel sektör, ikincisinde ise kamu sektöründe kişisel bilgilerin elektronik veri tabanlarına işlenme sürecine ilişkin düzenlemelerin gerekliliği ve bu düzenlemelerde dikkat edilmesi gereken ilkelerin altı çizilmiştir. Nitekim kişisel verilerin korunmasına ilişkin yasal düzenleme hazırlığına zaten başlamış Avusturya, Danimarka, Fransa, Almanya, Norveç gibi bir kısım üye

---

and Repealing Council Framework Decision 2008/977/JHA; bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680, Erişim Tarihi: 10.02.2021.

[121] Council of Europe, **Committee of Ministers Resolution N (73) 22 on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks In The Private Sector**, 26 Eylül 1973, https://rm.coe.int/1680502830, Erişim Tarihi: 10.02.2021.

[122] Council of Europe Committee of Ministers, **Resolution (74) 29 on the Protection of The Privacy of Individuals Vis-A-Vis Electronic Data Banks In The Public Sector**, 20 Eylül 1974, https://rm.coe.int/16804d1c51, Erişim Tarihi: 10.02.2021.

devletlerde, bu kararların yayınlanmasını izleyen beş yıl içerisinde kişisel verileri koruyan kanunlar yürürlüğe konulmuştur[123].

Bununla birlikte ilke kararının ardından üye devletlerin yürürlüğe koyduğu yerel mevzuatlar, kişisel verilerin korunmasına ilişkin farklı standartlar öngörmüş ve bu durum Avrupa Birliği pazarında ülkeler arası kişisel verilerin aktarımında engel teşkil etmeye başlamıştır. Bu farklılığın giderilmesi için, 1990 senesinde Avrupa Birliği Direktifi hazırlanması teklif edilmiş ve beş yıl süren hazırlığın ardından kişisel verilerin korunmasına ilişkin ilk AB düzenlemesi olan 95/46/EC sayılı Direktif kabul edilmiştir[124].

1995 yılından bugüne teknolojik gelişmeler ve bu gelişmelerin veri işlenmesine yansıması Direktif'te karşılığını bulamamıştır. Nitekim ilgili Direktif'in yürürlüğe girdiği sırada, AB nüfusunun yalnızca yüzde biri internet kullanmakta, hatta Google gibi pek çok firma henüz çevrimiçi hizmet dahi sunmamaktaydı[125]. Bu nedenle kişisel verilerin günün şartlarına uyarlanması ve daha iyi korunması amacıyla yeni bir hukuki alt yapı oluşturulmaya çalışılmıştır. Bu dönemde Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinde düzenlenen kişisel verilerin korunması hakkı, 2009'da Lizbon Antlaşması ile birlikte tüm üye devletlerce tanınması gereken bir hak haline gelmiş, yine Avrupa Birliği'nin İşleyişine İlişkin Antlaşma'nın 16. maddesi, Avrupa Parlamentosu ve Konseyi'ne kişisel verilerin işlenmesine ilişkin kuralları düzenleme yükümlülüğü getirmiştir[126]. Böylelikle kişisel verilerin korunması bağımsız bir hak olarak düzenlenmekle kalmamış, ayrıca bu hakka ilişkin yeterli korumanın sağlanması zorunlu hale gelmiştir.

Bu gelişmelerin ardından, 1995 tarihli Direktifi düzenleme ve güncelleştirme çalışmalarına 2009 yılında başlanılmış ve AB Konseyi, Parlamentosu ve Avrupa Veri Koruma Denetçisi dâhil farklı aktörlerin katıldığı süreç 2016 yılında düzenlenen ve

---

[123] Hatta aynı dönemde Portekiz, Avusturya ve İspanya'da kişisel verilerin korunması anayasal bir hak olarak koruma altına alınmıştır, bkz. Council of Europe, **Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, European Treaty Series Sayı: 108, https://rm.coe.int/16800ca434, Erişim Tarihi: 10.02.2021.

[124]Berna Akçalı Gür, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:25, Sayı:2, Prof. Dr. Ferit Hakan Baykal Armağanı, Aralık 2019, ss. 850-872, s.857, 858.

[125] Orla Lynskey, **The Foundations of EU Data Protection Law**, Oxford University Press: Oxford, Kasım 2015, s.4

[126] Akçalı Gür, s.858.

2018 yılında yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR") ile tamamlanmıştır. Kişisel verilerin korunmasında 1995 tarihli Direktif'in yerini almak üzere tüzüğün tercih edilmesi, tüzüklerin, AB kurumlarını, tüm üye devletleri ve bu devletlerin vatandaşlarını bağlayıcı, doğrudan uygulanır nitelikleri göz önüne alındığında, yeknesak bir uygulama sağlaması nedeniyle oldukça önemli bir adım olmuştur[127].

Kişisel verileri koruyan rejimleri bugün tüm sektörlere uygulanan, tek bir kaynakta toplanmış rejimler veya farklı sektörlere uyarlanmış dağınık düzenlemeler şeklinde ikiye ayırmak mümkündür. GDPR düzenlemesini diğer düzenlemelerden ayıran, devletlere iç güvenlik rejimi ve kamu düzeni tesisi gibi hususlarda belirli takdir yetkisi tanımakla birlikte, tüm alanlara, kurumlara ve kişilere uygulanabilecek bütüncül bir düzenleme teşkil etmesidir. Bu bağlamda Avrupa Konseyi tarafından imzaya açılan ve AB devletleri dışında da taraf olan pek çok devletin bulunduğu, kişisel veriler alanındaki en önemli uluslararası sözleşme olan 1981 tarihli Kişisel Verilerin Otomatik İşleme Tutulması Karşısında Bireylerin Korunması Sözleşmesi de vurgulanmalıdır[128]. AB çerçevesinde, kişisel verilerin korunmasına ilişkin kamu-özel sektör ayrımı yapmadan ortak bir düzenleme yapma geleneğinin izleri, GDPR yürürlüğe girmeden yıllar önce bu Sözleşme çerçevesinde de kendini göstermiştir.

Pek çok teknoloji şirketinin merkezi olan Amerika Birleşik Devletleri'nde ise, kişisel verilerin korunması rejimi GDPR sistemi ile oldukça farklılık göstermektedir. Bu rejimde ilk göze çarpan 1974 yılında yürürlüğe giren "Özel Hayatın Gizliliği Kanunu" olup[129], bu Kanun kapsayıcı ismine rağmen yalnızca federal kurumların kişisel veri işlemesi kapsamında hak ve yükümlülükler öngörmektedir. Bununla birlikte ilgili düzenleme kamu sektöründe veri işlenmesine ilişkin en kapsamlı kanunlardan birini teşkil etmektedir. Ancak kamu sektöründe kişisel verilerin korunmasına ilişkin düzenlemeler her federal devletin sınırları içerisinde değişkenlik göstermektedir. Özel sektör açısından ise kişisel verilerin korunma rejimi daha da

---

[127] Paul de Hert/Vagelis Papakonstantinou, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", **Computer Law and Security Review**, Cilt:28, Sayı: 2, Nisan 2012, ss. 130-142, s.131, 132

[128] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, ETS:108, T. 28.01.1981, Türkçe metin için bkz:https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf, Erişim Tarihi:11.01.2021.

[129] Kanunun orijinal adı için bkz. Privacy Act of 1974, 5 U.S.C. § 552a.

karmaşıktır; nitekim şirketlerin kanunlardan ziyade, ad hoc yapılar ve piyasanın "görünmez eli" ile düzenlendiği görülmektedir[130]. Bu çok katmanlı sistemde yeknesak bir korumanın tesisinden bahsetmek mümkün değildir. Bu anlamda, Amerikan sisteminde, GDPR düzenlemesine en yakın düzenleme, yalnızca Kaliforniya Eyaleti'nde geçerli olan ve 2018 yılında düzenlenen Kaliforniya Tüketici Gizliliği Yasası[131]'dır. Bu yasa, tüketicilere hakkında toplanan kişisel bilgilerle ilgili bilgi edinme, kişisel verilerin silinmesini talep etme ve kişisel bilgilerin üçüncü kişilere satılmasını engelleme gibi haklar tanımakla birlikte, bu hakları yalnızca "tüketici"lere tanımış ve yasanın uygulanma alanı "25 milyon dolardan fazla gelir elde eden şirketler, gelirinin yüzde ellisinden fazlasını tüketicilerin bilgilerini satmaktan elde eden şirketler veya her yıl en az 50 000 tüketicinin kişisel bilgilerini satın alan, satan veya paylaşan şirketler" ile sınırlanmıştır[132].

GDPR, yukarıda tartışıldığı üzere Amerikan sisteminden farklı olarak Avrupa'da sektör ayrımı ve ülke ayrımı yapmaksızın veri işlenmesine ilişkin doğrudan uygulanabilir tek tip bir rejim sistemi öngörmüştür. Bununla birlikte, ilgili düzenleme üye devletlere belli hakları sınırlama hususunda takdir yetkisi tanıyan istisnai maddeler de barındırmaktadır. Örneğin 85. madde "gazetecilik amaçları veya akademik, sanatsal veya edebi anlatım amacıyla gerçekleştirilen işleme faaliyeti açısından, kişisel verilerin korunması hakkı ile ifade ve bilgi edinme özgürlüğünü bağdaştırma amacıyla gerekli olması durumunda" üye devletlerin ilgili maddede sayılan haklardan muafiyet veya derogasyonu mümkün kılınmıştır. Ceza muhakemesi sürecinde veya suç işlenmeden önce veri işlenmesine ilişkin dikkat çekilmesi gereken diğer bir madde ise 23. madde olup, ilgili maddede temel haklar ve özgürlüklerin özüne dokunmaksızın, demokratik bir toplumun gereklerine uygun ve orantılı bir şekilde, maddede sayılan hakların milli güvenlik; savunma ve kamu güvenliği; suçu önleme, soruşturma, suçu tespit ve yargılama veya cezayı infaz etme gibi amaçlarla veya kamu güvenliğine yönelik tehditlere karşı veri işlenmesi hallerinde sınırlanabileceği belirtilmiştir. Daha da önemlisi, GDPR m. 2/2 (b) bendi ile sığınma,

---

[130] Lynskey, The Foundations of EU Data Protection Law, s.17.

[131] SB-1121 California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121, Erişim Tarihi: 25.01.2021.

[132] Greta Carlson/Jonathan McKinney/Elizabeth Slezak/Esther Wilmot, "General Data Protection Regulation and California Consumer Privacy Act: Background", **Journal of International Economic Law**, Cilt:24, Sayı: 1, 2020, ss. 62-69, s.67.

göç, polis ve adli mercilerin suçla mücadelede işbirliği gibi alanlarda veri işleme sürecini ve 2/2(d) bendi, aşağıda daha detaylı tartışılacağı üzere suçu önleme, soruşturma, tespit ve ceza infazında yetkili otoritelerce işlenen verileri kapsam dışında bırakmıştır[133]. Bu bağlamda GDPR'ın kapsayıcı olma ve sektörlere göre ayrım gözetmeme iddiası, belirli maddelerle zayıflatılmış, açıkta bırakılan kolluk, adli merciler ve suçla mücadele ve yargılama sürecinde yetkili otoritelerin veri toplamasına ilişkin süreç ise 2016/680 sayılı Direktif ile düzenlenmiştir. Suçla mücadele ve kamu düzeninin tesisinde her ülkenin kendi şartlarını gözeterek yerel düzenlemeler yapabilmesi amacıyla getirilen bu ayrı düzenleme, GDPR'a benzer haklar tanısa da suçla mücadele ve yargılama sürecinin sekteye uğramadan tamamlanabilmesi için kimi kısıtlamalar içermektedir.

Aşağıda önce hangi verilerin kişisel veri kabul edileceği ve kişisel veriler mevzuatlarında koruma altına alınacağı tartışılacak, ardından GDPR ve 2016/680 sayılı Direktif'in uygulama alanları ayırt edilerek, her iki düzenleme açısından da profilleme teknolojilerine karşı öngörülen hak ve yükümlülükler değerlendirilecektir.

2. Kişisel Veri Kavramı ve Kişisel Veriler Koruma Mevzuatı Kapsamında Değerlendirilen Veriler

Kişisel veri kavramı GDPR ve 2016/680 sayılı Direktif düzenlemesinin maddi olarak uygulanma alanını teşkil etmektedir. İlgili mevzuatlar kapsamındaki hak ve yükümlülükler, yalnızca bir veri, kişisel veri olarak tanımlandığı takdirde uygulanacaktır. Her iki mevzuat açısından da kişisel veri kavramı paralel olduğundan, bu kavram genel bir düzenleme olan GDPR üzerinden ele alınacak, ardından sırasıyla GDPR ve 2016/680 sayılı Direktif kapsamında profilleme teknolojilerine ilişkin haklar değerlendirilecektir.

Kişisel veri kavramını, kimliği belirli ya da belirlenebilir gerçek bir kişiye ilişkin her türlü enformasyon[134] olarak tanımlamak mümkündür. Dolayısıyla tüzel kişilere ilişkin enformasyon bu kapsamda değerlendirilemeyecektir. Gerçek kişiye ilişkin

[133] Lynskey, Criminal Justice Profiling, s.164, 165.
[134] "Enformasyon" kavramının tercih edilme nedeni aşağıda "enformasyon içerme unsuru" tartışılırken ele alınacaktır.

enformasyon, yalnızca kişinin kimliğini doğrudan tespit etmeyi mümkün kılan kimlik numarası gibi bilgileri içermemektedir; dolaylı olarak kişiyi tespit etmeyi mümkün kılan konum bilgisi, fiziksel, ruhsal, ekonomik, kültürel durumuna ilişkin bilgiler de kişisel veri kapsamındadır. Kişinin dolaylı olarak dahi tespitinin mümkün olmadığı durumlarda ise anonim veri söz konusu olacak ve bu tür bilgiler GDPR kapsamında korunmayacaktır[135].

GDPR 29. maddesine göre kurulmuş, veri koruması ile ilgili bir danışma kurulu olan "29. Madde Çalışma Grubu", kişisel veri kavramını dört unsura ayırarak açıklamaktadır. Buna göre kişisel veri kavramından bahsetmek için öncelikle bir enformasyon söz konusu olmalı, bu enformasyon gerçek bir kişiye ilişkin olmalı ve kişiyi belirli ya da belirlenebilir kılmalıdır[136]. Ancak günümüz teknolojileri karşısında bu unsurlardan özellikle belirlenebilir olma ve enformasyon kavramları dönüşüme uğramış, bu durum belki de amaçlananın çok ötesinde verinin, kişisel veri kavramı içerisinde eritilmesine yol açmıştır. Bu nedenle aşağıda özellikle tartışmalı olan kişiyi belirleme veya belirlenebilir kılma unsuru ve enformasyon kavramı, bugünün koşulları altında detaylı şekilde ele alınacaktır.

a) Belirli veya Belirlenebilir Gerçek Kişiye İlişkin Olma Unsuru

Gerçek bir kişiyi belirli kılan bir enformasyon, onun doğrudan tespitini ve bir gruptan ayrı olarak teşhis edilmesini mümkün kılar. Bu bağlamda kişinin ismi ve soy ismi, aynı ismi taşıyan başka kişilerin de bulunması halinde ilgili kişinin doğrudan tespitine elverişli değildir. Ancak GDPR, kişinin doğrudan belirlenmesinin mümkün olmadığı, başka verilerle birleştirildiğinde dolaylı olarak tespit edilebildiği durumlarda da uygulanmaktadır. Önemli olan bu verilerin tek başına kişiyi doğrudan tespit etmesi değil, birleştirildiklerinde kişiyi belirlemeyi mümkün kılmasıdır. Ancak bu durumda "belirlenebilir" kavramı oldukça geniş şekilde ele alınmış olacaktır. Nitekim 26. gerekçe maddesine göre, tespit etme sürecinin maliyeti, alacağı zaman ve teknolojik gelişmelerin sunduğu imkânlar ışığında, veri sorumlusu veya başka bir kişi tarafından

[135] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law", **Law, Innovation and Technology**, Cilt:10, Sayı: 1, 2018, ss. 40-81, s.43.
[136] Article 29 Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf, Erişim Tarihi: 16.02.2021.

makul kabul edilebilecek bir çabayla kişinin belirlenmesi mümkün ise, bu durumda ilgili veri belirlenebilir kabul edilecek ve GDPR kapsamında değerlendirilecektir[137]. Bu durum kişisel veri kavramını belirlerken, somut olayın koşullarına göre değerlendirme yapılmasını gerektirmekte, bu yönüyle kavramı göreceli kılmaktadır. Örneğin bugünün teknolojileriyle kişinin tespiti mümkün değilken, yeni bir gelişme aynı veriyi kişinin kimliğini belirlemeye elverişli kılabilir ve GDPR kapsamında değerlendirilmesini gerektirebilir. Bununla birlikte, veri sorumlusunun neyi amaçladığı da önemlidir. Çalışma Grubu, eğer kullanılan teknoloji, kimlik ifşasını amaçlayan bir teknolojiyse, veri sorumlularının ellerinde çok az enformasyon bulunduğu ve çok nadir durumlarda bu teknolojilerin kişilerin tespiti için kullanıldığı gibi iddialarının GDPR uygulamasının dışına çıkmak için yeterli olmayacağını belirtmektedir. Bu hususta önemli bir örnek MOBESE sistemleridir. Her ne kadar günlük hayatta kamera önünden geçen çoğu kişinin kimlik tespiti yapılmasa da bu teknolojinin amacı, gerektiğinde kişileri belirlemek olduğundan kaydedilen her veri, GDPR kapsamında kabul edilmelidir[138].

Bu konuda önemli diğer bir örnek ise Avrupa Adalet Divanı önüne gelen Breyer davasıdır[139]. Bu davada kişilerin sabit veya değişken IP adreslerinin kişisel veri olarak ele alınıp alınmayacağını değerlendirilmiştir. Davada esas soru, veri sorumlusunun elindeki verilerle kişiyi tespit edemediği ancak üçüncü kişinin işlediği verilerle birleştirdiğinde, kişi hakkında belirlenebilir enformasyon edinebildiği durumlarda kişisel veriden söz edilip edilemeyeceğidir. Ayrıca hangi koşulların "makul kabul edilebilecek bir çabayla" kimliği tespit etmeyi mümkün kıldığı hususunda somut bir tartışma yürütülmüştür. Olay özelinde, internet servis sağlayıcının IP adresini kayıt altına alması halinde, kişinin tespitinin mümkün olmadığı, dolayısıyla verinin "anonim olduğu" iddiası değerlendirilmiştir. Olayda IP adresine ilişkin verinin, üçüncü bir kişi olan erişim sağlayıcı elindeki verilerle birleştirilmesi halinde kişiyi tespit mümkün hale getirmesi hukuki tartışmayı doğurmuştur. Nitekim IP adresleri, işlendiği sırada hangi bilgisayardan ilgili internet sitesine erişildiğini göstermekle birlikte, doğrudan bilgisayarın sahibini ya da o sırada kimin bilgisayarı kullandığını tespiti mümkün

[137] Bkz. Recital 26 GDPR, https://www.privacy-regulation.eu/en/recital-26-GDPR.htm, Erişim Tarihi:11.02.2021,
[138] Bkz. Article 29 Working Party, s. 15, 16.
[139] Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland,19.10. 2016, ECLI:EU:C:2016:779, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582, Erişim Tarihi: 11.02.2021.

kılmamaktadır[140]. Ancak üçüncü kişi elindeki verilere erişim makul çaba ile mümkünse, bu tespitin yapılması mümkün hale gelmektedir. Mahkeme, belirlenebilirlik unsurunu değerlendirirken, tespiti yapmaya elverişli tüm verilerin tek kişinin elinde olması gerekmediğinin altını çizmektedir[141]. Bu durumda, bu verilerin hayatın olağan akışında orantılı ve makul bir çaba içerisinde talep edilmesi ve ardından kişinin tespiti mümkün ise kişisel veri olarak kabul edilmesi gerektiğini belirtmekte ve bu hususa örnek olarak ceza soruşturması amacıyla erişim sağlayıcılardan bilgi talep edilmesini öngören kanuni düzenlemelerin bulunması halinde, makul bir çabayla verilere erişilebileceğini belirtmektedir. Yine paralel bir yorumla, internet servis ve erişim sağlayıcılardan bilgi edinilmesini yasaklayan normlar bulunması halinde üçüncü kişilerden de veri toplanarak kişinin kimliğinin belirlenmesi oldukça güç olacak ve bu durumda kişisel verinin "belirlenebilirlik" unsuru karşılanmayacaktır[142].

Bu bağlamda günümüz teknolojileri dikkate alındığında, pek çok veri tabanından beslenen enformasyonun tek bir veri sorumlusu tarafından dahi birleştirilmesi mümkün hale gelmiştir. Örneğin internet sitelerince kullanılan çerezler ve benzeri uygulamalar tek başına cihazı kullanan kişiyi belirlemeyebilmektedir[143]. Diğer bir örnek olan "akıllı şehir" projeleri kapsamında, konum, yüz, görüşülen kişiler, sosyal ve politik faaliyetler gibi pek çok detaylı verinin eş zamanlı toplanması, kişinin belirlenebilmesini oldukça kolaylaştırmıştır. Bu durum geçmişte anonim kabul edilebilecek pek çok enformasyonun bugün kişisel veri olarak korunmasını gerektirmektedir. Henüz 2000 yılında, posta kodu, doğum tarihi ve cinsiyet bilgileri tek başına Amerikan halkının yüzde seksen yedisinin tespit edilmesini mümkün kılmıştır. Yine internet film veri tabanları, 2008 yılında 500 000 Netflix üyesinin tespit edilmesini sağlamıştır. 2013 yılına gelindiğinde ise Bradley Cooper ve Olivia Munn gibi ünlülerin, yalnızca kamusal anonim veri tabanı üzerinden yola çıkarak yorumlanan verileri ile dahi hangi mekânları ziyaret ettikleri ve taksi sürücülerine bahşiş verip vermedikleri belirlenmiştir. 2014 yılında kart sahiplerinin alışveriş yaptıkları yere ilişkin veriler, dört alışverişin sonunda anonim kabul edilen verilerin

---

140 İbid, para.38.
141 İbid, para. 43.
142 Frederik Zuiderveen Borgesius, "The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition", **European Data Protection Law Review**, Cilt:3, Sayı:1, 2017, ss. 130-137, s. 133, 135.
143 Borgesius, s. 136.

yüzde doksanın yeniden belirlenebilir kılınması için yeterli olmuştur [144]. Tüm bu teknolojik gelişmeler, belirlenebilir veri kavramını geniş yorumlamayı gerektirmekte, nitekim Adalet Divanı da bu tür bir yorumu destekleyen kararlar vermektedir. Bu nedenle veri işleyenler ve veri sorumluları, salt kendi işledikleri verinin ilgili kişiyi belirlemeyi mümkün kılmadığını belirterek veri haklarının tesisine ilişkin yükümlülüklerinden kaçınamayacaktır. Nitekim işledikleri verilerin, makul şartlar altında kendileri veya üçüncü kişiler tarafından başka verilerle birleştirildiğinde kişileri diğerlerinden ayırt etmeye elverişli olması halinde kişisel veri işlendiği kabul edilecektir.

b) Enformasyon İçerme Unsuru

Hukuk doktrininde, kişisel veri kavramının diğer unsurları sıklıkla vurgulanırken, kişiye ilişkin "enformasyon" kavramının, veri kavramından farkı üzerinde yeterince durulmamaktadır. Aynı şekilde 29. madde çalışma grubu da enformasyon kavramını tanımlamamış, daha ziyade hangi enformasyonun kişisel veri mevzuatı koruması altında kabul edileceğine dair örnekler sunmuştur. Çalışma Grubu, "herhangi enformasyon" teriminin kişisel veri kavramını geniş bir şekilde yorumlama amacıyla özellikle tercih edildiğinin altını çizmektedir. Bu anlayışla, söz konusu enformasyonun objektif veya sübjektif olması, doğruluğu ya da yanlışlığı, formatı (sözlü, yazılı, harfli şekil, fotoğraf, sayı ve sesle ifade edilmesi) fark etmeksizin kişisel veri teşkil edebileceğini vurgulamaktadır[145].

Bu bağlamda, enformasyon ("information") ile neyin kast edildiği, bu terimin "veri", "bilgi" gibi diğer kavramlardan farkının tespit edilmesi önem taşımaktadır. Enformasyon kelimesinin Türkçe kökenli bir karşılığı bulunmamakta, bu durum kimi zaman hatalı olarak tercümelerde bilgi kelimesinin kullanılmasına yol açmaktadır. Bazı kaynaklarda enformasyon yerine malumat kelimesi tercih edilse de bu kavram literatürde yaygınlık kazanamamıştır[146]. Latin kökenli "informatio"dan türetilmiş enformasyon kavramı, Platon'un "eidos" ("idea") kavramı ile Aristo'nun şekil

[144] Purtova, s.47, 48.
[145] Article 29 Working Party, s.6, 7.
[146] Abdurrahman Cihad Kayaduman/Harun Hilmi Polat, "Veri Temelli Enformasyon Tanımı", **Akademik Sosyal Araştırmalar Dergisi**, Cilt: 6, Sayı: 79, Ekim 2018, s. 326-336, s.335.

anlamına gelen "morphe" kavramından türetilmiştir[147]. Bugün ham halde bulunan verinin benzer verilerle birlikte gruplandırılarak işlenmiş ve bu bağlamda "şekil verilmiş" halini ifade etmektedir. Başka bir deyişle, veri, duyularımızla ya da sensörlerle toplanmış ancak henüz işlenmemiş ve bir anlam kazanmamıştır. Enformasyondan bahsetmek için ise, veriler arasında bağ kurulup bunlara bir anlam kazandırılmış olmalıdır[148]. Bilişim teknolojileri açısından bakıldığında, aslında gerçek hayattaki pek çok olay, hareket ve gözlemlerimiz, makinelerin okuyabileceği bir formatta, bağlamlarından koparılarak ve yapay zekânın bir anlam üretemeyeceği şekilde kaydedilmektedir. Veri madenciliği, yazılımlar aracılığıyla bu verilerin ilişkilendirilmesini, gruplandırılmasını ve bu yolla yorumlanabilir, anlamlandırılabilir kılınmasını sağlamaktadır. Benzer şekilde, tezin konusunu oluşturan profilleme teknolojileri de tekrar eden döngüler üzerinden verileri belli kategoriler altında toplama ve aralarında bağ kurmak amacı taşımaktadır[149]. Dolayısıyla, çeşitli kanallardan akan verinin kaydedilmesi, yeniden organize edilmesi ve analiz edilmesi mümkün olacak şekilde toplanması halinde enformasyon söz konusudur. Son bir benzetmeyle, veri, harflere benzer ancak enformasyon harflerin bir araya getirerek kelimeler üretilmesi gibidir.

Bununla birlikte hem insan beyni hem yapay zekâ açısından "bilgi" bir sonraki aşamadır. Bilgi ("knowledge"), düşünmeyi ve edinilen enformasyonu rasyonel bir şekilde akıl süzgecinden geçirmeyi gerektirir[150]. Bilgi, enformasyondan çok daha fazla emek ve zaman gerektirir ve enformasyona göre daha sistematik ve kalıcıdır. Verileri gruplayarak enformasyon halinde kaydetmek, karşılaştırmak, kıyaslamak ve aktarmak mümkünken, bilgi zaman ve tecrübeyle oluşur, dolayısıyla enformasyon gibi bir anda kaydedilmesi ve aktarılması mümkün değildir[151]. Nitekim bilgi, düşünce üretmeyi, neden ve niçin sorularına yanıt aramayı içerir; enformasyon ise kim, nerede, ne zaman sorularını yanıtlar ve yalnızca sonucu aktarır[152].

---

[147] Matthew Kelly/Jared Bielby, **Information Cultures in The Digital Age: A Festschrift in Honor of Rafael Capullo**, Springer: Wiesbaden, 2016, s.7

[148] Gene Bellinger/Durval Castro/Anthony Mills, "Data, Information, Knowledge, and Wisdom", https://www.systems-thinking.org/dikw/dikw.htm, Erişim Tarihi: 20.02.2021.

[149] Mireille Hildebrandt, "Profiling: From Data to Knowledge", **Datenschutz und Datensicherheit**, Cilt:30, Sayı:9, 2006, ss. 548-552, s.549.

[150] Purtova, s. 51.

[151] Belgin Arslan Cansever, "Bilgi Toplumunda Bir Kavram Kargaşası: Bilgi mi? Enformasyon mu?", **Sosyoloji Dergisi Armağan Sayısı**, 2017, ss. 41-50, s.47.

[152] Arslan Cansever, s.48.

Günümüzde büyük veri neredeyse kutsal bir anlam kazanmış ve bilgi kavramıyla iç içe geçecek şekilde kullanılmaya başlanmıştır[153]. Daha fazla veri toplanması ile kişiler ve olaylar hakkında bilgi edinileceğine dair inanç sorgulanmaz hale gelmiştir. Oysa yukarıda tartışıldığı üzere, henüz işlenmemiş, mantık süzgecinden geçirilmemiş veri, bilgi ile eş değerde değildir. Nitekim insan eliyle incelenmesi ve analiz edilmesi imkânsız hale gelen veri havuzlarından, ancak yazılımlarla bilgi üretilebilmektedir. Ancak burada göz ardı edilmemesi gereken husus, yapay zekâ teknolojilerinin insanların bilgi üretiminden farklı bir şekilde bilgi ürettiği gerçeğidir. Söz konusu teknolojiler, veri tabanlarından süzdükleri enformasyonlar üzerinden matematiksel olasılıklar kurmakta ve yalnızca tahminlerde bulunmaktadır. Örneğin, insanların anlamlandıramayacağı oranda enformasyonu süzerek kişilerin alışkanlıkları ve tercihlerine dair istatistiksel analizler üretmektedirler. Elbette bu durum, insanların hayatın genel akışından, tecrübelerinden, fiziksel, biyolojik, psikolojik ve toplumsal şartlarından yola çıkarak öğrendikleri nedensellik ilişkilerine göre çok daha otomatlaşmış bir öğrenmeye dayanmaktadır. Dolayısıyla teknolojik gelişmeler karşısında yapay zekâ tarafından üretilen "bilgi", yeni bir bilgi türü olarak karşımıza çıkmakta ve bu yeni bilgi türüne dayanarak kişilerin hayatları üzerinde sonuç doğuracak kararlar alınmaktadır[154].

Bu nedenlerle, GDPR kapsamında, bilgi terimi yerine enformasyon teriminin tercih edilmesi önemli bir ayrımdır. Bu durumda, kişisel verilerin korunması, mantık süzgecinden geçirilmiş bilgi aşamasından çok daha önce devreye girmektedir. Henüz işlenmemiş, ham haldeki veriler, toplandığı ve gruplar haline getirilerek enformasyon olarak ele alındığı andan itibaren ilgili mevzuatın koruma alanına girecektir.

c) Gerçek Bir Kişiye İlişkin Olma Unsuru

Bir verinin kişisel veri olarak kabul edilebilmesi için diğer önemli unsur, verinin gerçek kişiye ilişkin olmasıdır. Burada terim olarak ilgili kişi "hakkında" yerine "kişiye ilişkin olma" tabirinin kullanılması önem taşımaktadır. Nitekim bir veri, doğrudan ilgili kişi hakkında olmasa dahi içeriği, amacı ve kullanılmasının sonucunda

[153] Bilgi ile verinin hemen hemen eş anlamlı şekilde kullanıldığına dair, bkz. Elif Küzeci, **Kişisel Verilerin Korunması**, On İki Levha Yayınevi: İstanbul, 2020, s.13.
[154] Mireille Hildebrandt, **Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology**, Edward Elgar Publishing: Cheltenham, Mart 2015, s.25, 26.

o kişi üzerinde önemli bir etki doğuruyor, dolayısıyla kişi ile ilişkilendirilebiliyorsa, kişisel veri olarak değerlendirilebilecektir. Bu nedenle örneğin üçüncü bir kişi veya eşya hakkındaki enformasyon da kişisel veri olarak değerlendirilebilecektir[155].

29. madde Çalışma Grubu, doğrudan bir hastanın tıbbi test sonuçlarının ya da görüntüsünün kaydedildiği durumda, bu kişiye ilişkin kişisel veri işlendiğine dair şüphe bulunmadığını belirtmektedir. Bununla birlikte bir eşya da kimi durumda kişiye ilişkin veri olarak kabul edilebilir. Örneğin, bir evin değerinin genel olarak bölgedeki taşınmaz fiyatlarını belirlemede kullanılması halinde, bu veri kişisel veri kapsamında değerlendirilemeyecektir. Ancak aynı veri mülk sahibinin ne kadar vergi ödeyeceğini belirlemek için işlendiği takdirde, ev fiyatının kişiye ilişkin veri olarak kabul edilmesi gerekir. Bunun yanı sıra kişinin niteliklerini ve davranışlarına ilişkin veriler, bu kişiye yönelik muameleyi değiştirecek veya kişinin herhangi bir şekilde değerlendirilmesinde kullanılacak ise bu veriler de kişiye ilişkin veridir.

Sonuç olarak, bir verinin kişiye ilişkin olup olmadığına, bu verinin içeriğine, amacına veya sonucuna bakılarak karar verilir. İçeriği itibariyle kişisel veri olan belgeye örnek olarak kişinin kimlik bilgilerini gösteren belge verilebilir. Bir şirketteki telefon aramaları, şirketin telefon ücretinin ödenmesi için işleniyorsa, şirkete ilişkin veri iken, çalışanların çalışma saatlerini kontrol için işleniyorsa, amacı itibariyle çalışanlara ilişkin kişisel veridir. Bu bağlamda, verinin içeriği değil işlenme amacı kişilere ilişkin olup olmadığını tespitte belirleyicidir. Son olarak, verinin işlenmesi kişi üzerinde bir sonuç doğuruyor olabilir. Verinin işlenmesi, kişiye diğerlerinden farklı davranılmasına yol açacak nitelikte bir sonuç doğurma potansiyeli barındırıyor ise söz konusu veri sonucu itibariyle ilgili veri kişiye ilişkin veri kabul edilir. Örneğin, taksi işletmecisi, hangi bölgede hangi taksilerin hazır bulunduğunu müşterilerine hizmet amacıyla taksi uydu sistemiyle işliyor olabilir. Bununla birlikte söz konusu sistem, sürücülerin takip edilmesini, kendilerinden beklenen rotayı izleyip izlemediklerinin tespit edilmesini de mümkün kılmaktadır. Sonucu itibariyle bu sistem, belirli sürücülerin gözetimini mümkün kılacağından, kişiye ilişkin veri kabul edilecektir. Burada üzerinde durulması gereken husus, içerik, amaç ve sonuç unsurlarının

[155] Purtova, s. 54.

kümülatif şekilde aranmadığıdır. Bu unsurlardan herhangi birinin varlığı yeterlidir ve bu durumda ilgili veri "kişiye ilişkin" kabul edilecektir[156].

Avrupa Birliği Adalet Divanı da 29. Madde Çalışma Grubuna paralel şekilde kişiye ilişkin olma kavramını geniş yorumlamakta, içerik, amaç veya sonuca göre değerlendirme yapmaktadır. Örneğin, Divan, sınav kâğıdına erişim hakkının kişisel veri korumasından yararlanıp yararlanmayacağını değerlendirdiği Nowad kararında, ilgili verinin sınavı yazan kişiye ilişkin olup olmadığını içerik, amaç ve sonuç unsurlarından yola çıkarak ele almıştır. Divan, sınav kâğıdının katılımcının bilgisi, düşünme şekli, el yazısı gibi verileri barındırması sebebiyle içerik olarak kişi ile doğrudan ilişkilendirilebilir olduğunu belirtmiştir. Bunun yanı sıra, katılan kişinin performansını tespit ve değerlendirme amacıyla işlendiğini, dolayısıyla amaç unsuru açısından da kişiye ilişkin olduğunu belirtmiştir. Son olarak kişinin ileriki yıllarda, işe alımının değerlendirilmesinde etkili olacağı için sonuç unsuru açısından da kişiye ilişkin olduğu vurgulanmıştır. Hatta amaç ve sonuç unsuru değerlendirildiğinde, yalnız adayın yanıtları değil, üçüncü bir kişi tarafından yapılan değerlendirme ve kâğıt üzerindeki yorumlar da adaya ilişkin kişisel veri kabul edilmiştir[157].

Özellikle profilleme teknolojileri, günümüzde kişileri belli bir gruba ayırarak değerlendirmekte, bu yolla davranışlarını veya seçimlerini etkileyecek şekilde belli bir ürünü satın almaya yönlendirmekte, ödeme ve ücretlendirmelerde farklı muamele görmelerine yol açmaktadır. Yine ceza ve idare hukuku alanında, kişilerin topluma yönelik tehlike oluşturup oluşturmadıklarını tespit etmek üzere sevk edilmektedirler. Dolayısıyla bu teknolojiler eliyle toplanan veriler ilk bakışta, tek tek değerlendirildiğinde kişiye ilişkin olarak görünmese de amaçları veya sonuçları bakımından bütüncül şekilde ele alındıklarında, kişiye ilişkin kabul edilmelidir[158].

Sonuç olarak GDPR kapsamında korunan kişisel veriden bahsedebilmek için, bir enformasyon, gerçek bir kişiye ilişkin olmalı ve bu kişinin kimliği belirli veya belirlenebilir olmalıdır. Ancak günümüz teknolojileri karşısında, söz konusu kavramların veri işleme sürecinde bütüncül şekilde değerlendirilmesi gereklidir.

[156] Article 29 Working Party, s.9-11.
[157] Purtova, s.69-71.
[158] Purtova, s.55.

Nitekim profilleme ve diğer veri madenciliği teknolojileri, insan zihniyle gerçekleştirilmesi mümkün olmayacak bir bağlantı ağı kurmakta, tüm kaynaklardan sızan verileri süzerek kişilerin davranış örgülerini tespit edebilmektedir. Bu durum ise kişinin belirlenebilir olma ihtimalini geçmişe nazaran çok daha fazla mümkün kılmakta, anonim kalmayı neredeyse imkânsız hale getirmektedir. Bu nedenle kişisel veri kavramı, bu süreçlerin amacı ve sonucu değerlendirilerek ele alınmakta, kişinin maddi durumu, sosyal koşulları, politik tercihleri gibi pek çok hususta puanlandırma ve gruplandırma ile farklı muamele görmesine yol açıldığı durumlarda, toplanan enformasyon kişisel veri kabul edilerek koruma altına alınmaktadır. Yukarıda tartışılan Avrupa Adalet Divanı ve AİHM kararları da veri kavramının geçmişe nazaran çok daha geniş yorumlandığına işaret etmektedir.

d) Özel Nitelikli Kişisel Veriler

Yukarıda detaylı şekilde ele alınan kişisel veri kavramı, kendi içerisinde genel nitelikli veriler ve hassas veriler ile doğrudan veriler ve türetilmiş veriler gibi alt gruplara ayrılmaktadır.

Özel nitelikli kişisel veriler, kişilerin ırkı, etnik kökeni, siyasi görüşü, dini ve felsefi inançları, sendika üyeliği, sağlık ve cinsel yaşamları gibi daha hassas bilgi içererek ilgilerin ayrımcılığa uğrama risklerini arttırdıklarından, daha farklı bir rejim ile koruma altına alınmıştır.

Özel nitelikli kişisel verileri ifade etmek üzere veri koruma kanunlarında "hassas veri" (sensitive data), "özel kategori grubundaki kişisel veriler " (besonderer Kategorien personenbezogener Daten[159]) , “özel nitelikli kişisel veriler”, ve "özel korumaya layık veriler" (besonders schutzwürdige Daten) kavramlarının kullanıldığı görülmektedir[160]. Hangi veri gruplarının özel nitelikli veri kabul edileceği de ülkeden ülkeye değişiklik göstermektedir. Ana hatlarıyla 108 sayılı Sözleşme'nin 6. maddesinde ırksal kökene, siyasi görüşlere, dini ve diğer inançlara, sağlığa ve cinsel

[159] Alman Federal Kişisel Verilerin Korunması Kanunu, bkz. https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html#BJNR209710017BJNG000100000, Erişim Tarihi: 20.02.2021, benzer şekilde GDPR m.9.

[160] Sırasıyla Hollanda ve Avusturya Kişisel Verilerin Korunması Kanunu’ndan örnekleri aktaran Kaya, Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXIX, Sayı: 1-2, 2011, ss. 317-334, s.318.

yaşama ve geçmiş mahkûmiyetlere ilişkin veriler özel nitelikli veri olarak sayılmış ve bu tür verilerin özel niteliği hemen hemen tüm ülkelerde kabul edilmiştir. Kimi ülkelerin ulusal mevzuatlarında ayrıca genetik bilgilere (Polonya, İzlanda, Estonya ve Bulgaristan), ten rengine (İzlanda), milli kökene (Çek Cumhuriyeti), bağımlılıklara (Polonya), alkol, tıbbi ilaç ve uyuşturucu kullanımına (İzlanda), destek ve diğer sosyal refah yardımlarına (Finlandiya), işlenen ya da işlendiği iddia edilen suçlar için yürütülen kovuşturmalara (İngiltere) ilişkin veriler de özel nitelikli veri olarak kabul edilmiştir[161]. GDPR ise 9. maddesinde ırksal, etnik kökeni, politik veya felsefi fikirleri, sendika üyeliğini, kişinin cinsel hayatı ve yönelimini, sağlık bilgilerini belirten verilerin yanı sıra, ayrıca biyometrik ve genetik bilgilerin de özel nitelikli veri kategorisinde sayılacağını belirterek, bu verilerin işlenmesi için ayrı bir rejim öngörmüştür. Diğer veri türlerinden farklı olarak, özel nitelikli veriler açısından kural, veri işlemenin yasak olması, istisna ise maddede öngörülen amaçlarla ve özel önlemler alınarak verilerin işlenebilmesidir.

Bununla birlikte hangi verilerin özel nitelikli sayılacağının tespiti her zaman kolaylıkla yapılamamaktadır. Örneğin, bir kişinin dini inancını gösteren yemek tercihi veya bir kişinin cinsel saldırı suçunu işlediğine dair bilgi tartışmasız bir şekilde özel niteliklidir. Bununla birlikte, yalnızca merak sebebiyle bir bölgedeki sinagoglara ilişkin yapılan internet araması veya kişinin siyahi olduğunu gösteren bir fotoğrafın salt dini veya ırk niteliklerini içermesi nedeniyle özel nitelikli veri olup olmadığı tartışmalıdır. Örneğin İngiltere'de görülen Naomi Campbell davasında, siyahi bir manken olan Campbell'ın fotoğrafları, medyada siyahi bir manken olarak tanınan ve mesleğini yıllardır icra eden manken açısından özel nitelikli kişisel veri olarak kabul edilmemiş, ancak aynı davada, Campbell'ın the Narcotics Anonymous'ta uyuşturucu tedavisi gördüğü bilgisi ve bu tedavinin detaylarının paylaşılması sağlık ve zihinsel durumuna ilişkin özel nitelikli veri olarak kabul edilmiştir[162].

Günümüzde profilleme teknolojileri, özel nitelikli olmayan verileri işlemese dahi, tüm verileri ilişkilendirerek belli sonuçlara varmakta, kişinin sosyo-ekonomik durumu, politik görüşleri, ırkı gibi özel nitelikli verileri tespit edebilmektedir.

[161] Kaya, s.319.
[162] Campbell v MG N Lt d per Morlan d J [2002] EWH C 499 , (2002) HRLR 28 at parag 85- 86, aktaran Kaya, s.322, 323.

Dolayısıyla bu durumda, ilk bakışta işlenen veriler özel korumaya tabii olmasa da diğer verilerle birleştirildiğinde, bu veriler kişiye ilişkin özel nitelikte verileri açığa çıkarabilmektedir[163]. Bu nedenle özel nitelikte verilerin tespiti, daha geniş şekilde ele alınmalıdır. Nitekim 29. Madde Çalışma Grubu, posta kodu gibi kimi verilerin, dolaylı olarak özel nitelikli verileri açığa çıkarabildiklerinin altını çizmektedir. Ancak çoğu durumda, örneğin posta kodunu paylaşan kişi, oturduğu bölgenin sınıfsal-ırksal aidiyet analizinin yapılarak hakkındaki özel nitelikli verilerin paylaşılacağını bilmemekte, dolayısıyla özel nitelikli verisinin işlenmesi hususunda açık rızası bulunmamaktadır. Yine bu bağlamda, "Cambridge Analytica" skandalının ortaya koyduğu üzere, Facebook'ta paylaşılan veriler, kişilerin politik görüşlerine göre sınıflandırılması ve buna uygun haber ve reklamlarla hedeflenmeleriyle sonuçlanmıştır. Bu örnekte de kişilerin sonuçlarını bilmeden paylaştıkları verilerin işlenmesi ve bunlara dayanılarak özel nitelikli verilerin tespit edilmesi söz konusudur. Bu tür durumlarda, özel nitelikli verilerin korunma rejiminin dışına taşılmakta, bu verileri işlemek için aranan istisnai hiçbir hükme dayanmak mümkün olmamaktadır[164]. Dolayısıyla toplanan veriler kadar verilerin ne şekilde ve ne amaçla analiz edildiği de önem taşımaktadır. Yeni teknolojiler ışığında özel nitelikli olan ve olmayan veri ayrımı gittikçe güç hale geldiği, özel nitelikli olmayan verilerin de kolaylıkla özel nitelikli verilere dönüşebildiği dikkate alınmalıdır.

Tüm bu nedenlerle özel nitelikli verilerin işlenmesini sınırlandırabilmek adına doktrinde çeşitli görüşler öne sürülmüştür. Bunlardan ilki, özel nitelikli veri tespitinde, verinin işlenme amacının belirleyici olduğudur. Bu görüşe göre şayet, veri işleyen veya veri sorumlusu, profilleme teknolojilerinden yararlanırken kişilere ilişkin hassas verilere ulaşmayı amaçlıyorsa bu durumda tüm süreç boyunca GDPR m.9 veya diğer kişisel verileri koruma mevzuatlarındaki özel düzenlemelere riayet etmelidir. Örneğin uyuşturucu tedavisi gören kişilere dışarıdan yemek teslimi yapan bir firma, bu kişilerin sağlık durumlarına ilişkin analiz yapmak amacıyla veri madenciliği yapıyorsa, özel nitelikle veri koruma rejimine tabii olmalı, salt yemek teslimi amacıyla tedavi merkezindeki kişilerin adres bilgilerini işliyorsa özel bir rejime tabi olmamalıdır. Yine

[163] Article 29 Working Party, **Opinion 03/2013 on Purpose Limitation**, 00569/13/EN WP 203, 02.04.2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, Erişim Tarihi: 22.02.2021, s.47. Grup profilleme teknolojileri ile anonim verilerin dahi belirli bir sokakta oturan kişilerin etnik kökeni, siyasal görüşü, dini inançlarına dair tespit yapmak üzere kullanılabileceğine dair, bkz. Küzeci, s. 282.

[164] Wachter/Mittelstadt, "A Right to Reasonable Inferences", s.563.

bir haber kanalı, kişilerin dini görüşlerini ifşa amacı taşımadan tesadüfen belli kişilerin görüntülerini paylaştıysa, veri işleme sırasında özel nitelikli veri işleme amacı söz konusu değildir. Ancak bu kıstas kuşkusuz ki "tesadüfen işleme" gerekçesiyle özel nitelikli verilerin koruma rejiminden kaçınma imkânı barındırmaktadır. Nitekim 29. Madde Çalışma grubu da özel nitelikli verileri belirlerken verilerin işlenme amacı kıstasından kaçınmakta, fotoğraf, görüntü gibi verileri işleyen teknolojilerin, bu verileri işleme amacına bakılmaksızın özel nitelikli veri işlediklerini kabul etmek gerektiğini belirtmektedir[165]. Doktrinde özel nitelikli verileri kısıtlamak için kullanılan ikinci ölçüt ise bu verilerin hassas bilgileri kesin ve güvenilir şekilde ifşa etmeye elverişli olmasıdır. Örneğin bir kişinin sendika tarafından düzenlenen bir eyleme katılması, doğrudan sendika üyesi olduğunu kanıtlamamaktadır. Yine bir kişinin Avrupa Parlamentosunda çalışıyor olması, kesin bir şekilde siyasi görüşünü ifşa etmemektedir. Ancak yalnızca doğru ve kesin güvenilir bilgilerin hassas veri kabul edilmesi yönündeki bu görüş de günümüzde yetersiz kalmaktadır. Nitekim profilleme teknolojileri bu şekilde kesinlik ve doğruluk unsurlarını aramaksızın, nedensellik ilişkisi kurmaksızın kişileri belli hassas verilere göre gruplayabilmekte ve bu gruplama kişiler üzerinde hukuki ve sosyal sonuçlar doğurmaktadır. Ortaya çıkan sonuçlar bakımından, dayanılan verilerin doğru ve güvenilir olup olmaması, yapılan çıkarımlara göre kişinin hayatını etkileyen kararlar alınmasını engellememektedir[166]. Bu nedenle profilleme sürecinde, amaç ve güvenilir bilgi kıstaslarından ziyade, profilleme ve diğer teknolojiler ile elde edilen sonuçlar ve bu sonuçların kişiler üzerindeki etkileri dikkate alınarak özel nitelikli verilere ilişkin rejimin uygulanıp uygulanmayacağı belirlenmelidir.

e) Türetilmiş Veriler

Tez kapsamında incelenen profilleme teknolojileri ile kişisel verilerin işlenip bu veriler üzerinden yeniden çıkarım yapılması ve böylelikle yeni verilerin üretilmesi mümkün olmaktadır. Bu tür veriler için türetilmiş veya çıkarımsanan (inferred) veri kavramı kullanılmaktadır. Türetilmiş verilerin, birincil nitelikteki doğrudan verilerle aynı koruma rejiminden yararlanıp yararlanmadığı tartışmalıdır. Koruma rejimlerine yönelik tartışmalar nedeniyle türetilmiş veriler daha detaylı bir şekilde ele alınmalıdır.

---

[165] Wachter/Mittelstadt, "A Right to Reasonable Inferences", s.565, 566.
[166] **Ibid**., s. 566-568.

29. Madde Çalışma Grubu, kişisel verileri ilgili kişiden doğrudan/dolaylı temin edilen birincil veriler ve bunlar işlenerek türetilen veriler olarak iki gruba ayırmaktadır. Örneğin doğrudan ilgili kişinin bir kurum ile paylaştığı isim, soy isim gibi bilgiler, kişinin bizzat temin ettiği doğrudan veri olarak kabul edilecektir. Kişiler belirli hareket ve görüntüleriyle dolaylı veya pasif bir şekilde de veri sunabilir. Örneğin kişinin gözlemlenebilir klavye hareketleri, takip ettiği siteler, ses tonu, yürüme şekli gibi veriler de aracı olmaksızın ilgili kişiden elde edilen ancak kişinin pasif bir şekilde ele verdiği, dolaylı verilerdir[167]. Kişisel verileri koruma mevzuatları temel olarak birincil grup verileri korumayı amaçlamıştır. Bununla birlikte kişiye ilişkin verilerin birleştirilerek hakkında sağlık durumu, alacağı krediyi ödeyebilme potansiyeli gibi profil oluşturulması sonucu ortaya çıkan veriler, ilk grup verilerden türetilmiş verilerdir. Bunlar bizzat ilgili kişiden edinilmemiş, üçüncü kişi ya da veri sorumlusu tarafından başvurulan teknolojiler aracılığıyla çıkarım yapılarak elde edilmiştir. Türetilmiş (inferred) veri şeklinde adlandırılan bu veri grubunun kişisel verileri koruma mevzuatlarında yeterince koruma altına alınıp alınmadığı tartışmalıdır. GDPR kapsamında bu tartışmayı gidermek adına kimi maddelerde doğrudan verilere ilişkin kimi maddelerde ise türetilen verilere ilişkin özel düzenlemeler yapılmıştır. Örneğin GDPR 14. madde başlığı "kişisel verilerin veri sahibinden alınmadığı hallerde sağlanacak bilgiler" olup ilgili madde kişisel verilerin veri sahibinden alınmaması, başka bir deyişle veri sorumlusu veya üçüncü bir kişi tarafından işlenerek dolaylı veri elde edilmesi durumunda, ilgili kişinin bilgi alma hakkını açıkça düzenlemiştir. 29. Madde Çalışma Grubu da kişisel bilgilere erişim, düzeltme ve silinmesini talep etme gibi hakların profilleme ile türetilen verilere de uygulanması gerektiğini ayrıca belirtmektedir[168].

Bununla birlikte GDPR kapsamında verilerin taşınmasını düzenleyen 20. maddede, hükmün ilgili kişi tarafından veri sorumlusuna sağlanan kişisel verilere uygulanacağı açıkça belirtilmiştir. Dolayısıyla bu madde, yalnızca doğrudan verilerin başka bir veri sorumlusuna iletilmesi durumunda uygulanabilecektir. Bu durumda

---

[167] Article 29 Working Party, **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation**, 2016/679, 17/EN, http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826, 06.02.2018, Erişim Tarihi: 25.02.2021, s.8.

[168] Article 29 Working Party, **Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation**, s.47.

kişinin verilerinden türetilmiş yeni veriler açısından verilerinin taşınmasına ilişkin haklarına başvurması mümkün olmayacaktır. Bu nedenle, ilgili verilerin doğrudan veya türetilmiş veri olup olmadığı ayrımı, kimi hakların uygulama alanını belirleme açısından önem arz etmektedir.

3. Kişisel Veri İşleme Boyutuyla Profilleme Teknolojileri ve Bu Teknolojilerin Barındırdıkları Riskler

Profilleme gündelik hayatta, canlı organizmaların tümü tarafından hayatta kalmak ve ortamlarına uyum sağlamak için güdüsel şekilde gerçekleştirilmektedir. Hangi verinin yaşama ayak uydurmak için önemli olduğuna karar veren canlılar, bunu biriktirdikleri tecrübe ve çevrelerini analiz etme yoluyla gerçekleştirmektedir[169]. Algoritmalar eliyle gerçekleştirilen profilleme de gündelik yaşamda gerçekleştirilen profillemenin bir yansımasıdır. Ancak farklı olan, teknolojik profillemenin hayatta kalma güdüsüyle değil, şirketlerin belli kişiler ya da kişi gruplarını hedef alarak kâr edebilmesi veya hükümetlerin toplumu kontrol edebilmesi amacıyla gerçekleştirilmesidir. Bu amaçlarla kişilerin sosyo-ekonomik durumu, eğilimleri, güvenilirliği gibi niteliklerine dair genel çıkarımlar yapılmakta ve bu çıkarımlar üzerinden kişi ya da grupların gelecekteki hareketlerine dair öngörülerde bulunulmaktadır[170]. Yine diğer bir fark, algoritmaların tecrübelerden değil, geçmiş verilerden yola çıkarak geleceği matematiksel olarak tayin edilmeye çalışmalarıdır

Ana hatlarıyla profilleme, veri madenciliğinin özel bir türü olarak nitelendirilebilir. Nitekim profilleme teknolojileri de büyük veri tabanlarından yola çıkarak sınıflandırmalar ve belli özelliklere dayanan kategoriler yaratılmaktadır. Bu yolla, kişilere, gruplara, kimi zaman coğrafi yer ve bölgelere dair profiller oluşturulmaktadır. Profiller eliyle kişilerin tekrar eden özellikleri üzerinden modeller oluşturarak eğilimleri ve gelecekte sergileyecekleri davranışları tespit edilmeye çalışılmaktadır. Bu modeller, geleceğin daha öngörülebilir olmasını sağlama iddiası taşımakta ve kimi zaman pazarlama ve stratejik uygulamaların geliştirilmesi, kimi

---

[169] Mireille Hildebrandt, "Defining Profiling: A New Type of Knowledge?", İçinde: **Profiling the European Citizen**, Ed. Mireille Hildebrandt/ Serge Gutwirth, Springer Science: Dordrecht, Mayıs 2008, s.26.

[170] Stefanie Hänold "Profiling and Automated Decision-Making: Legal Implications and Shortcomings", Robotics, İçinde: **AI and the Future of Law**, Ed. Marcelo Corrales/Mark Fenwick/Nikolaus Forgó, Springer Science: Dordrecht, Kasım 2018, ss.123-154, s.125.

zaman ise cezai ve idari önlemlerin alınmasında kullanılmaktadır. Teknoloji eliyle türetilmiş bu bilgi, hipotezlerden yola çıkan ve test edilerek kabul edilen bilgi kavramından farklı olup yalnızca geçmişteki verileri birbirine bağlayan ve bu verilere dayalı olarak "göreceli" bir niteliğe dayanan tahminler silsilesinden oluşmaktadır[171].

a) Grup Profillemesi- Bireysel Profilleme Ayrımı

Profilleme teknolojileri ele alınırken bu teknolojilerin nasıl bir sınıflandırmaya dayandığı önem taşımaktadır. Nitekim AB mevzuatı çerçevesinde profillemeye ilişkin düzenlemeler kimi profilleme teknolojilerini dışarıda bırakmaktadır.

Profilleme teknolojileri temel olarak sınıflandırdıkları kişiler bakımından bireysel profilleme ve grup profillemesi olarak ikiye ayrılmaktadır. Bireysel profilleme, bir kişinin belirlenebilmesi veya şahsına özel niteliklerin tespit edilebilmesi için gerçekleştirilen profilleme türüdür[172]. Bu profilleme türü bir kişinin verilerinden yola çıkarak bu kişinin alışkanları, yaşam tarzı, genetik özellikleri ve davranış kalıplarının ortaya çıkarılması ile sonuçlandığı için kişisel verilerinin korunması hakkına daha yoğun bir müdahale içerir. Örneğin kişinin gün içinde klavye kullanma şekli ve sıklığı ve yine zaman içerisinde ziyaret ettiği internet sitelerinden yola çıkarak çevirimiçi alışkanlıklarının belirlenmesi ve kişinin bu yolla diğerlerinden ayırt edilmesi bireysel profilleme örneğidir[173]. Böylelikle kişi tekrar internette arama yaptığında, kendisine has oluşturulan profil üzerinden tespit edilebilir ve bu profile uygun ürün ve hizmetlere yönelik reklamlarla hedeflenebilir hale gelmektedir. Bu tür profiller, elbette yalnızca şirketler tarafından ilgi görmemektedir. Kişilerin tercihleri ve davranış kalıplarını öngören profiller, işverenler, göçmen idareleri ve hükümetler tarafından da talep edilmekte ve böylelikle bireyler hakkında öngörülerde bulunulmakta, geçmiş ve potansiyel gelecek davranışları üzerinde hâkimiyet kurulmaya çalışılmaktadır[174].

---

[171]Francesca Bosco/Niklas Creemers/Valeria Ferraris/Daniel Guagnin/Bert-Jaap Koops,"Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities", İçinde **Reforming European Data Protection Law**, Ed. Serge Gutwirth/Ronald Leenes/Paul de Hert, Springer Science: Dordrecht, 2015, s.3-33, s.6-7.

[172]Elena Gil González/Paul de Hert, "Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data: An Analysis of GDPR Provisions and Principles", **ERA Forum**, Cilt: 19, 2019, ss:597–621, s.610.

[173] Hildebrandt, "Profiling: From Data to Knowledge", s.549.

[174] Hildebrandt, "Defining Profiling: A New Type of Knowledge?", s.20,21.

Kişilerin alışkanlıklarını, bilgi birikimlerini, toplum düzenine karşı risk oluşturup oluşturmadıklarını değerlendiren bireysel profilleme teknolojileri, kendi içerisinde doğrudan bireysel profilleme teknolojileri ve dolaylı bireysel profilleme teknolojileri olarak ikiye ayrılmaktadır. Doğrudan bireysel profillemede, profilleme salt bir kişi üzerinde gerçekleştirilmekte ve bu kişinin davranış kalıpları tespit edilmeye çalışılmaktadır. Dolaylı bireysel profillemede ise, bireysel profilleme ve grup profillemesi yöntemlerini birleştirilerek, pek çok kişinin hareketlerinin bütününden yola çıkılmakta, benzer nitelikte kişilerin gruplandırılmasının ardından, kişiler ait oldukları gruba göre değerlendirilmektedir. Dolayısıyla bir nevi tümden gelim yöntemiyle, benzerlik gösterdikleri gruplar üzerinden bireylerin değerlendirilmesi söz konusudur. Örneğin sigorta şirketleri, sigara içen bir kişinin ait olduğu "sigara içenler" grubu üzerinden varsayımlarda bulunmakta ve bu kişinin potansiyel özellikleri ve sağlık riskleri dolaylı bireysel profilleme ile ele alınmaktadır. Yine benzer şekilde, bir kişinin televizyon izleme alışkanlığı, bu alışkanlığa sahip diğer kişilerin profillerinden yararlanılarak analiz edilmekte ve kişinin cinsiyeti, yaşı ve diğer niteliklerini ortaya koymak üzere kullanılmaktadır[175].

Grup profillemesinde ise veri madenciliği teknolojileri ile benzer özellikleri veya benzer davranış kalıplarını paylaşan kişi grupları tespit edilmektedir. Kimi zaman profilleme teknolojileri önceden belirlenmiş sabit gruplar üzerinden hareket etmekte, bu teknolojiler yoluyla hazır olarak verilmiş grubun ortak davranış örgüleri belirlenmektedir. Buna örnek olarak politik bir parti üyelerinin oluşturduğu gruba veri madenciliği yöntemleri uygulanması verilebilir. Yine solak olan veya yeşil gözlü kişi grupları, en baştan ortak özellikleri üzerinden belirlenmiş gruplara örnektir. Bunun yanı sıra grup profillemesi önceden bir grup belirlenmeksizin uygulanabilir ve algoritmalar büyük veriler üzerinden kendiliğinden ortak özellikler tespit ederek gruplar oluşturabilir. Örneğin farklı veri tabanlarından edinilmiş enformasyona uygulanan profilleme teknolojileri, 1-3 yaş arası çocuk sahibi olan ve belli bir bölgede ikamet eden kişilerin her on günde bir koli bira tükettiği gibi örüntüler kurabilir ve bu örüntü üzerinden bu özellikleri taşıyan kişileri aynı grup içerisinde sınıflandırabilir[176]. Bu sınıflandırmalar, kişilerin kazanç oranı, kredi ödememe riskleri, tehlikeli

[175] Hildebrandt, "Defining Profiling: A New Type of Knowledge?", s.41, 42.
[176] Gil González/ De Hert, s.608.

hastalıklara yakalanmaları gibi sonuçlara varmak üzere ve bu sonuçlara dayalı politikalar üretmek amacıyla kullanılmaktadır.

Grup profilleme teknolojileri açısından önemli diğer bir ayrım, "gruba dair özelliklerin tüm bireylere dağıtıldığı" veya "dağıtıcı olmayan" profilleme teknolojileri ayrımıdır. Bunlardan ilki, gruba dair tespit edilen özelliklerin koşulsuz şartsız şekilde tüm üyeler tarafından paylaşıldığını varsaymaktadır. "Üniversite mezunu 25 yaşındaki kişiler" bu tür bir gruba örnektir. Dolayısıyla bir bireyin bu gruba ait olduğu tespit edildiği noktada, ilgili kişinin 25 yaşında belirlenen eğitim grubundaki kişilere atfedilmiş tüm özellikleri taşıdığı kabul edilmektedir. Bununla birlikte dağıtıcı olmayan profilleme teknolojileri, olasılık ve varsayımlara dayanır ve grup içindeki bireyler arasında da karşılaştırmalar yapılmasına olanak tanır. Örneğin Hare'nin "suçluluk hissetmeme, yüzeysel kibarlık, patolojik yalancılık ve saldırganlığı kontrol edememe" gibi nitelikler üzerinden yaptığı psikopat profili, kişileri bu özellikleri gösterdikleri orana göre ele almakta, bu yönüyle dağıtıcı olmayan nitelikte bir profilleme teşkil etmektedir. Bir kişi bu niteliklere ilişkin yapılan değerlendirmede otuz puan üzerinden düşük bir puan alıyorsa gruba ait kabul edilmekle birlikte, diğer grup üyeleriyle tamamen aynı niteliklere sahip olduğu varsayılmamaktadır. Dolayısıyla dağıtıcı olmayan grup profillemesi, kişilerin bireysel olarak değerlendirilmesini de gerektirmektedir[177].

Kişilerin belli özellikleri referans alınarak grup üzerinden değerlendirilmesi kuşkusuz bireysel otonomi ve insanın karmaşık yapısını göz ardı eden bir yaklaşım olup genellemeler üzerinden indirgemeci ve ayrımcı uygulamalara yol açabilmektedir. Örneğin belli posta koduna sahip bölgede oturan kişilerin, kredi borcu ödeyememe veya suç işleme potansiyelinin yüksek olması gibi niteliklerle ilişkilendirildiği durumda, salt yaşadıkları mahalle üzerinden değerlendirilen kişiler, borcuna sadık veya kurallara uyan bir yapıda olsa dahi grupla birlikte ortak yaptırımlara maruz kalacaktır. Kuşkusuz ki kişilerin genellemeler üzerinden adaletsiz şekilde değerlendirilmesi her toplumda insan eliyle de gerçekleştirilen bir uygulamadır. Ancak akıllı teknolojiler eliyle gerçekleştirilen profillemeleri farklı kılan, bu uygulamanın büyük ölçekli şekilde gerçekleştirilmesi ve kimi zaman insan gözüyle dahi tespit edilmesi mümkün olmayan bağlar kurmalarıdır. Bu durum ayrımcılık yasağı teşkil

[177] Hildebrandt, "Definin Profiling: A New Type of Knowledge?", s.21.

eden dil, ırk, renk, cinsiyet, siyasi düşünce gibi kategorilere ek, yeni ve henüz düzenlenmemiş ayrımcılık zeminleri yaratmaktadır. Böylelikle kimi zaman insanlar tarafından anlaşılması mümkün olmayan makine öğrenmesi mekanizmaları ile seri şekilde ayrımcı sonuçlara varılmakta, bu sonuçlara dayalı uygulamalar teknolojinin tarafsız olduğu iddiası ile meşrulaştırılmaktadır[178].

b) Profilleme Sürecinin Aşamaları

Profilleme ana hatlarıyla üç aşamada gerçekleştirilmektedir. İlk aşamada farklı kaynaklardan büyük veri toplanması sağlanmaktadır. Örneğin market alışverişleri, toplu taşıma hareketleri, telefon faturası gibi veriler toplanmakta, bu aşamada veri toplama süreci anonim verilere dayanabilmektedir. İkinci aşamada toplanan veriler yazılımların analizinden geçirilerek belli davranış kalıpları çıkartılmaktadır. Böylelikle algoritmalar aracılığıyla belli davranış modelleri arasında bağlantılar ve benzerliklerin ortaya konulması sağlanmaktadır. Bu aşamada gündelik hayatta insanların başvurduğu sağduyu ve genel mantık yürütme sürecinden farklı olarak tamamen otomatik şekilde veriler arasında bağlantı kurulmaktadır. Örneğin genel mantık kuralları çerçevesinde, çikolata tüketimi ile kredileri süresinde ödeme arasında bağlantı kurma mümkün değilken, algoritmalar istatistiksel sonuçlara dayanarak kredi borcunu ifa etmemiş yüksek oranda kişinin daha çok çikolata tükettiğini ileri sürebilmektedir. Ancak bu bağlar sayısal ve istatistiksel olup, neden-sonuç ilişkisine dayanmamakta, dolayısıyla kimi zaman insan muhakemesi yoluyla anlaşılması mümkün olmamaktadır. Son aşamada ise kurulan bu bağlantılar belli ya da belirlenebilir kişilere uygulanmakta, geçmiş verilerinden ve davranış örgülerinden yola çıkılarak gelecek hareketleri öngörülmektedir. Bu öngörüler, kişiler hakkında verilen kararlara temel alınmaktadır. Tüm bu süreç boyunca dikkat çeken husus, farklı kişi ya da grupların ürettiği büyük verilerden yola çıkarak istatistiksel bağlar kurulması ve kişilerin yalnızca belli gruplara ait olmaları dolayısıyla, kişilikleri ve şahsi tercihleri göz ardı edilerek değerlendirilmesidir[179]. Dolayısıyla sürecin sonunda belli kişilere dair yeni türetilmiş bilgilere varılmaktadır. Bu bilgi, var olan verilerden yola çıksa da

---

[178] Anton Vedder, "KDD: The Challenge to Individualism", **Ethics and Information Technology**, Cilt:1, 1999, ss. 275–281, s.277, 278.

[179] Le Comité des Ministres du Conseil de l'Europe, **La Protection des Personnes à l'Égard du Traitement Automatisé des Données à caractère personnel dans le Cadre du Profilage** Recommandation, CM/Rec(2010)13, 23.11.2010, Editions du Conseil de l'Europe: Strasbourg Cedex, s.43.

geleceğe dair olasılıkları tespit etmeleri dolayısıyla yeni bir bilgi olarak nitelendirilmektedir. Ancak bu bilgi, kişi ile arasında bağlantı kurulan gruplar üzerinden türetilmekte, otomatik olarak kurulan bağlantılardan ibaret olup test edilmemiş ihtimallere dayanmaktadır. Bu nedenle profilleme teknolojileri ile grup aidiyeti üzerinden işleyen ve kişilerin otonom yapısını hiçe sayan, aynı zamanda bilimsel olarak onaylanması güç olan yeni bir bilgi türü doğmuştur. Bu yeni bilgi türü, insanlar üzerinde önemli sonuçlar doğuran, onları otomatik profiller üzerinden açıklayan yeni bir gerçeklik yaratmaktadır.

c) Profilleme Teknolojilerinin Barındırdıkları Riskler

Profilleme yapılırken yukarıda bahsedilen her üç aşamada da çeşitli risklerin doğma ihtimali bulunmaktadır. Örneğin profillemede kullanılan yazılımın oluşturulması sırasında kullanılan model veya analiz yönteminde hata yapılabileceği gibi, yazılıma sunulan verilerin yanlış veya güncellenmemiş olması veya varılmak istenen amaca hizmet etmeyen, kapsam dışı verilerin yazılımda kullanılmış olması mümkündür. Yine önemli olan bir husus, örneğin ticaret alanında kullanılmak üzere tasarlanmış ve şirketin kâr oranını artırmayı amaçlayan bir yazılımın, ceza hukuku gibi başka bir alanda kullanılmasının sakıncalı olmasıdır. Bu nedenle profillemenin henüz ilk aşamalarında, başvurulacak algoritmik karar mekanizmasının kullanılacağı alanın nitelikleri dikkate alınarak doğru modelin seçilmesi, girdi verilerin özenle ele alınması ve risk değerlendirilmesinin yapılması büyük önem taşımaktadır[180].

Bunun yanı sıra, eğer sisteme girilen veriler, en baştan ayrımcılığa yol açmaya elverişli verilerse, profillemenin ileriki aşamalarında, belli kişi ve gruplara yönelik ayrımcı sonuçlara varılması kaçınılmaz olacaktır. Böyle bir durumda, algoritmalar bir nevi ayrımcı verilerden ayrımcı sonuçlar üreten, kendi kendini doğrulayan mekanizmalara dönüşmektedir. Nitekim kendilerine sunulan verilerden yola çıkarak öğrenen yapay zekâ modellerinin, verilerin taraflı olması halinde, farklı bir sonuca varması mümkün değildir[181]. Yanlış veya taraflı verilere dayanılması veya hatalı bir şekilde bir kişinin belirli bir gruba ait tüm nitelikleri gösterdiği iddiası, kişiler hakkında

[180] Stephan Dreyer/ Wolfgang Schulz, **The General Data Protection Regulation and Automated Decision-making: Will it Deliver?**, Bertelsmann Stiftung: Gütersloh, Ocak 2019, s.14, 15.
[181] Ibid, s.14.

adil olmayan kararlar alınmasına[182], belli kişi ve grupların sosyal veya cezai yaptırımlarla toplumdan ayrıştırılmalarına yol açabilmektedir.

Profilleme teknolojileri açısından diğer bir sorun, verileri bağlamı dışına çıkararak ele almalarıdır. Bir bütün teşkil eden özel hayatın farklı bölümlerinden toplanan bu veriler, doğru ve güncel olsalar dahi, kişilerin hangi bağlamda ne tür davranışlar sergileyeceklerinin gerçek resmini yansıtmamaktadır. Bu durum gruplar ve kişiler hakkında hatalı ve tek yönlü bir profil çıkarılmasına yol açabilmektedir. Yine bu veriler, belli bir arka planda anlam ifade ederken, bağlamı dışına çıkarıldığında farklı anlam ve sonuçlara yol açabilmektedir. Örneğin, 45 yaşında çocuk sahibi bir bankacının anti militarist sol bir partiye oy vermesi, her Pazar kilise ayinlerine katılması ve iç mimarlık dergileri okumayı sevmesi, hayatının farklı alanlarına ilişkin, farklı nedenlerle gerçekleştirdiği etkinliklerdir. Ancak profilleme bilgileri ile ilgili kişi, yaşı, hangi şartlar altında ve hangi nedenle bu aktiviteleri gerçekleştirildiği belirlenmeksizin, salt yaşı, oy kullandığı parti veya mimari zevki sebebiyle homojen şekilde ait olmadığı bir grupla ilişkilendirilebilecektir[183]. Bu durum, kişilerin hatalı genellemeler üzerinden kodlanmasına yol açtığı kadar, aynı zamanda farklı profil gruplarıyla eşleştirilme riskinin bilinciyle, belli hareketleri yapmaktan kaçınmalarına yol açmakta ve ifade özgürlüğünü kısıtlayıcı bir etki de doğurmaktadır.

Tüm bu nedenlerle, profilleme teknolojilerine karşı kişisel verileri işlenen ilgililerin, veri işleme sürecinden haberdar edilmeleri, verilerini her aşamada kontrol edebilmeleri, gerektiğinde düzeltme veya silme haklarını kullanabilmeleri, profilleme ile varılan sonuçlara itiraz edebilmeleri oldukça önem taşımaktadır. Yine bu teknolojilerin çalışma modelinin ve vardıkları sonuçların, hayatın olağan akışı karşısında bütüncül bir mantık yürütme kapasitesine sahip insanlar tarafından denetimi oldukça önem taşımaktadır.

Bu hakların gerçek anlamda kullanılabilmesi ve profilleme teknolojilerinin denetlenebilmesi için, yazılımların işleyiş şekli, hangi verilerin ne amaçla tercih edildiği gibi bilgilerin ve varılan sonuçların şeffaf ve anlaşılabilir şekilde ilgili kişilerle

---

[182] Gutwirth/Hildebrandt, s.34.

[183] Franck Dumortier, "Facebook and Risks of 'De-contextualization' of Information", İçinde: **Data Protection in a Profiled World** (Ed: Gutwirth, Serge/Poullet, Yves Poullet, De Hert, Paul), Springer: Dordrecht, Ağustos 2010

paylaşılması elzemdir. Bununla birlikte kimi özel şirketler ürettikleri yazılım hususunda "ticari sır" veya oluşturdukları veri tabanlarına ilişkin "telif hakkı" gibi gerekçelerle yazılımlara ilişkin şeffaf bilgi tesis etmekten kaçınmakta[184], kimi durumlarda ise kendi kendine öğrenen yapay zekâ teknolojilerinin gelişimi ile kurulan bağların açıklanması teknik sebeplerle kendiliğinden imkânsız hale gelmektedir[185]. Aşağıda, Avrupa Birliği mevzuatı çerçevesinde, gelişen teknolojiler karşısında profilleme uygulamalarının doğurduğu risklere karşı öngörülen hakların ne şekilde tanındığı detaylı şekilde ele alınacaktır.

4. GDPR ve 2016/680 sayılı Direktif Kapsamında Profilleme Teknolojilerine İlişkin Düzenlemeler

a) Profilleme Teknolojilerine İlişkin GDPR ve 2016/680 Sayılı Direktifin Uygulama Alanlarının Tespiti

Avrupa Birliği kapsamında kişisel verilerin korunmasına dair iki temel düzenleme olan GDPR ve 2016/680 sayılı Direktif profillemeye ilişkin düzenlemeler barındırmaktadır. 2016/680 sayılı Direktif, suçla mücadele ve ceza muhakemesinin sağlıklı işleyişi için kimi haklar açısından farklı düzenlemeler ve istisnalar barındırmaktadır.

Günümüzde kimi özel şirketler salt suçla mücadele alanında kullanılmak üzere teknolojiler üretebilmektedir. Özel şirketler tarafından toplanan veriler ve bu veriler üzerinden gerçekleştirilen profilleme sonuçları kolluk kuvvetleri tarafından kullanılabilmektedir. Bu durum, GDPR düzenlemesinin mi yoksa 2016/680 sayılı Direktifin mi uygulanacağı hususunda karışıklıklara yol açabilmektedir. Bu nedenle, her iki düzenlemenin kesiştiği noktaların ve hangi durumlarda hangi düzenlemenin geçerli olacağının tespiti önem taşımaktadır.

GDPR, Türkçe karşılığı ile Avrupa Birliği Genel Veri Koruma Tüzüğü, isminin de gösterdiği üzere kişisel verilerin korunmasına ilişkin genel nitelikli bir düzenleme

---

[184] Gutwirth/Hildebrandt, s. 35.

[185] Sandra Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, profiling, Discrimination, and the GDPR", **Computer Law and Security Review**, Cilt:34, 2018, s.436-449, s.443.

olup, özel-kamusal ayrımı yapmaksızın, veri işlemeye ilişkin temel ilke ve hakları belirlemektedir. Bununla birlikte GDPR 23. maddede veri sorumlusu ve veri işleyenin milli güvenlik, milli savunma ve kamu güvenliği söz konusu olduğunda, GDPR 12 ila 22. maddeler ve 34. maddede öngörülen haklar ve yükümlülüklerin kapsamının kısıtlanabileceği belirtilmiştir[186]. 23. maddedeki kısıtlamaların yanı sıra, GDPR m. 2/f.2 (d) bendinde GDPR hükümlerinin kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkili makamlar tarafından kişisel verilerin işlenmesi sürecine uygulanmayacağı belirtilmiştir. Bu alanda öngörülen boşluk 2016/680 sayılı Direktif ile doldurulmuştur[187].

2016/680 sayılı Direktifin uygulanması için, kişisel verilerin suçla mücadele veya ceza muhakemesi sürecinin işleyişi sırasında işlenmesi yeterli değildir. Aynı zamanda bu verilerin ilgili düzenlemenin m.3/7 kapsamında gösterilen "yetkili merci" tarafından işlenmesi gereklidir. İlgili fıkrada suç tehlikesini önleme, suçla mücadele, soruşturma, cezai yargılama ve suç tespiti ile infazında yetkili olan merciler ve ilgili ülke kanununda bu amaçlarla kamusal yetki kullanma hakkı ile donatılmış kurumlar yetkili merci olarak gösterilmiştir. Bu durumda örneğin kolluk görevlilerinin suçla mücadele amacıyla veri işlemesi halinde Direktif uygulanacak, bunun yanı sıra özel bir şirket, yerel kanunlar ile m.3 kapsamında sayılan amaçlar çerçevesinde yetkilendirilirse, özel şirketin işlediği kişisel veriler de 2016/680 sayılı Direktif ile koruma altına alınacaktır[188]. Ancak yetkili merciler Direktif kapsamında kalan suçla mücadele ve suçun kovuşturulması gibi amaçlar dışında veri işlediklerinde işlenen veri yine GDPR kapsamında değerlendirilmelidir. Örneğin kolluk tarafından kullanılan veriler, sağlık veya sosyal hizmetler alanında kullanılmak amacıyla özel bir şirkete transfer ediliyorsa, bu noktada veri transfer rejimi artık suç alanı dışına çıktığından yeniden GDPR hükümleri devreye girecektir. Bunun yanı sıra özel bir şirket, kanunla

---

[186] Bu kısıtlama, ancak temel haklar ve özgürlüklerin özüne dokunmaksızın, demokratik bir toplumda gerekli ve orantılı olacak şekilde gerçekleştirilebilecektir.

[187] Lynskey, Criminal Justive Profiling, ss. 163, 164.

[188] Krzysztof Gartska, "Between Security and Data Protection: Searching for a Model of a Legal Big Data Surveillance Scheme within the European Union Data Protection Framework**", HRBDT Occasional Paper Series**, Kasım 2018, https://www.researchgate.net/publication/329339463_Between_Security_and_Data_Protection_Searching_for_a_Model_of_a_Legal_Big_Data_Surveillance_Scheme_within_the_European_Union_Data_Protection_Framework_2018_HRBDT_Occasional_Paper_Series, Erişim Tarihi: 14.03.2021, s.10.

açıkça görevlendirilmediği takdirde, kolluk faaliyeti kapsamında kalacak bir amaçla veri işlese dahi, 2016/680 sayılı Direktifte belirtildiği üzere yetkili merci olmadığından, bu durumda veri işlenme sürecinde GDPR hükümleri geçerli olacaktır[189]. Dolayısıyla Direktifin uygulanabilmesi için suç işlenmesini önleme ve yargılama faaliyeti gibi sınırlı sayıda belirtilen amaçlar ve yine Direktif kapsamında belirtilen yetkili merci tarafından işlenme şartlarının kümülatif olarak bulunması gerekmektedir.

Bunun yanı sıra hem GDPR hem 2016/680 sayılı Direktif milli güvenlik tesisi amacıyla veri işlenmesi sürecine uygulanamamaktadır. Nitekim Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın m. 4/f. 2 hükmü uyarınca da milli güvenliğe ilişkin hususlar üye devletlerin iç işleyişine ilişkin sorun olarak değerlendirilerek Avrupa Birliği mevzuatı ve yetki alanının dışında bırakılmıştır[190]. Ancak milli güvenlik kavramı, sınırları belirlenmesi ve kamu güvenliği kavramından ayrılması güç bir kavramdır. Nitekim kavramın belirsizliği, üye devletlerin örneğin kimi zaman toplantı ve gösteri yürüyüşlerini "milli güvenlik" kapsamında değerlendirmesi ve bu kapsamda kişisel verilere yönelik müdahalelerin AB mevzuatı dışında kaldığını ileri sürmesi gibi uygulamalara zemin hazırlamaktadır. Bununla birlikte Avrupa İnsan Hakları Mahkemesi, Klass ve Diğerleri/Almanya ve Rotaru/Romanya gibi pek çok kararında milli güvenlik kapsamında kaldığı iddia edilen istihbarat örgütlerinin veri toplamasını değerlendirmiş ve özellikle gizli koruma tedbirlerinin öngörülebilir bir rejimle düzenlenip düzenlemediğini, bunun yanı sıra orantılı ve demokratik bir toplumda gerekli olup olmadığını AİHS m. 8 kapsamında değerlendirerek yetki alanını genişletmiştir[191].

Avrupa Birliği Adalet Divanı da son dönem kararlarında özellikle 2016/680 sayılı Direktifin yürürlüğe girmesinin ardından, ceza adaleti kapsamında veri işlenmesini denetleme yetkisinden yararlanarak kimi zaman milli güvenlik alanında değerlendirilebilecek kanunları incelemektedir. Örneğin Tele2Sverige ve Watson

---

[189] Lynskey, Criminal Justive Profiling, s. 165.
[190] Lynskey, Criminal Justice Profiling, s. 165.
[191] AİHM, Klass ve Diğerleri/Almanya, Başvuru No. 5029/71, Karar Tarihi: 06.09.1978, AİHM, Rotaru/Romanya, Başvuru no. 28341/95, Karar Tarihi: 4.5.2000, aktaran Anna Dimitrova/Maja Brkan, "Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts Before and After the NSA Affair", **Journal of Common Market Studies**, Cilt: 56, Sayı:4, 2018, ss. 751–767, s.761.

kararı ve yine Digital Rights Ireland kararlarında, Divan büyük veri işlenmesi ve veri saklanmasına izin veren yerel kanunların Avrupa Birliği mevzuatı ile uyumlu olup olmadığını detaylı şekilde değerlendirmiştir[192]. Dolayısıyla milli güvenlik alanı AB yetkisi dışında tutulsa da bu istisna kişisel verilerin korunmasına sınırsız bir müdahaleyi mümkün kılan açık bir kart olarak kullanılamayacaktır. Gerek AİHM gerekse Adalet Divanı bu yetkinin hukuk devletine uygun şekilde kullanımını tesis etmek adına gözcülük görevini yerine getirmektedir.

Sonuç olarak ceza muhakemesi alanında profilleme teknolojilerinin kullanılması hem GDPR hem 2016/680 sayılı Direktifin kapsama alanında değerlendirmeyi gerektirmektedir. Nitekim bu süreçte özel şirketlerin işlediği verilerin de ceza muhakemesine dâhil edilmesi söz konusu olmaktadır. Bu alanda devletlerin milli güvenliğini ilgilendiren istihbarat organlarının veri işleme süreci dahi, kişisel verilerin korunması ve demokratik hukuk devletinin gereklerine aykırılık bakımından incelemeye tabiidir. Aşağıda öncelikle GDPR kapsamında profilleme teknolojilerine karşı öngörülen düzenlemeler ardından Direktif bünyesinde yer alan hak ve yükümlülükler ele alınacaktır.

b) Profilleme Teknolojilerine İlişkin GDPR Bünyesinde Yer Alan Düzenlemeler

Profilleme, GDPR bünyesinde 4.maddede "*gerçek bir kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimi"*[193] şeklinde tanımlanmıştır.

Dolayısıyla GDPR kapsamında profillemeden bahsedebilmek için öncelikle otomatik işleme söz konusu olmalıdır. Otomatik işleme, insan eliyle değil, bilgisayar, telefon gibi işlemciye sahip olan cihazlar tarafından ve algoritmalar aracılığıyla

[192] Lynskey, Criminal Justice Profiling, s.166.

[193] Türkçe çeviri için bkz. https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (Erişim Tarihi: 10.10.2020)

gerçekleştirilen işleme faaliyetidir. Otomatik kavramı, makine eliyle işlenmeyi içermekle birlikte otonom kavramından farklıdır. GDPR, insanlar gibi bağımsız ve kendi kendine düşünebilen, başka bir deyişle otonom yapay zekâ eliyle profilleme gerçekleştirilmesini aramamakta, yalnızca, bilgisayar, dijital asistan, radyo frekans tanımlama cihazları gibi pek çok farklı makine aracılığıyla veri işlenmesini aramaktadır[194]. Yine GDPR kapsamında bir profillemeden bahsedebilmek için, kişisel veri söz konusu olmalıdır. Yukarıda kişisel veri kavramı başlığında detaylı şekilde ele alındığı üzere, günümüzde, ilk başta belirli bir kişiye işaret etmeyen veriler üçüncü kişinin işlediği verilerle birleştirildiğinde, kişi hakkında belirlenebilir enformasyon elde edilmesi mümkün hale gelmiştir. Bu nedenle klasik anlamda anonim veri-kişisel veri ayrımı gittikçe aşınmakta, bir verinin kişisel veri olup olmadığı daha geniş bir değerlendirme yapılmasını gerektirmektedir. Eğer başvurulan profilleme teknolojilerinin kullanılma amacı, bireyleri tespit etmeye elverişli bilgi edinmek ise veya yapılan profilleme ile kişiye diğerlerinden farklı davranılmasına yol açacak bir sonuca varılıyorsa, kullanılan veriler henüz belirli bir kişiye işaret etmese dahi GDPR koruması gündeme gelebilmektedir. Yine otomatik işleme yöntemleri ile "makul kabul edilebilecek bir çabayla" kişinin kimliği tespit etmek mümkünse veya kişi üzerinde sonuç doğuracak kararlar alma mümkün ise yine GDPR kapsamında hakların gündeme gelebileceği bir profilleme söz konusudur. Aksi halde, kullanılan verilerin doğruluğunun ve hukuka uygun işlenip işlenmediğinin kontrolü mümkün olmayacaktır[195]. Son olarak ilgili tanımda yalnızca kişisel veriden bahsedilmekle birlikte, bu veri bizzat ilgili kişinin verisi olmak zorunda değildir. Kuşkusuz bu veri, sürecin sonunda kişi ile ilişkilendirilebilir ve onun özelliklerini gösterebilir nitelikte bir veri olmalıdır. Ancak üçüncü kişiye ait veriler de profilleme sırasında kullanıldığından, tüm profilleme sürecinin yalnızca bir kişiye ait kişisel verilerden ibaret olması şeklinde bir yorum hatalı olacaktır[196].

Son olarak, ilgili tanımda profillemenin amacı gerçek kişilerin bireysel özelliklerinin tespit etmek olarak gösterilmiştir. Dolayısıyla profilleme teknolojilerini

---

[194] Otonom ve otomatik kavramları arasındaki fark için bkz Hildebrandt, "Defining Profiling: A New Type of Knowledge?", s.26-29.

[195] Tene Omar/ Polonetsky Jules, "Big Data for All: Privacy and User Control in the Age of Analytics", **Northwestern Journal of Technology and Intellectual Property**, Cilt: 11, Sayı: 5, 2013, s.258.

[196] Kuner, Christopher/ Bygrave, A. Lee/ Docksey, Christopher (Eds), **The EU General Data Protection Regulation (GDPR): A Commentary**, Oxford University Press: Oxford, 1. Baskı, 2020, s.533, 534.

ayırt eden unsur, yalnız kişisel verilerin toplanmasından ibaret olmamasıdır, verilerin bireysel özellikleri tespit etmek adına analiz edilmesi söz konusudur[197]. Bununla birlikte GDPR m.22'deki özel düzenleme bireylerin yalnız analiz edilmesini değil bu analize dayanarak haklarında karar alınmış olmasını da aramaktadır. Oysa profilleme teknolojilerinin kullanıldığı her durumda, kişiler hakkında analiz yapılmakla birlikte, bu analizlerden yola çıkılarak mutlaka kişi hakkında bir karar alınması veya kişinin bir yaptırıma maruz bırakılması zorunlu değildir. Ancak GDPR, yapılan profillemenin ardından kişi hakkında önemli bir etki doğuran bir karar alındığı halleri düzenlemekte, bu kararın tamamen otomatik ve insan kontrolünden bağımsız bir şekilde alınmasını engellemek istemektedir. Böylelikle kişileri salt otomatik sistemlerle bir nevi "nesne" gibi değerlendiren ve sosyal yaşamı doğrudan etkileyen kararların denetimsiz sonuçlar doğurması engellenmek istenmiştir. Bu amaçla GDPR kapsamında 22. madde ile profilleme de dâhil olmak üzere yalnızca otomatik karar mekanizmalarına dayanılarak alınan ve hukuki veya ciddi şekilde etki doğuran kararlara karşı ilgili kişinin itiraz edebilmesi mümkün kılınmıştır[198].

Elbette kişilerin salt otomatik şekilde profilleme ile alınan kararlara karşı itiraz edebilmesi için öncelikle verilerinin işlendiğini bilmeleri, haklarında verilmiş hukuki veya benzer nitelikte ciddi bir etki doğuran karardan haberdar olmaları gerekir. Yine bu karara itirazın anlamlı olabilmesi için, profillemenin nasıl işlediği ve kararın ne şekilde alındığını anlayabilmeleri gerekir. Nitekim bu nedenle GDPR kapsamında 13. ve 14. maddeler ile veri sorumlusunun bilgilendirme yükümlülüğü, bunun yanı sıra 15. madde ile ilgili kişinin erişim hakkı düzenlenmiştir. Böylelikle profilleme sürecinde ilgili kişinin haklarını gerçek anlamda kullanabilmesini mümkün kılan hükümler açıkça öngörülmüştür. Ancak özellikle derin öğrenme ağları gibi teknolojilerin kullanıldığı durumlarda, profilleme yazılımlarının işleyişi "kara bir kutu" içerisinde yürümekte, kararların ne şekilde alındığını değerlendirmek, teknik donanıma sahip olmayan kişiler, hatta bizzat yazılımları üreten kişiler için bile güç olabilmektedir. Bunun yanı sıra suçla mücadele için gizliliğin gerekliliği veya yazılımcının patent hakları, profilleme mekanizmalarının nasıl işlediğinin açıklanmasının önüne geçebilmektedir.

---

[197] Article 29 Data Protection Working Party, **Guidelines on Automated individual decision-making and Profiling for the Purposes of Regulation 2016/679**, 2017, s.6,7, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (Erişim Tarihi: 11.10.2020).
[198] Aşıkoğlu, s.153.

Tüm bu engellere rağmen, erişim ve bilgilendirmeye dair belli haklar kullanılabilir ve profilleme gerçekleşmeden önce dahi ilgili kişi belirli müdahalelerde bulunulabilir. Ancak kimi durumda, kullanılan veriler güncel ve doğru olsa, bunun yanı sıra başvurulan yazılım şeffaf bir kodla yazılmış olsa dahi varılan nihai sonuç hukuka uygun olmayabilir. Bu nedenle profilleme ile varılan sonuçların ve bu sonuçlara dayanarak gerçekleştirilen uygulamaların hukuk devletinde meşruiyeti ayrıca sorgulanmalıdır. Kişisel verilerin korunmasına ilişkin normların, profilleme sonucu ortaya çıkan "türetilmiş verilerin" hukuka uygunluğu denetlemede yeterli olup olmadığı tartışmalıdır. Bu tür verilere dayanılarak alınmış kararların şekil kadar esas yönünden incelenmesi de elzemdir[199]. Yine bu tür kararların ayrımcılık yasağı, masumiyet karinesi gibi temel ilke ve haklarla çatışıp çatışmadıkları ve toplumsal yaşam üzerine etkileri değerlendirilmelidir.

Bu nedenle aşağıda öncelikle profillemenin ilk ayağını oluşturan veri toplama aşamasına ilişkin GDPR m. 5 ve m. 6 değerlendirilecek, hangi ilkeler ve şartlar altında kişi ve gruplara ilişkin veri toplamanın hukuki olduğu ele alınacaktır. Veri toplamanın ardından kişilere ilişkin profil oluşturulması ve bu profillere dayanılarak kişiler hakkında alınan kararların uygulanması aşaması değerlendirilecek ve bu aşamada GDPR 22. maddede düzenlenen kişinin kendisi ile ilgili hukuki veya benzer şekilde önemli sonuçlar doğuran ve salt otomatik işleme faaliyetine dayalı kararlara tabi olmama hakkı ele alınacaktır. Son olarak bu haklara başvurulmasını mümkün ve anlamlı kılan şeffaflık hakları ele alınacaktır. Bu başlık altında ilgili kişinin veri işleme süreci hakkında bilgilendirilmesini düzenleyen GDPR m. 13 ve 14 ile verilere erişimi mümkün kılan m. 15 değerlendirilecektir. Son olarak günümüzde GDPR kapsamında yer alan tüm bu hakların profilleme teknolojilerine karşı şirketler ve hükümetler karşısında güçsüz taraf olan bireylerin korunması için yeterli olup olmadığı değerlendirilecektir.

[199] Wachter/ Mittelstandt, "A Right to Reasonable Inferences", s.504.

aa) Profillemenin İlk Aşamasına İlişkin Düzenlemeler: GDPR Kapsamında Veri Toplama Sürecinin Hukukiliği ve Veri İşlenmesine İlişkin Temel İlkeler

Profilleme teknolojileri ile veri işleme sürecinin ilk aşaması olan veri toplama süreci sonraki aşamaların hukuka uygun kabul edilebilmesi için oldukça önem taşımaktadır. Her ne kadar profillemeye ilişkin temel düzenlemeler, profilleme teknolojilerinin sevk edilmesinden sonra alınan kararlara yönelik olsa da bu sürecin ilk ayağını oluşturan veri toplama kısmına uygulanacak normların da tartışılması gereklidir.

aaa) Veri İşlemenin Hukuki, Adil ve Şeffaf olması ilkesi

Bu süreçte uygulanacak temel ilkeler GDPR madde 5'te gösterilmiştir. Madde 5/1 (a) bendi en temel prensipler olan veri işlemenin hukuki, adil ve şeffaf olmasının gerekliliğini vurgulamaktadır. Veri işlemenin hukukiliği ilkesi 6. maddede daha detaylandırılmış, hangi koşullarda veri toplama zemininin meşru sayılacağı bu maddede açıkça sayılmıştır. Buna göre kişisel veriler ancak verisi işlenen ilgili kişinin onayı, veri sahibinin taraf olduğu bir sözleşmenin ifası ve uygulanması için veri işlemenin gerekli olması, veri sorumlusunun yasal bir yükümlülüğünü yerine getirmesi, ilgili kişi veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusunun resmi yetkisini kullanabilmesi, veri sorumlusunun ilgili kişinin hak ve menfaatlerinden üstün bir meşru amacı olması halinde işlenebilir. Sayılan bu amaçlar arasında hiyerarşik bir üstünlük yoktur, başka bir deyişle hiçbir amaç diğerinden daha üstün ya da daha meşru değildir[200].

Bununla birlikte veri işleme sürecinin hukuki olması, yalnızca veri işlemenin 6. maddede sayılan amaçlardan birine dayanması ile sınırlı değildir. Hukuki işleme için Avrupa Birliği Temel Haklar Şartı madde 52/1 ve Avrupa İnsan Hakları Sözleşmesi m. 8/1 de dikkate alınmalı, veri işleme sürecinin ilgili öngörülebilir bir düzenlemeye

[200] González/ De Hert, s. 599.

ve meşru bir amaca dayanmasının yanı sıra, demokratik bir toplumda gerekli ve orantılı olması gerektiği de göz önünde bulundurulmalıdır[201].

GDPR 5. maddede öngörülen veri işleme sürecinin adil olması ilkesi ise verinin kişinin kandırılması gibi hukuka aykırı yöntemlere dayanmadan veya bilgisi dışına çıkmadan işlenmesini gerektirir. Bu ilkenin gerçekleştirilmesini mümkün kılan ve GDPR m.22 kapsamında daha detaylı ele alınacak olan diğer ilke ise verinin şeffaf şekilde işlenmesidir. GDPR 39. gerekçe maddesinde bu ilke, gerçek kişilere kendileri ile ilgili veri topladığını, bu verilerin işlendiğini ve bu işlemenin hangi ölçekte gerçekleştiğini veya gerçekleştirileceğini şeffaf şekilde gösterme şeklinde açıklanmıştır. Bu şeffaflığın kişiyi açık ve anlaşılır şekilde bilgilendirme ve hakkında toplanan veriye erişimini sağlama ile tesis edileceği vurgulanmıştır[202]. Aksi halde kişilerin veri işleme sürecindeki risklerden haberdar olması ve kişisel verilerinin korunmasına ilişkin haklarını talep etmeleri mümkün olmayacaktır.

bbb) Belirli, Açık, Meşru Amaçla Veri İşleme İlkesi

Amaca uygun olma ilkesi kişisel verilerin korunması mevzuatının köşe taşı ilkelerinden biri olup, diğer pek çok ilkenin uygulanabilmesini de mümkün kılmaktadır. GDPR m.5/1 (b) bendinde düzenlenen bu ilkeye göre kişisel verilerin belirli, açık ve meşru amaçlarla toplanması ve bu amaçlara uygun şekilde işlenmesi gerekir. Başka bir deyişle, verilerin ne amaçla işleneceğine sürecin en başı olan veri toplama aşamasında karar verilmiş olmalıdır[203]. Henüz veri toplanmadan önce veri toplama amacının belirli olması, aslında ilgili kişiden ziyade veri sorumlusunun oto-regülasyonuna ilişkin bir unsurdur. Veri sorumlusunun veri işlemeden önce neden veri topladığına karar vermesini ve bunu net bir şekilde belirlemesini gerektirir. Nitekim veri toplamaya başlamadan önce veri toplama amacının net bir şekilde bilinmesi, hangi verilerin bu amaç kapsamında gerekli olduğunu ve hangi verilerin veri toplama süreci dışında bırakılması gerektiğini tespit edebilmeyi sağlayacaktır. Bu nedenle bu aşamada "pazarlama amaçlı" veya "gelecek araştırmalarda kullanılmak üzere"

---

[201] European Union Agency for Fundamental Rights, **Handbook on European Data Protection Law,** Publications of European Union: Luxembourg, 2014, ss.64-67.
[202] Recital 39 EU GDPR, https://www.privacy-regulation.eu/en/recital-39-GDPR.htm, Erişim Tarihi: 22.03.2021.
[203] Kuner/ Bygrave/ Docksey, s.315.

şeklinde net sınırlarla çizilmemiş hedefler, amaç sınırlaması ilkesini ihlal edecektir. Bununla birlikte veri toplama amacının hangi durumlarda belirli kabul edileceğinin sınırı, veri işleme sürecinin bağlamına ve bu süreçten etkilenecek kişi grubuna göre de değişecektir. Bu noktada en önemli husus, verileri toplanacak kişilerin, kendileri ile bu amaç paylaşıldığında, verilerinin neden ve nasıl işleneceğini anlayabileceği netlik ve öngörülebilirlikte bir amacın belirlenmesidir. Amacın anlaşılır şekilde ortaya konulması, ortalama bir kişinin bu amacı anlayabilmesi şeklinde yorumlanmalıdır[204]. Veri sorumlusu birden fazla amaçla veri işleyecek ise tüm bu amaçlar ayrı ve belirli şekilde ifade edilmelidir. Birden fazla amaçla veri işlemek mümkün olmakla birlikte, bu amaçların belirli olması zorunludur. Bu durum özellikle büyük veri üzerinden sınırsız bilgi üretme potansiyelini barındıran teknolojileri kısıtlamak adına büyük önem arz etmektedir[205]. Veri toplama amacının açık olması ise veri toplama işlemine başlandığında, amacın ilgili kişilere anlaşılır şekilde ifade edilmesini gerektirir. Amacın açıklığı, veri işleme sürecinin şeffaflığı ve verisi işlenen ilgililer tarafından sürecin öngörülebilir olması açısından önemlidir. Son olarak veri işleme amacı, GDPR m. 6 kapsamındaki meşru veri işleme amaçlarına dayanmalı ve daha genel bir bakışla, tüm kişisel verileri koruma mevzuatı ve diğer mevzuat açısından hukuka uygun olmalıdır[206].

ccc) Amaca uygunluk ilkesi

Amaca uygunluk ilkesi, yalnız veri toplama aşamasında değil, sonraki aşamalarda da ilk tespit edilen amaçla uyumlu bir şekilde veri işlemeyi gerektirir. Bununla birlikte "uyumlu amaç" kavramından neyin anlaşılması gerektiği uygulamada çeşitli soru işaretleri doğurabilir. Bu nedenle GDPR m. 6 f. 4 kapsamında hangi amaçların veri toplama sırasında belirlenen amaçla uyumlu sayılacağına ilişkin belirli kıstaslar öngörülmüştür.

Buna göre AB mevzuatında veya üye devletlerin yerel mevzuatları ile 23. maddedeki kamu güvenliği, suçla mücadele, kamu yararına vergi toplanabilmesi,

---

[204] Hannes Westermann, **Change of Purpose: The effects of the Purpose Limitation Principle in the General Data Protection Regulation on Big Data Profiling**, Lund Üniversitesi Hukuk Fakültesi, Yüksek Lisans Tezi, 2018, s.46, 47.

[205] Jonas Breyer, "Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-GVO", **Datenschutz und Datensicherheit**, Cilt:42, Sayı:5, 2018, ss.311-317, s.313.

[206] Westermann, s.47, 48.

sosyal güvenlik haklarının tesis edilebilmesi gibi amaçlarla, demokratik bir toplumda gerekli ve orantılı müdahale içeren bir norma dayanarak veri işlendiği takdirde ikincil amaç ilk amaçtan farklı olabilir. Bunun yanı sıra GDPR ile getirilen diğer bir yenilik, ilgili kişinin veri işleme amacı değiştiği takdirde bundan haberdar edilmesi ve ilgili kişinin onay vermesi halinde ikincil amacın uyumlu ve hukuka uygun kabul edilmesidir[207]. Eğer bu iki durum söz konusu değil ise yine GDPR m.6 f. 4 gereği, kişisel verilerin toplanma amaçları ile planlanan diğer işleme amaçları arasında bağlantı bulunmalı, veri toplama sürecinin arka planı ve bağlamı, veri işleyen ve ilgili kişi arasındaki ilişki gözetilerek değerlendirilmelidir. Yine bu değerlendirme sırasında işlenen verinin niteliği; özel nitelikli mi yoksa hassas olmayan kişisel veri mi olup olmadığı dikkate alınmalı, ileriki safhalarda veri işlemenin ilgili kişi üzerindeki etkileri ve bu süreçte yeterli önemlerin alınıp alınmadığı gözetilmelidir[208]. İleriki aşamalarda ortaya çıkan amaçların uyumluluğu, ikincil amacın, ilk amacın bir nevi "alt başlığı" olmasını gerektirmez. Ancak sonradan ortaya çıkan amaçlar, verisi işlenen kişinin hayatın olağan akışında öngörebileceği şekilde ilk amaçla ilişkili olmalıdır. Bununla birlikte, gerçekleştirilecek veri işlemenin kişiler üzerinde doğuracağı etki de dikkate alınmalı, yeni amacın "uyumlu amaç" kabul edilebilmesi için bir risk değerlendirilmesi yapılmalı ve ikincil amaç ilk amaca ek, yeni risklere yol açmamalıdır. Bununla birlikte GDPR m. 5 f. 2 gereği yine GDPR m. 89'da sayılan amaçlarla yeniden veri işlendiği durumlarda, veri işlemenin de facto şekilde ilk amaçla uyumlu kabul edildiği görülmektedir. Gönderme yapılan 89. maddeye göre, kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veri işleme faaliyetleri bu tür doğrudan ilk amaçla uyumlu amaç olarak değerlendirilecektir. Ancak bu istisnai durumlarda dahi, asgari veri işleme ilkesine ("data minimisation") riayet edilmeli, takma isim kullanarak ve hatta veri öznesini anonim hale getirmeye elverişli teknik yöntemlere başvurulmalıdır [209]. Uygulamada profilleme teknolojileri ile büyük veri analizi yapan kimi şirketler istatiksel amaçlar istisnasına başvurarak amaç sınırını aşmaya çalışmaktadır. Ancak bu noktada dikkat edilmesi gereken husus, GDPR 162. gerekçesinde de belirtildiği üzere istatistik oluşturma istisnasına belli kişileri etkileyen kararlar alma amaçlandığı takdirde başvurulamayacağıdır. Başka bir deyişle, belli kişileri diğerlerinden ayırt etmeye

[207] Westermann, s.56.
[208] Kuner/Bygrave/Docksey, s.316, Aksoy Retornaz/Güçlütürk, s.298.
[209] Kuner/ Bygrave/ Docksey, s.341, 342.

elverişli ve bu kişilere yönelik farklı uygulama ve kararlar almayı mümkün kılan büyük veri analizi teknolojileri, istatistiksel amaç kapsamında değerlendirilemez[210].

Özellikle pek çok kaynaktan beslenen profilleme teknolojileri açısından amaç sınırı büyük önem taşımaktadır. Profilleme teknolojileri kullanılmadan önce veri toplama aşamasında ne amaçla veri toplanacağı ve profilleme ile hangi sonuçlara varılmak istendiğinin baştan tespiti önem taşımaktadır. Bununla birlikte veri toplama kavramı dar yorumlanmamalıdır. Örneğin büyük veri üzerinden kişinin yaşı, tercihleri ve diğer özelliklerinin tespiti de "türetilmiş" yeni bir veri toplama kapsamındadır. Bu nedenle türetilmiş veriler, birincil verilerin uzantısı olarak kabul edilmemeli, eğer türetilmiş veriler yeni bir amaca hizmet ediyor ise amaç sınırlaması kuralına aykırı kabul edilmelidir. Bununla birlikte, bu tür teknolojilerine başvuran büyük şirketler, veri toplama amaçlarını çok geniş tutarak türetilmiş verileri de aynı amaç çerçevesinde toplamaya ve işlemeye devam etmektedir. Bu bağlamda örneğin "kişiye özel reklam yapabilme amacıyla profilleme yapılması" amacı belirli ve açık bir amaç teşkil etmez. Nitekim bu amaçla hangi verilerin neden toplandığı ve bu veriler arasında ne tür bağlantılar kurulacağı ilgili kişi açısından açık değildir. Ayrıca bireyselleştirilmiş reklam uygulaması gibi geniş bir amaçla uygulanan profilleme teknolojileri aracılılığıyla kişilerin sağlık durumu, özel hayatı, cinsel yönelimleri gibi beklenmedik verilere ulaşılması mümkün olabilmektedir. Bu nedenle profilleme teknolojileri açısından amaç daha da belirgin olmalı, ilgili kişiye örneğin "Konum bilgileri, ziyaret edilen siteler ve tıklanan linkler yaş, cinsiyet ve ilgi alanlarını belirlemek amacıyla kullanılacaktır." şeklinde açık bir amaç sunulabilmelidir[211]. Yine örneğin Facebook gibi sosyal medya kurumlarının, kişilerin arkadaşlarıyla fotoğraflarını paylaşabilmesi amacını sunarak fotoğraf verilerini işlemesi, amaç sınırlaması ilkesine uygun olmakla birlikte, bu fotoğrafların kişinin yaşını tespit etme, kişiye özgü reklamların gösterme gibi hedeflerle profilleme yapmak üzere kullanması ilk amaçla uyumlu olmayan bir amaç teşkil edecektir. Dolayısıyla amaca uygunluk ilkesi, öncelikle sınırsız sayıda veri toplayıp ardından bunları analiz etmeye yönelmiş pek çok şirketin ve kuruluşun bu uygulamalarını hukuka aykırı kıldığı büyük önem taşımaktadır. Özellikle ceza muhakemesi kapsamında verilerin kişiler veriler hukukuna uygun şekilde

[210]Bkz, GDPR Gerekçe 162, https://www.privacy-regulation.eu/en/recital-162-GDPR.htm, Erişim Tarihi:25.03.2021, aynı yönde bkz Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data", **Seton Hall Law Review**, Cilt: 47, 2017, ss.995-1020, s.1008.
[211] Westermann, ss. 52, 53.

toplanılması, hukuka aykırı delil başlığı altında inceleneceği üzere, bu verilerin ceza muhakemesinde kullanıp kullanılamayacağının tespitinde özel bir önem arz etmektedir.

ddd) Asgari Veri İşleme İlkesi

GDPR 5. maddede düzenlenen diğer bir ilke 5/1 (c) bendindeki asgari veri işleme ilkesidir. Bu ilke gereği, veri işleme sırasında, belirlenen amacın gerektirdiği ölçü ve gereklilikte veri işlenmelidir. Bu ilke işlenen kişisel verilerin yalnız niceliğini değil niteliğini de ilgilendirir. Örneğin iş başvurusunda kişiden uyuşturucu kullanıp kullanmadığına dair veri talep etme, istenen verinin niteliği ve önemi gereği veri işleme amacına ulaşmada ölçüsüz nitelikte bir veridir. Dolayısıyla asgari veri işleme ilkesi, amaç dışında ek veri veya niteliği gereği ölçüsüz veri işlememeyi gerektirir[212]. Bu ilke aynı zamanda, veri depolamanın sınırlılığı ile bağlantılı olup işlenen verilerin amacı dışında tutulmasını ve saklanmasını engellemektedir[213]. Bu ilke, günümüzde maksimum veri ile daha doğru analiz yapılacağı iddiasına dayanan büyük veri uygulamalarına önemli bir sınırlama getirmektedir. Sürekli veri etkileşime dayanan nesnelerin internetinin hızla güç kazanırken, asgari veri işlemenin bu teknolojilerin doğru sonuçlara varmasına engel olacağı karşı görüşüne rağmen[214], bu ilke kişilerin verileri üzerinde hâkimiyetlerini kaybetmemeleri için ödün vermeyi gerektirmektedir. Bu nedenle yeni teknolojilerin uygulama modeli olarak en az veri ile en etkin işleyişe sahip olmayı mümkün kılacak şekilde tasarlanmaları, GDPR kapsamındaki düzenlemeler uyarınca zorunluluk arz etmektedir [215]. Son olarak bu ilke, veri işleme amacına ulaşılmasına rağmen veri saklanmasının önüne geçmesiyle, bu verilerin hacklenmesi ve çalınması tehlikesine karşı, veri güvenliğinin tesis edilmesi açısından da önem taşımaktadır[216].

---

[212] Aksoy Retornaz/Güçlütürk, s. 296.
[213] Kuner/Bygrave/Docksey, s.317.
[214] Bu görüşte olan Hildebrandt, asgari veri kullanma ilkesinin profilleme teknolojilerinin doğru sonuçlar vermesini engelleyeceğini, asgari veri kullanmak yerine taraflar arasındaki bilgi asimetrisini en aza indirmenin ve profillemeye karşı haklarını ileri sürmelerini mümkün kılmanın daha yerinde olduğunu belirtmektedir, bkz. Mireille Hildebrandt, "Who is Profiling Who? Invisible Visibility", İçinde **Reinventing Data Protection**, Ed: Serge Gutwirth/Yves Poullet/Paul de Hert/Cécile de Terwangne/Sjak Nouwt, Springer: Dodrecht, Haziran 2009, ss.249-252, s.251.
[215] Wachter, "Normative challenges of identification in the Internet of Things", s.446
[216] Zarsky, s.1010.

eee) Doğru Veri işleme ilkesi

GDPR m. 5/1 (d) bendinde ele alınan bu ilkeye göre işlenen veriler veri işlemenin tüm sürecinde doğru ve güncel olmalıdır. Özellikle veri toplama aşamasında verilerin hatalı olması, tüm süreci baştan etkileyecek ve bu veriler üzerinden tekrar türetilen verilerle söz konusu hataların katlanarak artma riski ortaya çıkacaktır. Bu nedenle doğru olmayan verilerin düzeltilmesi veya silinmesi büyük önem taşır. Bununla birlikte yalnızca belirli bir kişiye ait verilerin düzeltilmesi özellikle profilleme sistemleri açısından yeterli değildir. Makine öğrenmesi ile verileri süzerek bağlantılar kuran profilleme teknolojileri, öğrenme sırasında hatalı verilerle eğitildiğinde, kaçınılmaz olarak hatalı sonuçlara varabilir. Bu durumda yalnızca bireysel olarak verilerin düzeltilmesinin talep edilmesi sistemsel bir sorun haline gelen hatalı öğrenme sürecinin önüne geçmede yetersizdir. Nitekim COMPAS gibi kişilerin tekrar suç işleme potansiyeli barındırıp barındırmadıklarını tespit eden profilleme sistemleri, uzun yıllar sonucu toplanmış taraflı verilere dayanarak oluşturulmuş ve neticesinde siyahi kişileri daha yüksek tekerrür suçlu riski oluşturan kişiler olarak kategorize etmiştir. Bu durumda ilgili kişi hakkında varılan hatalı sonuç, kişinin kendi verilerinin hatalı olmasından değil, üçüncü kişilere ait verilerin de taraflı şekilde toplanmış olmasından kaynaklanmaktadır. Bu noktada, ilgili kişinin bireysel haklarına başvurması, profilleme teknolojilerinin dayandığı tüm verilen "tehlikeli" puanının yanlışlığını tartışmaya açamayacaktır. Bunun yanı sıra, ilgili kişi hakkında profillemenin ardından varılan sonuç (kişinin tekrar suç işleyeceği bilgisi) henüz gerçekleşmediğinden, varılan kararın doğruluğu ya da yanlışlığını iddia etmek mümkün değildir. Böyle bir durumda ilgili kişinin karşılaştığı sorunu GDPR m. 5 f. 1 (d) bendindeki verilerin doğruluğu ilkesinden hareketle çözmesi mümkün değildir, nitekim kişilerin kendi verileri üzerindeki bireysel hakları ile profilleme sistemini ve sistemi eğitmede kullanılan üçüncü kişilere ait verilerin taraflılığını tartışmaya açması mümkün değildir[217]. Bu nedenle profilleme teknolojileri karşısında bireysel hakların ötesine geçen düzenlemelere ihtiyaç duyulmaktadır. Bu tartışma profilleme de dâhil olmak üzere münhasıran otomatik karar almayı düzenleyen 22. maddenin ele alındığı aşağıdaki bölümde tekrar ayrıntılarıyla değerlendirilecektir.

[217] Michael Butterworth, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework", **Computer, Law and Security Review**, Cilt: 34, 2018, ss. 257–268, s.261, 262.

bb) Profillemenin Analiz ve Karar Alma Aşamasına İlişkin GDPR Kapsamındaki Düzenlemeler

aaa) GDPR madde 22: Yalnızca Otomatik İşleme Faaliyetine Dayalı Karara Tabi Olmama

Toplanan büyük verilerin analizi ile oluşturulan profiller ve bu profillere dayanan karar alma sürecinde, devlet ve özel kurumların kontrolünde işleyen bu süreçte bireyler gölgede kalmakta, sürecin öznesi olamamaktadır. Bu nedenle veri toplamanın düzenlenmesi, bu verilerin analiz edilmesi ve analizlerin kararlara dönüştürülmesini sınırlayan hukuki düzenlemelerin yapılması büyük önem taşımaktadır. Nitekim Avrupa Birliği Komisyonu, 1993 tarihinde yapay zekâ ve profilleme teknolojilerinin gelişim hızı karşısında, insanların tamamen otomatik şekilde alınan kararlara tabi olabileceğine dair çekincesini dile getirmiş[218], bu çekinceler ışığında GDPR kapsamındaki düzenlemenin öncüsü olan 1995 tarihli Kişisel Verilerin Korunması Direktifi bünyesinde otomatik karar alma süreçlerine dair haklar öngörülmüştür[219]. Bu dönemde yayınlanan açıklayıcı raporlarda, profillemeye ilişkin düzenlemenin ardında yatan ihtiyacın, otomatik sistemlerin hata yapma ihtimaline dair duyulan kuşkudan ziyade, insanların geleceklerini tayin eden kararların "verilerinin gölgesinden" yola çıkan makinelerce alınmaması, başka bir deyişle makinelere karşı insan onurunun korunması olduğu görülmektedir[220]. GDPR kapsamında 22. madde ile öngörülen düzenlemenin ardında da bu amaçlar yatmakta, bunun yanı sıra 71. gerekçe maddesi ile verilerdeki muhtemel hataların profilleme teknolojileri ile katlanarak artma ihtimali ve yine ayrımcılığa yol açan sonuçların doğma ihtimaline de ayrıca dikkat çekilmektedir[221].

---

[218] Comission of European Communities, **Amended Proposal for a Council Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data**, COM(92) 422 final—SYN 287, 15.10.1992, https://aei.pitt.edu/10375/1/10375.pdf, Erişim Tarihi: 11.04.2021, s.26

[219] İlgili Direktif için bkz. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, Official Journal of the European Communities No: L 281/31, 23.11.1995.

[220] Isac Mendoza/Lee A. Bygrave, "The Right Not to be Subject to Automated Decisions Based on Profiling", 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855 Erişim Tarihi: 11.04.2021, s.84.

[221] GDPR 71. Gerekçe, https://www.privacy-regulation.eu/en/recital-71-GDPR.htm, Erişim Tarihi: 11. 04.2021.

GDPR 22. maddenin metni içerik olarak değerlendirildiğinde, ilk paragrafta yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkının düzenlendiği, ikinci paragrafta otomatik karar alma sürecine dair bazı istisnalar tanındığı, üçüncü paragrafta ise bu istisnaların söz konusu olduğu durumlarda hangi önlemlerin alınması gerektiği düzenlenmektedir. Son paragraf ise profilleme sonucu oluşabilecek ayrımcı uygulamalara karşı önlem olarak hassas nitelikli verilere dayalı karar alınmasını yasaklayan bir düzenleme içermektedir[222].

aaaa) GDPR m. 22'nin Hukuki Niteliği

Her ne kadar 22. maddenin ilk fıkrası "veri sahibinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dâhil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı" şeklinde "hak"tan bahsetse de bu maddenin bir hak mı yoksa yasak mı öngördüğü tartışmalara yol açmaktadır. Bu tartışma, yalnızca doktrinle sınırlı bir tartışma olmadığı, uygulamayı doğrudan etkilediği için üzerinde ayrıca durulmalıdır. Nitekim 22. maddenin bir hak olarak kabul edilmesi durumunda, bu madde ancak hak sahibinin talebi halinde uygulanabilecekken, bu maddenin salt otomatik yollarla karar alınmasını yasaklayan bir madde olarak kabul edilmesi halinde ilgili koruma, veri sorumluları tarafından re'sen tesis edilecektir. Dolayısıyla bu maddenin "bir hak" olarak kabulü, koruma alanını daraltmaktadır. Bu tartışmayı çözümleyebilmek adına öncelikle maddenin amacı ve GDPR bünyesinde düzenlendiği yer ele alınmalı, ardından maddedeki tüm fıkralar bir arada okunmalıdır.

Maddenin amacı öncelikli olarak insan onurunun, verilerin gölgesine ve makinelerin insafına terk edilmeksizin korunmasıdır. Amaççı yorumla, madde ile re'sen otomatik profilleme ve karar almanın önüne geçilmek istendiğini söylemek daha yerinde olacaktır. Bununla birlikte madde GDPR bünyesinde kişinin haklarını düzenleyen Üçüncü Bölüm altında yer almaktadır. Ancak daha detaylı bir okuma yapıldığında, bu bölümde sistematik bir ayrıma gidilmediği ve haklar kadar 13. ve 14. maddede olduğu gibi veri sorumlusuna dair yükümlülüklerin de aynı bölümde öngörüldüğü dikkate alınmalıdır[223]. Ayrıca 22. maddenin başlığı, bu bölümde

[222] Mendoza/Bygrave, s. 85.
[223] Kuner/ Bygrave/Docksey, s.531.

düzenlenen “itiraz hakkı”, “veri taşınabilirliği hakkı” gibi maddelerden farklı olarak “hak” ifadesini barındırmamakta, “profil çıkarma da dâhil olmak üzere otomatik münferit karar verme” şeklinde düzenlenmektedir. Son olarak ilgili madde bütün olarak daha detaylı ele alındığında, ikinci fıkrada sayılan “sözleşme yapılması veya uygulanması için gerekli olma”, “Avrupa Birliği veya üye devlet hukukun çerçevesinde izin verilmiş olma” veya “veri sahibinin açık rızasına dayanma” istisnaları söz konusu olduğunda kişiler hakkında salt otomatik işleme faaliyetlerine dayanan karar almaya cevaz verildiği görülmektedir. Ters anlamıyla, bu istisnalar hariç kişiler hakkında önemli sonuçlar teşkil edecek kararların salt otomatik şekilde alınması yasaklanmıştır[224].

Dolayısıyla 22. madde hukuki niteliği gereği yasak koyucu bir madde olarak ele alınmalı ve ikinci fıkrada sayılan istisnalar hariç kişiler hakkında salt otomatik şekilde profilleme de dâhil otomatik karar alınması yasak olarak değerlendirilmelidir. Nitekim bu yorum, insan onurunu koruma ve kişisel verileri yeni teknolojiler karşısında savunmasız bırakmama amacıyla daha uyumlu ve daha etkin bir koruma tesis edilmesini mümkün kılacaktır[225].

22. maddenin içeriği daha detaylı değerlendirildiğinde, maddenin uygulanması için üç temel koşul arandığı görülmektedir. Bunlardan ilki, kişi hakkında bir kararın alınması, ikincisi bu kararın sadece otomatik veri işleme faaliyetine dayanması ve üçüncüsü ise bu kararın kişi üzerinde hukuki veya benzer nitelikte önemli bir etki doğurmasıdır. Bununla birlikte, her üç koşul da çeşitli belirsizlikler içermektedir. Aşağıda ilgili şartlar daha detaylı şekilde değerlendirilecektir.

bbbb) Kişi Hakkında Bir Karar Alınması

22. maddenin uygulama alanı bulabilmesi için öncelikle kişi hakkında bir karar alınmış olması gereklidir. Bununla birlikte “karar” dan ne anlaşılması gerektiği GDPR kapsamında belirtilmemiştir. Karar kavramı salt hukuki bir kararı içermese de en azından bağlayıcı etkiye sahip olmalıdır. Nitekim 4. maddede tanımlandığı üzere, her profilleme faaliyeti bir karar alma içermemektedir. Profilleme daha ziyade, verilerin

[224] Mendoza/Bygrave, s. 85, 86.
[225] Mendoza/Bygrave, s.87.

gruplandırıp aralarında bağlantı kurularak bilgi üretilmesini içerir. 22. maddedeki "karar" kavramı, bu anlamda maddenin ne zaman uygulanacağına dair bir sınırlandırma getirmekte, profilleme veya otomatik işleme sonucu, varılan bilgilere dayanılarak bir karar alınması gerektiğini vurgulamaktadır[226]. Ancak karar kavramı, hukuki anlamda yalnızca yetkili kamu otoritelerince alınan bağlayıcı kararlar ile sınırlı tutulmamakta, çok daha geniş anlamıyla belli bir kişiye yönelik tutum ve tavır değişikliği yaratacak ve sonuç doğuracak güçte bir değerlendirme yapılması şeklinde ele alınmaktadır. İlgili maddede karar için belirli bir şekil şartı öngörülmemiştir. Örneğin bir özel şirketin plan, tavsiye, tasarım şeklinde nitelendirdiği bir uygulama, kişi üzerinde bağlayıcı ve önemli sonuçlar doğuruyorsa 22. madde kapsamında ele alınmalıdır. Dolayısıyla farklı şekillerde ve farklı nitelendirmelerle ortaya çıkan ancak sonuç itibariyle kişiyi farklı bir muameleye tabi tutan her türlü uygulama karar olarak değerlendirilmelidir[227].

cccc) Kişi Hakkında Alınan Kararın Yalnızca Otomatik İşleme Faaliyetine Dayalı Olması

22. maddenin uygulama alanı bulabilmesi için kişi hakkında, kendisinin ya da kendisi ile ilişkilendirebilecek üçüncü kişilerin kişisel verilerinden yola çıkarak alınan kararın yalnızca otomatik işleme faaliyetine dayalı olması gerekir. İnsan müdahalesi her halde kararın "yalnızca otomatik" şekilde alınmadığı anlamına gelmeyecektir. Nitekim kimi durumlarda gerçek bir kişinin profilleme ile alınan kararları doğrudan onaylaması söz konusu olabilir. Gerçek anlamda insan müdahalesi ve kontrolü ile kast edilen, gerçek kişinin şeklî bir şekilde profilleme teknolojilerini onaylaması değildir. Kişilerin salt otomatik karar mekanizmalarına tabi olmadığından bahsedebilmek için, bir insanın alınacak karar üzerinde etkisi olması, dolayısıyla yetkili bir kişi olması, bunun yanı sıra sürece hâkim olması ve gerçek bir değerlendirme yapabilmiş olmasını gereklidir[228]. Burada bir insanın alınacak kararda etkili olması, gerektiğinde bu kararı değiştirebilme imkân ve iktidarı olması anlamına gelmektedir. Profilleme veya diğer otomatik karar alma mekanizmalarının, insanlar tarafından alınacak karara destek

[226] Häuselmann, Andreas Nicolas, "Profiling and the GDPR: Harmonised Confusion", **Jusletter**, 12.02.2018, https://jusletter.weblaw.ch/juslissues/2018/924/profiling-in-the-gdp_3b8e8a124f.html__ONCE&login=false, Erişim Tarihi: 11.04.2021, s.13, 14.
[227] Kuner/Bygrave/Docksey, s.532.
[228] Häuselmann, s.14.

olma amacıyla kullanıldığı ve süreç üzerinde tek belirleyici olmadığı durumlarda, 22. madde uygulama alanı bulamayacaktır[229]. Ancak insan müdahalesinin etkin bir müdahale olabilmesi, aşağıda tartışılacak "kara kutu" problemi ile yakından ilişkilidir. Nitekim insan müdahalesi sırasında, yetkili kişi, profilleme teknolojilerinin çalışma modelini anlayamıyor ve bu teknolojilerin, vardıkları sonuca ne şekilde ulaştıklarını takip edemiyorsa, gerçek anlamda bir kontrolden bahsetmek mümkün olamayacaktır. Dolayısıyla gerçek bir insan müdahalesi, ancak profilleme yazılımlarının açıklanabilir olması ile mümkündür.

Üzerinde durulması gereken bir diğer nokta, salt otomatik karar alma ifadesinin profillemenin ilk ayağı olan veri toplama aşamasını da kapsayıp kapsamadığıdır. Aksi bir yorumla, insan eliyle toplanmış verilere dayanılarak profilleme yapıldığı hallerde, "salt otomatik yollarla karar verilmediği" ileri sürülebilir ve sürecin 22. maddede belirtilen yasak kapsamı dışında kaldığı iddia edilebilir. Kural olarak veri işleme ifadesi, verinin toplanma sürecinden, nihai olarak saklanmasına kadar tüm aşamaları kapsamaktadır. Ancak otomatik karar alma ifadesi ile bu sürecin verilerin toplandığı ilk aşamadan itibaren otomatik olması kast edilmemektedir. Nitekim 22. maddenin amacı, verilerin ilk toplanma şeklinden ziyade, gruplandırılma ve ilişkilendirme sürecinin gerçekleştiği profilleme ve karar alma aşamalarını düzenlemektedir. Dolayısıyla profillemenin salt otomatik olarak yapılması ve buna dayanılarak otomatik karar alınmasının önüne geçilmek istenmektedir. Bu nedenle örneğin ilkin insan eliyle toplanmış verilerin, otomatik araçlarla analiz edilerek karar alınması durumunda, yine karar alma sürecinde mutlaka insan müdahalesi bulunması gereklidir. Aksi halde, söz konusu "yalnızca otomatik işlemeye dayalı karar alınması" yasağı çiğnenmiş olacaktır[230].

dddd) Kişi Hakkında Alınan Kararın Hukuki veya Benzer Nitelikte Ciddi Etki Doğurması

Otomatik işlemeye dayalı karara GDPR m. 22'nin uygulanabilmesi için kişi hakkında verilen karar hukuki veya benzer nitelikte ciddi etkiler doğurmalıdır. Hukuki etki doğuran kararlar, bir kişinin hak ve yükümlülükleri üzerinde değişiklik yaratan

[229] Dreyer/Schulz, s.18.
[230] Kuner/Bygrave/Docksey, s.533.

veya hukuki statüsünü değiştiren kararlardır. Bir sözleşmenin kurulması ya da feshi, seçme ve seçilme hakkının etkilenmesi örnekleri hukuki etki olarak değerlendirilebilir[231]. Örneğin bir kişinin profilleme teknolojileri eliyle tekrar suç işleme ihtimalinin belirlenmesi ve bu nedenle tutukluluğunun devamına karar verilmesi kuşkusuz hukuki nitelikte bir etki doğurmaktadır. Belçika Kişisel Verileri Koruma Kurulu, kişileri hedef alan otomatik reklamcılık uygulamalarını da kişilere yönelik ürün arzı ve fiyat arzına etki etmeleri sebebiyle hukuki etki doğuran kararlar kategorisinde değerlendirmiştir[232]. Yine sosyal yardımdan mahrum bırakılmaya yol açan, bir ülkeye girişi engelleyen, kamu kurumları tarafından daha fazla gözetim ve denetime maruz bırakılmaya yol açan, fatura ödememe sebebiyle otomatik olarak telefon hizmeti sözleşmesini iptal eden tüm otomatik karar alma mekanizmaları hukuki etki doğuran niteliktedir[233]. Bununla birlikte maddede belirsiz olan husus "hukuki niteliğe benzer nitelikte ciddi bir etki"nin ne olduğudur. Otomatik veri işlemeye dayalı kararın ne zaman ciddi sayılabilecek eşiğe ulaştığı tartışmalıdır. Örneğin bir üniversiteye kayıt olabilmek, bir öğrencinin sınav sonuçlarını değerlendirmek[234], bir kişinin kart limitini oturduğu bölge üzerinden yapılan profillemeye dayanarak düşürmek ilgili kişiyi hukuki etkiye benzer nitelikte etkileyen kararlara örnektir. Bununla birlikte, bir kararın kişi üzerinde ciddi bir etki doğurup doğurmadığı olayın şartlarına göre belirlenmelidir. Kullanılan profilleme teknolojisinin müdahale yoğunluğu, ilgili kişinin beklenti ve talepleri, yine ilgili kişinin azınlık veya çocuk gibi kırılgan statüde bulunması veya sosyo-ekonomik güçlük içinde bulunması alınan kararın etkisini derinleştiren unsurlardır. Örneğin ekonomik güçlük içinde olduğu profilleme uygulamalarıyla tespit edilen kişiye düzenli olarak çevirim içi kumar uygulamalarının gösterilmesi tüm koşullar değerlendirildiğinde ilgili kişinin iradesini manipüle edebilecek ve daha fazla borçlanmasına yol açabilecek niteliktedir. Dolayısıyla ciddi bir etki, ilgili kişinin yaşam koşullarını, davranışlarını, seçimlerini değiştirme potansiyeline sahip etkidir. Nitekim günümüzde otomatik karar alma mekanizmalarının gücü, kimi durumlarda

---

[231] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, 2017, https://www.apda.ad/sites/default/files/2018-10/decisions_automatitzades_i_profiling.pdf, Erişim Tarihi: 20.04.2021, s. 10.

[232] Frederik Borgesius Zuiderveen, **Improving Privacy Protection in the Area of Behavioural Targeting**, Doktora Tezi, Amsterdam Üniversitesi Hukuk Fakültesi, Aralık 2014, s. 375.

[233] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision Making, s.10.

[234] Häuselmann, s.17.

kişinin toplumdan dışlanması veya ayrımcılığa uğraması derecesine dahi ulaşabilmektedir[235].

eeee) Otomatik İşlemeye Dayalı Karar Almayı Mümkün Kılan İstisnai Hükümler

GDPR m.22, yukarıda belirtilen ve m. 22 f.1'de sayılan 3 şartın bir arada bulunması halinde uygulama alanı bulacaktır. Maddenin zıt anlamından, kural olarak kişisel verilere dayanılarak ve yalnızca otomatik işleme sonucu kişileri hukuken veya ciddi ölçüde etkileyen karar alınmasının yasak olduğu anlaşılmaktadır. Bununla birlikte 22. maddenin 2. fıkrası, salt otomatik işlemeye dayalı karar alabilme yasağının istisnalarını düzenlemektedir. İlgili maddeyi "salt otomatik işleme faaliyetine dayalı karar alma"nın mümkün olduğu istisnai haller olarak okumak da mümkündür[236]. İstisnai hallerden ilki, hakkında karar alınan ilgili kişi ile veri sorumlusu arasında bir sözleşme yapılması veya uygulanması için otomatik veri işlemeye dayalı karar alınmasının gerekli olmasıdır. Bu istisna için, taraflar arası sözleşme yapılma aşamasında bulunulmalı ve bu sözleşmenin yapılabilmesi veya uygulanabilmesi için otomatik şekilde veri işlenmesi yoluyla karar alınması gerekli olmalıdır. Gereklilik ile anlaşılması gereken, örneğin profilleme teknolojilerine başvurmadan, daha az müdahaleci bir yöntemle sözleşme kurulmasının mümkün olmamasıdır[237]. Dolayısıyla gereklilik testi, söz konusu istisnanın sınırlarını daraltmaktadır. Bu konuda profilleme teknolojileri açısından 29. madde Çalışma Grubunun yorumu özellikle dikkate alınmalıdır. Örneğin internet servisinden yararlanan kişilerin çevirim içi hareketlerinden yola çıkarak hayat tarzları ve zevklerini tespit eden profilleme yapılması, sözleşme yapılması istisnası kapsamında değerlendirilemez. Nitekim ilgili kişi salt alışveriş yapmak kimi zaman ise bir hizmetten yararlanmak amacıyla ilgili internet sitesini ziyaret etmektedir. Kişi, hakkında profil oluşturulduğu yönünde bilgilendirilse dahi, bu durum bizatihi profillemeyi "sözleşmenin kurulması için gerekli olma" istisnası kapsamında değerlendirmek için yeterli değildir. Nitekim herhangi bir ürünü beğenen kişinin satın alması için, internet üzerindeki tüm

[235] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision Making, s.11, 12.
[236] Maja Nišević, "Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR", **Global Privacy Law Review**, Cilt:1, Sayı: 2, 2020, ss. 104-115, s.111.
[237] Häuselmann, s.18.

hareketlerinin takip edilmesi gereklilik arz etmez. Dolayısıyla bu tür durumlarda m. 22/2 (a) fıkrasında düzenlenen bu istisnaya dayanılamaz[238].

22. maddenin ikinci fıkrasında sayılan diğer bir istisna, otomatik veri işlemeye dayalı karar alınmasının, Avrupa Birliği mevzuatı veya üye devletlerin iç mevzuatınca açıkça öngörüldüğü ve mümkün kılındığı hallerdir. Ancak bu düzenlemeler 22/2 (b) bendinde belirtildiği üzere ilgili kişinin hak ve özgürlükleri ile meşru çıkarlarını koruyucu tedbirler içermelidir. GDPR 71. gerekçe maddesinde, dolandırıcılık ve vergi suçlarını tespit ve kontrol etme veya sunulan hizmetin güvenliğini tesis etme amacıyla profillemeye izin veren düzenlemeler bu istisnaya örnek olarak gösterilmiştir[239]. Ancak bu istisna, her ülkenin farklı düzenleme yapmasını mümkün kılmakta, GDPR hükümlerinin Avrupa Birliği genelinde yeknesak bir veri koruma rejimi tesis etmek üzere sevk edildiği düşünüldüğünde, bu amaçtan uzaklaşma tehlikesi barındırmaktadır[240]. Ayrıca ilgili istisna, otomatik karar alma sürecinde alınması gereken önlemler ve tanınması gereken hakların sayıldığı m. 22/3 fıkrasının dışında tutulmuştur. Başka bir deyişle kanunla açık bir düzenleme söz konusu olan hallerde GDPR m.22/3 uygulama alanı bulmayacaktır[241]. Bununla birlikte açık düzenleme söz olduğu hallerde dahi hakların dengesinin gözetilmesi ve kişi haklarının otomatik işlemeye dayalı alınan kararlara karşı güçlendirilmesi zorunludur.

22. maddedeki son istisna ise 2.fıkranın (c) bendinde düzenlenen ilgili kişinin açık rızası bulunması halidir. Bu maddede neden "rıza" ifadesinin ötesine geçilerek "açık rıza" ifadesinin tercih edildiği üzerinde durulmalıdır. GDPR kapsamında açık rıza ifadesine kişisel verilerin korunmasına yönelik özel risk arz eden durumlarda yer verildiği görülmektedir. Buna örnek olarak özel nitelikli verilerin işlenmesi, verilerin üçüncü ülkeye transfer edilmesi gibi durumlar verilebilir. GDPR kapsamında 4.

---

[238] Article 29 Data Protection Working Party, **Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC**, 844/14/EN WP 217, 09.04.2014, https://www.fia.org/sites/default/files/2019-11/Excerpts%20-%20Opinion%2006-2014%20on%20 the%20notion%20of%20legitimate%20interests%20of%20the%20....pdf, Erişim Tarihi: 27.04.2021, s.17.

[239] Recital 71, GDPR, https://www.privacy-regulation.eu/en/recital-71-GDPR.htm, Erişim Tarihi: 27.04.2021.

[240] Häuselmann, s.18.

[241] GDPR m. 22/3 veri sorumlusunun en azından insan müdahalesinin sağlanması hakkı başta olmak üzere ilgili kişinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki haklarının tanınmasını, kişi özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirler uygulamasını zorunlu tutmaktadır.

maddenin 11. fıkrasında ise "açık" ifadesine yer verilmemiş, ancak rıza aranan tüm hallerde dışa yansıyan ve şüpheye yer bırakmayan bir irade beyanı aranmıştır. Bu fıkraya göre rızadan bahsedilebilmesi için kişinin rızasını aydınlatıldıktan sonra, özgür iradeye dayalı, sınırlı ve kuşkuya yer vermeyecek şekilde dışarı yansıyan davranış veya beyanıyla vermiş olması gerekir. Salt rıza aranan durumlarda dahi dışa yansıyan irade beyanı aranırken, "açık rıza" ifadesi ile farklı olarak neyin aranması gerektiği GDPR kapsamında belirtilmemiştir[242]. GDPR uygulaması açısından bağlayıcı olmayan 29. Madde Çalışma grubu, açık rıza aranan durumlarda ilgili kişinin rızasının kanıtlanması gerektiğini, bu durumda kişinin yazılı beyanını almanın rıza hususundaki şüpheleri tamamen ortadan kaldırmak adına önemli olduğunu vurgulamaktadır. Bununla birlikte, yazılı beyan GDPR kapsamında bir şekil şartı olarak öngörülmemiştir[243]. Nitekim uygulamada da elektronik ortamda ilgili kişinin bir form doldurması istenmesi, email veya taranmış imzalı bir belge ile rızasını doğrulaması veya elektronik imza kullanması gibi yöntemlere başvurulmaktadır.

Profilleme sürecinde önemli olan, ilgili kişinin her farklı veri işleme süreci için ayrı ayrı rıza göstermesidir. En baştan tüm işlemler için toplu rıza alınması uygulaması yerinde değildir. Yine rıza alma yönteminin kişiye gerçekten seçme şansı bırakması oldukça elzemdir. Bu bağlamda örneğin internet sayfasına erişim sırasında çerez uygulamalarını kabul etmeyen kişilere servis sağlanmaması durumunda gerçek bir rızadan bahsedilemez. Yine rıza istisnası kapsamında, bu istisnanın GDPR 5. maddedeki şeffaflık ve 13. ile 14. maddelerdeki bilgi edinme hakkı ve yükümlülüğü ile birlikte düşünülmesi gerekir. Nitekim kişilerin gerçek anlamda bilgilendirilmedikleri veya işleyişini idrak edemedikleri bir sürece rıza göstermeleri mümkün değildir. Özellikle profilleme uygulamaları sırasında, kişilerin okuması ve anlaması mümkün olmayan uzun ve karmaşık metinler ile gerçek anlamda aydınlatılmaları değil, tersine bir nevi tasarlanmış anlaşılmazlık içerisinde, şekli olarak

---

[242] Açık rıza kavramının aktif bir eylem ile rızayı ortaya koyma anlamına geldiği, dolayısıyla kişinin sessiz kalması, örneğin kişisel verilerinin işlenmesine imkân veren ayarları değiştirmemesi halinde zımnen rıza gösterdiğinin kabul edilemeyeceği yönünde bkz, Evik, Vesile Sonay, "Avrupa Birliği Çerçevesinde Kişisel Verilerin Korunması", Tebliğ, Sanal Dünya'da Adalet, **Uluslararası Suç ve Ceza Film Festivali**, 22.11.2019, https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=9uscff-teblig.pdf, Erişim Tarihi: 30.04.2021.

[243] Article 29 Data Protection Working Party, **Guidelines on Consent under Regulation 2016/679,** 17/EN WP259, Revised Version 10.04.2018, https://ec.europa.eu/newsroom/article29/items/623051, Erişim Tarihi: 30.04.2021, s.18.

onaylarının alınması söz konusu olmaktadır. Rızanın bu şekilde alınması halinde, salt otomatik işlemeye dayalı karar alma hukuka uygun kabul edilmemelidir[244].

ffff) GDPR m. 22 Kapsamında Öngörülen Koruyucu Önlemler

Salt otomatik işlemeye dayalı karar alınan hallere cevaz veren m.22/2 kapsamındaki bazı istisnai hallerde, m. 22/3 kapsamındaki önlemlerin alınması zorunlu kılınmıştır. Buna göre m. 22/3 kapsamında öngörülen önlemlerin alınması, yalnızca sözleşme yapılması ve uygulanması için gerekli olma ve açık rıza bulunması hallerinde zorunludur. Başka bir deyişle, otomatik karar almaya cevaz veren "AB mevzuatı veya üye devletlerin iç mevzuatınca öngörülme" istisnası halinde 22/3'te sayılan önlemlerin alınması zorunlu tutulmamıştır[245]. 22/3'te yer alan düzenlemenin içeriği incelendiğinde, ilgili kişilere tanınması gereken asgari hakların sayıldığı görülmektedir. Buna göre hakkında karar alınan kişi, en azından insan müdahalesinin sağlanması hakkı, kendi görüşünü ifade etme ve karara karşı çıkma yönündeki haklarından yararlandırılmak zorundadır. İlgili fıkrada asgari olarak tanınması gereken haklar sayılsa da bunlar tüketici şekilde sayılmamıştır. Veri sorumlusu, kişinin özgürlükleri ve meşru menfaatlerinin güvence altına almak amacı ile tedbirler alacak ve ilgili kişinin verilerinin korunması için asgari olarak m.22/3'te sayılan haklardan ve dilerse daha fazla haktan yararlanmasını sağlayabilecektir[246]. Bununla birlikte özellikle kişinin karara anlamlı şekilde karşı çıkabilmesi için kararın ne şekilde alındığının kendisine açıklanması gereklidir. GDPR m. 22/3 kapsamında kişiye profilleme teknolojileri ile alınan kararın ne şekilde alındığının ex post şekilde açıklanması hakkının tanınıp tanınmadığı ise tartışmalıdır. Aynı tartışma aşağıda ele alınacak ve GDPR bünyesindeki 13 ve 14. maddeler kapsamında da yürütülmektedir[247]. Bu bağlamda GDPR 71. gerekçe maddesi ele alındığında, kişilerin

---

[244] Gil González/ De Hert, s. 601.

[245] Bununla birlikte GDPR m. 22/2 kapsamında AB ve üye devletlerin mevzuatınca otomatik karar almaya cevaz veren hukuki düzenlemelerin bulunması halinde, bu düzenlemelerin ilgili kişinin özgürlükleri ve meşru menfaatlerini güvence altına alınmak üzere uygun tedbirleri içermesi gerektiği açıkça belirtilmiştir. Dolayısıyla tüm istisnai hallerde hak ve özgürlükleri koruyucu tedbirler alınmalıdır. GDPR m. 22/3'te öngörülen tedbirlerin bu fıkraya uygulanmayacak olması bu nedenle bir fark yaratmamaktadır. Herhangi bir önlem almaksızın otomatik karar alınma mekanizmalarının sevk edilmesi hiçbir istisnai durumda söz konusu olmayacaktır.

[246] Kuner/Bygrave/Docksey, s.538.

[247] Kuner/ Bygrave/ Docksey, s.538.

profilleme de dâhil olmak üzere otomatik işlemeye dayalı alınan kararların açıklanmasını talep etme hakkı olduğunun belirtildiği görülmektedir. Gerekçede bu hak açıkça tanınsa da gerekçeler bağlayıcı olmadığı ve 22. madde bünyesinde bu hak açıkça tanınmadığı için söz konusu tartışmayı çözümlemek kolay olmamaktadır. Bu nedenle bütüncül bir yorum yapabilmek adına GDPR kapsamında ilgili maddeler, bir sonraki başlıkta şeffaflık hakları şemsiyesi altında birlikte ele alınacaktır.

gggg) GDPR m. 22 Kapsamında Özel Nitelikli Verilere Dayanılarak Otomatik Karar Alma Yasağı

22. maddenin 4. fıkrasında kural olarak otomatik işlenen verilere dayanılarak karar alınırken, GDPR 9/1 maddesinde atıfta bulunulan özel kategorilerdeki kişisel verilere dayanılması yasaklanmıştır. GDPR m. 9/1'te sayılan veriler, ırk veya etnik köken, siyasi görüş, dini veya felsefi inançlar ya da sendika üyeliğini içeren kişisel veriler ile gerçek bir kişinin kimlik teşhisinin yapılması amacıyla işlenen genetik verileri ile biyometrik verilerin, sağlık verilerini veya cinsel yaşamı veya cinsel yönelimine ilişkin verilerdir. Özel nitelikli veri işleme yasağının istisnası, GDPR 9/2 maddesinin (a) veya (g) bendinde belirtilen ilgilinin açık rızası veya AB ile üye devlet iç hukuku mevzuatına dayanan ve kamu yararı adına veri işlemenin söz konusu olduğu hallerdir. Bu istisnai durumlarda, ilgilinin hakları, özgürlük ve meşru menfaatlerinin güvence altına alma amacıyla uygun tedbirlerin alınması gerektiği özellikle belirtilmiştir. Aslında 22. maddenin 4. fıkrası, özel nitelikli verileri düzenleyen GDPR 9. maddeye ek bir düzenleme getirmemektedir. Özel nitelikli kişisel veri, 22. madde gereği yine açık rıza bulunması veya AB mevzuatı ile üye devlet mevzuatlarında özel nitelikli veri işlemeye cevaz veren düzenlemelere dayanılarak kamu yararına veri işlenmesi halinde profilleme teknolojilerinde kullanılabilecektir[248]. Bununla birlikte ilgili yasağın 22. maddede tekrar ele alınması, profilleme teknolojilerinin özel niteliğinden kaynaklanmaktadır. Nitekim milyonlarca veri henüz ilişkilendirilmeden önce, özel nitelikli veri teşkil etmeyebilir. Ancak profilleme teknolojilerinin uygulanmasının ardından kişilere ilişkin özel nitelikli veriler açığa çıkabilir. Dolayısıyla 22. madde, profilleme sonucu elde edilen türetilmiş verilerin, özel nitelikli olması halinde bunlara dayanılarak karar alınmasını yasaklamakta, böylelikle

[248] Dreyer/Schultz, s.21.

türetilmiş özel nitelikli verilere ilişkin ortaya çıkabilecek tartışmaların önünü kapamaktadır. Böylelikle m. 22/4 lafzı karşısında özel nitelikli veri işleme yasağının yalnızca doğrudan kişiden elde edilmiş veriler için geçerli olduğu, türetilmiş verilere uygulanamayacağı şeklinde daraltıcı yorum yapmak mümkün olmayacaktır. Bu durumda örneğin, başta kişinin alışveriş alışkanlıkları gibi özel nitelikli kişisel veri teşkil etmeyen verilerden yararlanan profilleme uygulamaları, bu alışkanlıklarından yola çıkarak kişinin sağlık verilerine ilişkin çıkarımlar yaparsa, bu durumda sağlık verisi ikincil ve türetilmiş veri olsa dahi, 22/4 açık hükmü gereğince kişi hakkında karar verilirken kullanılamayacaktır[249]. Dolayısıyla ilgili yasağın 22. madde bünyesinde düzenlenmesi, özel nitelikli verilerin koruma alanına ilişkin belirlilik kazandırdığından önem taşımaktadır.

bb) GDPR Kapsamında Şeffaflık Hakları ve Kara Kutu ("Black Box") Problemi

Profilleme teknolojileri bugün makine öğrenmesinin kazandığı hızla daha karmaşık bir yapıya bürünmekte, bu teknolojilerin hedefi olan kişiler ise işleyişine hâkim olamadıkları bu yazılımlara tabii olmaktadır. Bu bilgi asimetrisi, kişilerin profillemenin verilerinin üzerinde yarattığı veya yaratacağı riskleri değerlendirmelerini ve bunlara karşı kişisel verilerinin korunması için hak mekanizmalarını işletmelerini güçleştirmektedir[250]. Profilleme başta olmak üzere otomatik değerlendirme mekanizmalarını daha şeffaf hale getirebilmek ve şirketler, hükümetler ile vatandaşlar arası eşitsiz konumda, kişilerin haklarını güçlendirebilmek için GDPR kapsamında belli hak ve yükümlülükler öngörülmüştür. GDPR bir yandan veri sorumlularına bilgilendirme yükümlülüğü getirirken, diğer yandan ilgili kişilere verilerine erişim ve gerektiğinde bu verileri düzeltme ve silinmesini talep etme hakları tanımıştır. Aşağıda profilleme teknolojileri ile veri işleme sürecini "kara kutu" olmaktan çıkarmayı amaçlayan GDPR m.12'deki "ilgili kişinin haklarının kullanımına ilişkin şeffaf bilgilendirme hakkı", 13. ve 14. maddedeki veri işlenmesi sürecinde "ilgili kişiyi bilgilendirme yükümlülüğü", 15. maddedeki "ilgili kişinin veriye erişim hakkı" ele alınacaktır. Ardından bu hakların profillemeye ilişkin ana düzenleme olan 22. maddedeki insan müdahalesinin sağlanması hakkı, veri sahibinin kendi görüşünü

[249] González/ De Hert, s.614.
[250] Häuselmann, s.20.

ifade etme hakkı ve karara karşı çıkma hakkı ile ilişkisi kurulacaktır. GDPR kapsamında en temel prensiplerden biri olan ve 5. maddede dile getirilen şeffaflık prensibi, ilgili kişinin verilerinin ne amaçla ve ne şekilde işlendiği, profilleme teknolojilerinden yararlanılıyorsa bu teknolojilerin varlığı ve olası sonuçları hakkında aydınlatılmasını da gerektirir[251]. Profillemeye özel bu şeffaflık düzenlemelerine 13, 14 ve 15. maddeler bünyesinde ayrıca yer verilmiştir. Aşağıda şeffaflık başlığı altında toplanan tüm bu düzenlemeler detaylarıyla ele alınacaktır.

aaa) İlgili Kişiyi Bilgilendirme Yükümlülüğü

GDPR 12. maddenin 7. fıkrası veri sorumlularının kişiyi bilgilendirme yükümlülüğünü kolaylıkla okunabilir ve anlaşılabilir şekilde yerine getirmesi gerektiğini belirtmektedir. Yine aynı maddenin 1. fıkrası, bilginin özlü, şeffaf ve kolaylıkla erişilebilecek şekilde tesis edilmesi gerektiğinin altını çizmektedir. Bu bağlamda tüm sürecin kişinin okumasını neredeyse imkânsız hale getirecek uzunluk ve karmaşıklıkta açıklanması 12. madde ile örtüşen bir bilgilendirme yöntemi olmayacaktır. Yine veri işleme sürecinin kişiyi ne şekilde etkileyeceği, kişiyi profilleme sürecinin tüm teknik detaylarıyla boğmaksızın, açık şekilde ortaya konulmalıdır[252].

GDPR 13. ve 14. madde, ilgili kişiye yönelik bilgilendirmenin neleri içermesi gerektiğine dair ayrıntılı düzenlemeler içermektedir. 13. madde, bizzat ilgili kişiden veri edinildiği durumlarda yapılması gereken bilgilendirmenin içeriğini düzenlerken, 14. madde ilgili kişinin verilerinin doğrudan kendisinden edinilmediği durumlarda, veri işleyenin bilgilendirme yükümlülüğünü düzenlemektedir. Dolayısıyla kişinin bizzat verisini paylaşmadığı, örneğin önceden farklı veri sorumlusu tarafından toplanmış verilerinin, başka bir veri sorumlusu tarafından profilleme amaçlı işlendiği durumlarda da bilgilendirilmesi gerekir. Her iki madde de kişiye, verilerinin hangi veri sorumlusu tarafından işlendiğinin açıklanması gerektiği, ayrıca veri işlemenin amacının ve hangi hukuki zemine dayandığının belirtilmesi gerektiği düzenlenmiştir.

---

[251] Recital 60, GDPR, https://www.privacy-regulation.eu/en/recital-60-GDPR.htm, Erişim Tarihi: 02.05.2021.

[252] Sandra Wachter/Brendt Mittelstadt/Chris Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", **Harvard Journal of Law and Technology**, Cilt: 31, Sayı: 2, Spring 2018, ss. 841-887, s.865, 866.

Bunun yanı sıra, eğer ilk belirlenen amaç dışına taşan farklı bir amaçla veri işlenmeye devam edilmek isteniyorsa, kişi bu hususta bilgilendirilmelidir. Yine verilerin üçüncü bir ülke ya da uluslararası bir organizasyona aktarılması ihtimali söz konusu ise kişi bu durumdan haberdar edilmelidir. Verilerin bizzat ilgili kişiden temin edilmediği durumlarda 14. madde gereği ayrıca işlenen veri kategorileri ve verilerin kimden temin edildiğinin açıklanması gerekir. Bu durumda verilerin bizzat kişiden edinilmediği ancak farklı veri tabanlarından toplandığı hallerde, kişiye işlenen doğrudan veya dolaylı tüm veri kategorileri açıklanmalıdır. Örneğin kişinin kimlik bilgisi, iletişim verileri, bulunduğu yerin verisi, politik görüşleri, dini görüşleri, beslenme tercihleri, internet geçmişi gibi farklı türden verileri işlendiyse, kişinin tüm bu veri grupları hakkında bilgilendirilmesi zorunludur. Bu bağlamda, "sağlık verileriniz işlenmektedir" şeklinde bir açıklama yapılması, sağlık verilerinin çok geniş kapsamlı olması nedeniyle veri kategorisi açıklama yükümlülüğünü yeri getirme açısından yetersiz olacaktır. Bu örnekte "kan basıncı", "hamilelik yaşı" gibi daha kapsamlı bir açıklama yapılması verilerin işlenme amacını ve bu amaç dışına taşılıp taşılmadığını göstermek açısından önem teşkil etmektedir. Böylelikle özellikle profilleme sürecinde, bu maddeler sayesinde kişi henüz verileri profilleme uygulamalarında kullanılmadan önce bilgi sahibi olabilecektir. Yine verilerin elde edildiği kaynakların detaylı şekilde açıklanması, kişinin ilk kaynakta toplanmış verilerini tekrar gözden geçirebilmesini sağlamak açısından önem taşımaktadır. Bu nedenle kamusal-özel sektör ayrımı yapılmaksızın, veri kaynağı ifşa edilmelidir[253]. Bu bilgilendirme sırasında ayrıca ilgili kişiye verilerine erişme, verilerinin silinmesini talep etme, Kişisel Verileri Koruma Kuruluna başvurma gibi haklarının hatırlatılması zorunludur. Bu durumda kişi, veri işlenmesi sürecinin daha en başından sürece müdahil olabilecek, haklarına başvurabilecektir[254].

bbb) İlgili Kişinin Verilere Erişim Hakkı

Şeffaflık ilkesinin tesisi açısından kişilerin verilerine erişim hakkını düzenleyen 15. madde ise, 13. ve 14. maddelerdeki gibi veri sorumlusunun yükümlülüklerini değil, ilgili kişinin haklarını düzenlemiştir. Bu nedenle 15. maddenin uygulanabilmesi için hak sahibinin talepte bulunması gereklidir. İlgili madde uyarınca, erişim hakkını

[253] Kuner/Bygrave/Docksey, s.444.
[254] Kuner/Bygrave/Docksey, s.428

kullanan kişi, verilerinin işlendiğini onaylayan ya da inkâr eden bir cevap alabilecektir. Kişi 13. ve 14. maddede sayılan bilgiler henüz tesis edilmediyse, talebiyle birlikte ilgili maddelerde sayılan tüm bilgilere erişebilecektir. İlgili hak, herhangi bir ücret ödemeyi gerektirmeksizin, veri sorumlusunun sağladığı bilgilerden daha da fazla bilgiye erişimi mümkün kılmaktadır. Bu maddeyi özel kılan, örneğin Twitter gibi milyonlarca kişinin verilerini işleyen veri sorumlularının herkese yönelik genel geçer yaptığı bilgilendirmeden farklı olarak, talepte bulunan kişiye özel, bireyselleştirilmiş bir cevap verilmesini gerektirmesidir. Örneğin verilecek cevapta, kişiye özel şekilde, verilerinin ne zamandan beri saklanmakta olduğu belirtilecektir[255]. 15. madde, veri sorumlusunun veri işledikten sonra işlediği verileri açıklamasını gerektirmektedir. Dolayısıyla, henüz veri işlemeden önce veya profilleme teknolojisi kullanılmadan önce bilgilendirme yükümlülüğü öngören 13. ve 14. maddelerden farklı olarak, 15. madde ex post açıklama gerektiren bir haktır ve veri işleme süreci boyunca veya veri işleme tamamlandıktan sonra kullanılması mümkündür[256].

ccc) Profilleme Teknolojilerine İlişkin Özel Bilgilendirme Düzenlemeleri

GDPR 13/2 (f) bendi ve 14/2 (g) bendi ve son olarak 15/1 (h) bendinde aynı ifadeyle yer alan düzenlemelere göre, ilgili kişiler haklarında profil çıkarma da dâhil olmak üzere otomatik yollarla verilen kararın varlığı, bu teknolojilerin işleme mantığı ve otomatik veri işleme sürecinin önemi ve öngörülen sonuçları hakkında "anlamlı" bilgi edinebilmelidir. Kuşkusuz ki veri işleme sürecine ve profilleme teknolojilerinin işleme mantığına dair açıklanan bilgilerin anlamlı olabilmesi için açıklamalar teknik bilgiye sahip kişilere yönelik ifadelerle yapılmamalı, açıklama yapılırken ortalama düzeyde bireyler esas alınmalıdır. Bunun yanı sıra açıklanan bilgilerin işlevsel bir anlamı da olmalıdır. Yapılan açıklama, kişinin karar alma sürecini anlamasını ve bu süreçte kendisine tanınmış itiraz etme, görüşlerini sunma gibi haklar ile verilerinin düzeltilmesini ve silinmesini talep etme gibi diğer haklarını kullanmasını mümkün kılmalıdır. Bu nedenle, anlamlı bilgi edinme kavramı üye devletlerin GDPR çevirilerinde daha ziyade "faydalı" veya "kullanışlı" bilgi şeklinde yer almıştır[257].

---

[255] Kuner/Bygrave/Docksey, s.462.

[256] Andrew D. Selbst/Julia Powles, "Meaningful Information and the Right to Explanation", **International Data Privacy Law**, 2017, Cilt: 7, Sayı: 4, ss.233-242, s.234.

[257] Örneğin GDPR metninin Almancasında "ausgekräftige" ve Fransızcasında "informations utiles" kavramları kullanılmaktadır, bu yönde bkz. Selbst/Powles, s.236.

aaaa) Profillemeye Dayalı Karar Alındığını, Bu Kararın Önemi ve Sonuçlarını Açıklama Zorunluluğu

GDPR 13/2 (f), 14/2 (g) bendi ve son olarak 15/1 (h) bentlerinde aynı ifadelerle yeknesak şekilde düzenlenen ilk şart ilgili kişinin hakkında profillemeye dayanılarak alınmış bir kararın varlığından haberdar edilmesidir. Bu tür bir kararın varlığı, önemi ve sonuçları ilgili kişiye anlaşılır şekilde iletilmelidir. Örneğin bir araç sigortası şirketi, profilleme teknolojilerine başvurarak kişilerin sigorta primlerine ilişkin karar almakta ise, öncelikle kişilere tehlikeli araç kullanma şeklinin sigorta primini arttıracak bir etkiye sahip olduğunu belirtmeli ve hangi faktörlerin tehlikeli araç sürmeyi tespit etmede dikkate alındığını açıklamalıdır. Şirket, araç kullanma hızı, akıllı araç kullanmakta ise ani fren yapma sayısı gibi verileri toplayarak sürücünün tehlikeli araç kullanma davranışını profillemekte ise, örneklerle bu faktörleri açıklamalıdır. Bu açıklama kişilere, hangi verilerinin işlendiğini göstereceği gibi, yüksek prim ödeme sonucundan kaçınma olanağını da tanıyacaktır. 13. ve 14. maddedeki açıklamalar, kişi hakkında profilleme amaçlı veri toplanmaya başlanacağı zaman yapılmalıdır. Böylelikle kişi, henüz sürecin başında verilerinin ne şekilde işleneceği ve ne tür bir karara tabi olacağı hakkında önceden bilgi sahibi olacak ve süreci kontrol edebilecektir.

22. maddenin 3. fıkrasındaki haklar ve 71. gerekçe maddesi ile birlikte okunduğunda, profilleme gerçekleştirilerek kişi hakkında karar alındığı takdirde, kişiye hakkında bir karar alındığı bildirmek yeterli olmayacaktır. Bu kararın gerekçesi açıklanmalı ve böylece ilgili kişinin sonuca itiraz edebilmesi mümkün kılınmalıdır[258]. Kişi hakkında karar alınmasının ardından, yine bu kararın alınmasında etkili olmuş veriler ve bu veriler üzerinden ne şekilde profilleme yapıldığı gerekçelendirilmelidir[259]. Dolayısıyla tüm bu haklar kümesi birlikte değerlendirildiğinde, 22. madde kapsamında giren otomatik karar alma sistemleri aracılığı ile kişisel veri işlendiği takdirde, veri işleme sürecinin tüm aşamalarını şeffaf hale getirmek zorunludur.

---

[258] Kuner/Bygrave/Docksey, s.441.

[259] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision Making, s.26.

bbbb) Profilleme Teknolojilerinin İşleme Mantığını Açıklama Zorunluluğu

Profilleme sırasında gerçekleştirilen otomatik işleme yönteminin açıklanması yükümlülüğü doktrinde oldukça tartışmalıdır. Tartışmanın ekseni, kullanılan modelin tasarımının ve işleyiş şeklinin tamamen açıklanmasının zorunlu olup olmadığı üzerinedir. Ayrıca profillemeye konu algoritmayı eğitmek için kullanılan verilerin ve türetilen verilerin paylaşılmasının gerekip gerekmediği sorusuna verilecek yanıt net değildir. Çoğu durumda kodlama yöntemlerini ve algoritmaları eğitmek için kullanılan veri tabanları, "ticari sır", "fikri mülkiyet" gibi haklarla korunmakta ve teknoloji firmaları tarafından paylaşılmamaktadır. AB mevzuatında, veri tabanlarının içeriği dahi sui generis bir hak olarak korunmakta[260], durum sürecin açık şekilde yürütülmesini daha da güç bir hale gelmektedir. Nitekim GDPR 63. gerekçe maddesinde bu husus "ilgili kişilerin erişim hakkı, ticari sır veya fikri mülkiyet haklarını olumsuz etkilemeyecek şekilde değerlendirilmelidir"[261] şeklinde dile getirilmiştir.

Profilleme teknolojilerinin mantığının açıklanmasında ikinci engel, bugün teknolojide kaydedilen ilerlemeler ile veriler arasında ne şekilde bağlantı kurulduğunun bizzat kodlamayı yapan kişi tarafından dahi anlaşılmasının güç hale gelmesidir. Algoritmaların kendi kendine öğrendiği veya insan nöronlarına benzer yapay ağlar gibi yöntemlere başvurulduğu takdirde, veriler arasında kurulan bağların ve varılan sonucun her aşaması adım adım takip edilememektedir. Bu nedenle girdiler ile varılan sonuçlar arasındaki süreç "kara kutu" olarak adlandırılmaktadır. Ancak tüm sistemler kara kutu şeklinde işlememektedir. Örneğin kural-temelli sistemlerde ise "eğer…o halde" ("if…then") şeklinde koşullar içeren kurallar baştan belirlenmekte[262] veya karar ağaçları kullanılarak, kararların alınış mantığı takip edilebilmektedir. Daha karmaşık olan makine öğrenmesi modellerinde ise sisteme hem girdi hem çıktı verileri yüklenmekte, sistemin bu iki veri kümesi arasında kendi kendine bağlantı kurarak

---

[260] Şener, Yavuz Selim, **Fikri Mülkiyet Hukukunda Dijital Veri Tabanlarının Korunması**, İstanbul Kültür Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, 2013, s.7.

[261] GDPR Recital 63, https://www.privacy-regulation.eu/en/recital-63-GDPR.htm, Erişim Tarihi:25.04.2021.

[262] Bahadır Karasulu, "Büyük Veri Çağında Bilişim Sistemleri için Zeki Teknikler Destekli Karar Vermenin Rolü: İnceleme ve Analiz", İçinde **Akıllı Teknoloji ve Akıllı Yönetim**, Ed. Vahap Tecim/Çiğdem Tarhan/ Can Aydın, Gülermant Matbaacılık: İzmir, Eylül 2016, ss.1-11, s.5.

kurallar üretmesi beklenmektedir. Dışardan takip edilmesi güç olan makine öğrenmesi modelinde, makine baştan verilen kuralları takip etmek yerine, kendi kendine kuralları optimum hale getirmektedir[263]. Yeni makine öğrenme modellerinin takip edilebilir sistemlere nazaran çok daha karmaşık yapısının, gerçek hayata daha uygun ve doğru sonuçlar elde etmeyi mümkün kıldığı sıklıkla ileri sürülmekte, bu nedenle açıklanabilir kural temelli öğrenme modelleri yerine, derin yapay sinir ağları yoluyla öğrenme gibi modeller tercih edilmektedir. Yapay sinir ağı, kimi zaman perceptron adı verilen tek bir sinir ağı, kimi zaman ise farklı yapay sinir katmanlarının birleştirilmesi ile oluşturulur. Ancak bu sistemler, ağ içinde üretilen verilere nasıl ulaşıldığı hususunda şeffaflık içermemektedir[264].

Kara kutu şeklinde işleyen sistemlerin daha doğru sonuçlar verdiği iddiası kanıtlanmamıştır. Aksine, özellikle ceza adaleti alanında kullanılan karmaşık modellere karşı üretilen basit, şeffaf ve takip edilebilir modellerin de eşit performansı gösterdiği görülmektedir[265]. Buna rağmen çoğu ülkede hala şeffaflık haklarının kullanımına imkân tanımayan modellerin kullanıldığı görülmektedir.

Özellikle ceza muhakemesi sürecinde savunma hakkı ve daha genel olarak adil bir yargılamanın tesisi, kişisel veri işlemenin şeffaflığı ilkesi ve sistemin mantığını açıklama yükümlülüğü ile doğrudan bağlantılıdır. Kişisel verilerin korunması mevzuatı açısından, otomatik karar alma sistemlerine ilişkin 29. Madde Çalışma Grubunun yaptığı açıklama uyarınca, veri sorumlusu, kullanılan yazılımın vardığı sonucu ve bu sonuca nasıl ulaştığını, ilgili kişinin anlayabileceği yalınlıkta açıklamalıdır. Bunun için veri sorumlusunun kullanılan algoritmanın tüm çalışma modelini teknik şekilde ifade etmesi veya algoritmayı tamamen ifşa etmesi gerekli değildir.

Bu durumda örneğin kişiye kredi verme konusunda bir algoritma kullanan veri sorumlusu, algoritmanın dayandığı verileri kendisi toplayıp işlemiş olmasa dahi ilgili

---

[263]Lilian Edwards/Michael Veale, "Slave To The Algorithm? Why A 'Right To An Explanation' Is Probably Not The Remedy You Are Looking For", **Duke Law and Technology Review**, Cilt: 16, Sayı:1, 2017, ss.18-84, s.25.

[264] Han Liu, **Rule Based Systems for Classification in Machine Learning Context**, University of Portsmouth, Doktora Tezi, Kasım 2015, s.83.

[265] Angelino Elaine/Nicholas Larus-Stone/Daniel Alabi/Margo Seltzer/Rudin Cynthia,"Learning Certifiably Optimal Rule Lists for Categorical Data", **Journal of Machine Learning Research**, Cilt:18, 2018, ss. 1-78, s.42.

kişiye bu kararın alınış şeklini ve ayrıca kararda yararlanılan verileri kimden ve nasıl elde ettiğini açıklamak zorundadır[266]. Verilen karara nasıl ulaşıldığının anlaşılabilmesi için, sonuç açısından önemli olan etkenler ve hangi verilerin sonucu belirlemede ağırlıklı olarak dikkate alındığı belirtilmelidir[267]. Bu durumda örneğin kredi verme kararına ilişkin profilleme yapan şirketin, ilgili kişinin profillemeye konu olmuş borç verileri, hesap hareketleri, adli sicilindeki dolandırıcılık gibi suçlara ilişkin verileri, ticari sicilindeki iflasa dair verileri gibi profillemeye konu tüm verileri paylaşılması gerekir. Veri sorumlusunun ayrıca kredi puanı veren algoritmanın test edildiğini, etkin ve tarafsız şekilde sonuç alınması için gerekli önlemlerin alındığını da paylaşması beklenmektedir[268].

Her ne kadar GDPR kapsamında kullanılan algoritmanın genel mantığının açıklanması öngörülse de kara kutu şeklinde işleyen karmaşık yapılı algoritmaların bu açıklamayı ne kadar mümkün kılacağı tartışmalıdır. Bu tür algoritmalar günümüzde ceza adaletinde kişilerin kaçma şüphesi veya tehlikeliliğinin tespitinden, sağlık sektöründe hastalık teşhisine kadar pek çok alanda kullanılmaktadır. Söz konusu karmaşık algoritmalara karşı duyulan güven, bilgi edinme hakkının özüne aykırı durumlara yol açabilecektir. Oysa son dönem yapılan çalışmalar yukarıda da belirtildiği üzere kural temelli, kolay takip edilebilir algoritmaların en az karmaşık yapay nöron ağları kadar doğru sonuçlara varabildiğini göstermektedir. Örneğin Amerika'da ceza adaletinde kullanılan ve kara kutu şeklinde işleyen COMPAS modelinin, tekerrür tehlikesini gösteren ve işleyiş şekli kolaylıkla takip edilebilen CORELS modelinden daha güvenilir olmadığı görülmüştür. CORELS modeli kural temelli bir algoritma türüdür. CORELS, kişinin sınıfsal ve sosyal statüsünü de içeren yüz otuzdan fazla faktör içeren COMPAS uygulamasından farklı olarak yalnızca kişinin yaşı ve önceden işlediği suç sayısı gibi az sayıda bilgi içermekte, telif hakkı engeli taşımaksızın ücretsiz ve işleyişi herkese açık şekilde kullanılabilmektedir[269].

---

[266] Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision Making, s.25.

[267] Kuner/Bygrave/Docksey, s.463.

[268] Veri sorumlusu, ayrıca iletişim detaylarını paylaşarak ilgili kişinin itiraz edebilmesini mümkün kılmalıdır. Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision Making, s.26.

[269] Synthia Rudin, "Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead", 22.09.2019, https://arxiv.org/abs/1811.10154, s.6, Erişim Tarihi: 29.04.2021.

Bununla birlikte günümüzde başta Amerika olmak üzere çeşitli ülkelerde ceza adaletinde yorumlanabilir, şeffaf algoritmaları tercih edilmediği görülmektedir. Bu algoritmaları üreten şirketlerin, söz konusu algoritmalar kişi haklarını ihlal riski barındırsa ve hatalı sonuçlara yol açsa dahi, sorumlulukları doğmamakta, ilgili firmalar yazılım modelleri üzerinden oldukça yüksek kâr payı elde etmeye devam etmektedir[270]. Örneğin, Amerika başta olmak üzere Hollanda, Finlandiya, İngiltere, Almanya, Avusturya ve Singapur mahkemelerinde kullanılan SAVRY, suça sürüklenmiş çocukların suç işleme tehlikesini belirlerken ailesinde hüküm giymiş kişi bulunup bulunmaması ve sosyo-ekonomik durumları gibi pek çok unsuru dikkate almakta, ancak tehlike riskini belirlerken hangi etkenlerin sonuca varmada ağırlıklı olduğunu açıklamamaktadır. SAVRY de COMPAS profilleme teknolojisinde olduğu gibi belli sınıf ve ırklara mensup kişilerin daha ağır risk grubu olarak belirlenmesine yol açmakta, ancak şeffaf olmamasına ve doğruluk oranı test edilmemesine rağmen, adil yargılama ilkesinin ihlali pahasına ceza adaleti sisteminde kullanılmaktadır. COMPAS teknolojisini yargı önüne taşıyan Loomis davasında olduğu gibi, SAVRY için açılan davada da mahkeme teknolojiyi üreten ve kullanan şirkete karşı yaptırım öngörmemiş ve ilkesel olarak bu teknolojilerin hükmü belirlerken kullanılmaması gerektiğine ilişkin bir değerlendirme yapmamıştır. Mahkeme, yalnızca açılan dava özelinde, profilleme teknolojisinin sonuçlarını karara esas almamakla yetinmiştir[271].

cccc) Şeffaflık İlkesinin Tesisi İçin Kara Kutu Problemine Karşı Çözüm Önerileri

Şeffaflık ilkesini tesis açısından doktrinde kara kutu problemini aşmak için önerilen yöntemlerden biri, "karşı olguları açıklama" teorisidir. Buna göre, profilleme teknolojilerinde neden ile sonuç arasında nasıl bir bağlantı kurulduğunu detaylı açıklayacak şekilde "kara kutu"yu açmak ve sistemin işleyiş modelini açıklamak gerekmeyecektir. Bunun yerine, kişiye örneğin kredi verilmesinin reddi hususunda "Yıllık geliriniz 30 000 dolardır. Eğer geliriniz 45 000 dolar olsaydı, kredi alabilecektiniz." şeklinde sonuca etkili dış unsurun ne olduğu, olumlu karara ulaşmak

---

[270] Rudin, s.4.

[271] Superior Court of the District of Columbia Family Court, Juvenile and Neglect Branch, Dava No:2017 DEL, aktaran Richardson, Rashida/Schultz, Jason M./Southerland, Vincent M., **Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems**, AI Now Institute, Eylül 2019, https://ainowinstitute.org/litigatingalgorithms-2019-us.html, Erişim Tarihi: 29.04.2021, s.9, 10.

için ne yapılabileceği belirtilmelidir. Böylelikle kişiye itiraz hakkını kullanabileceği oranda açıklama yapılmasının yeterli olacağı ileri sürülmektedir[272]. Ancak bu durumda, tam olarak aydınlatılamayan modelin işleyişini gerçek anlamda ifşa eden "karşı olguları açıklama" söz konusu olmamaktadır.

Şeffaflığın tesisi için diğer öneriler arasında algoritmanın çalışma modelinde, kişiye özel verilerin kullanıldığı veya kişiye en yakın görülen diğer kişilerin verilerinin sistemde işlendiği kısmın bölgesel olarak tespit edilmesi ve açıklanması yer almaktadır. Böylelikle tüm sistemin değil, sistemin bir bölümünün çözümlenerek paylaşılabileceği ve yazılımı koruyan fikri mülkiyet haklarının da ihlal edilmeyeceği ileri sürülmektedir. Yine "vekil model" oluşturma tekniği, karmaşık bir profilleme yazılımının kritik olan girdi ve çıktılarını dikkate alarak daha basitleştirilmiş, bu modelin bir nevi vekili olan bir model üretmeyi ve böylelikle sürecin takibini kolaylaştırmayı amaçlamaktadır. Genelde ilk modeli taklit eden bu ikincil modellerde, karar ağacı gibi daha kolay takip edilebilir ve şeffaf modeller kullanılmaya çalışılmaktadır[273]. Ancak bu öneriler kara kutu problemini aşmak için yalnızca yama niteliği taşımakta, özellikle ceza yargılamasında kişinin neyle suçlandığını açıkça anlamasının önüne geçerek savunma hakkının özünü ihlal etmektedir.

Nitekim ceza adaletinde kullanılan profilleme teknolojileri çok farklı verilere dayanmaktadır ve hangi verilerin sonuca etkili olduğu ve varılan sonucun doğru olup olmadığı vekil modellerle açıklanamamaktadır. Vekil model oluşturma önerisi kullanılan verileri ve bu verilerin kullanılma amacını göstermede yetersiz kalmakta, özgün modeli basite indirmektedir. Vekil yöntemi ile modelin genel işleyişindeki hata ve ihlal risklerini tespit mümkün olmadığı gibi, aksine hata payı barındıran genel model indirgenirken hata payı katlanarak artmakta ve sistem orijinaline sadık kalınmaksızın temsil edilmektedir.

Tüm bu çözümlerin yetersizliği karşısında kara kutu problemine yol açan karmaşık teknolojiler yerine şeffaf ve kural temelli modeller tercih edilmelidir. Ancak kara kutu modellerinde ısrar edilmesi durumunda, kuşkusuz ki GDPR kapsamında

---

[272] Wachter/Brendt/Russell, "Counterfactual Explanations Without Opening the Black Box", s.844, 845.
[273] Deeks, Ashley, "The Judicial Demand for Explainable Artificial Intelligence", **Columbia Law Review**, Cilt:19, Sayı:7, Kasım 2019, ss.1829-1850, s.1836,1837.

öngörülen ilgili kişiye profillemenin işleyiş mantığı ve sonuçlarını açıklama yükümlülüğü içeriği boş bir yükümlülük olarak kalmaya mahkûm olacak ve kişisel verilerin korunması mevzuatının yanı sıra ceza muhakemesinin ana ilkesi olan adil yargılanma ilkesi zedelenmiş olacaktır.

c) Profilleme Teknolojilerine İlişkin 2016/680 Sayılı Direktif Bünyesinde Yer Alan Düzenlemeler

Profilleme teknolojileri günümüzde kolluk kuvvetleri tarafından başta Amerika olmak üzere Avrupa'nın çeşitli ülkelerinde suç işlenmeden önce potansiyel suç işleme tehlikesi barındıran kişileri ve suç işlenme riskinin yüksek olduğu mahalleri tespit etmede kullanılmaktadır. Henüz suç yoluna girilmeden önceki bu alanda, ceza muhakemesinin masumiyet karinesi, çelişmeli yargı, adil yargılanma hakkı gibi temel ilkeleri uygulama alanı bulamadığından, bu teknolojilere maruz kalan kişiler, idareye karşı daha korunmasız durumda bırakılmaktadır. Bu teknolojilere aynı zamanda ceza muhakemesinde de şüphelinin kaçma riski, suçta tekerrür ihtimali ve buna dayanarak tutuklama veya serbest bırakma gibi tedbirlere karar verilmesinde başvurulmaktadır. Ceza muhakemesi alanında profilleme teknolojilerinin kullanımı Amerika'da yaygın olmakla birlikte, Kıta Avrupası'nda bu uygulamalara yok denecek kadar az başvurulmaktadır. Son olarak, bu teknolojilere koşullu salıverme ve infaz rejiminin tayininde etmede her iki kıtada da sıklıkla başvurulmaktadır. Tezin konusu bu teknolojilerin ceza muhakemesinde kullanımı ile sınırlanmıştır. Bu aşamada her ne kadar hâkim tarafından sürecin kontrol edildiği ve son sözün yine hâkime ait olduğu ileri sürülebilecek ise de sanığın haklarını güçlendirmek adına kişisel verilerin korunması rejiminin uygulanması büyük önem taşımaktadır. Bu bağlamda ceza muhakemesinde kişisel verileri koruyan hükümlere uygun veri işlenmesi, amaca uygunluk, ilgiliye işlenen verilerini açıklama hakkı, şeffaflık ilkesi gibi ilkelerin üzerinde özenle durulmalıdır.

Profilleme teknolojileri genellikle özel şirketler tarafından üretilmekte ve bu teknolojilerin dayandığı veriler evleviyetle ticaret, internet, bankacılık gibi faaliyetler sırasında toplanmaktadır. Ancak ilgili verilerin suçla mücadele veya yargılama sürecini tamamlama gibi amaçlarla kullanılıp kullanamayacağı ve bu amaçla kullanıldığı takdirde genel kişisel verileri koruma rejimine bu süreçte başvurmanın

mümkün olup olmadığı hususunda soru işaretleri bulunmaktadır. Avrupa Birliği bünyesinde kişisel verilerin korunmasına ilişkin genel bir düzenleme olan GDPR kapsamındaki 2/f.2 (d) bendinde GDPR hükümlerinin kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkili makamlar tarafından işlenmesi sürecinde uygulanmayacağı belirtilmiştir. Ancak sayılan bu amaçlarla suç önleme ve yargılama sürecinde yetkili olmayan makamlarca, örneğin özel şirketler tarafından veri işlendiği hallerde her hâlükârda GDPR hükümlerine uygun işleme yapılmış olmalıdır. Bu nedenle yukarıda detayları ile ele alınan GDPR düzenlemeleri büyük önem taşımaktadır.

GDPR ile m.2/f. 2 (d) bendi ile ceza muhakemesi sürecinde yetkili otoritelerce veri işlenmesi Tüzüğün kapsamı dışında bırakılmıştır. 2016/680 sayılı Direktif bu boşluğu doldurmakta, kümülatif şart olarak Direktif kapsamında sayılan amaçlar ve yine Direktif kapsamında yetkili kabul edilen otoritelerce veri işlenmesi halinde uygulama alanı bulmaktadır. İlk maddede, bu amaçlar suçun önlenmesi, soruşturulması, yargılanma, suçun infazını gerçekleştirme ve kamu güvenliğine karşı yönelmiş tehlikeleri önleme amaçları olarak sınırlanmıştır. Yalnızca 3. maddenin 7. fıkrasında gösterilen yetkili mercilerin bu amaçlarla veri işlemesi halinde Direktif uygulama alanı bulur. İlgili fıkra yetkili mercileri suç tehlikesini önleme, suçla mücadele, soruşturma, cezai yargılama ve suç tespiti ile infazında yetkili olan merciler ve ilgili ülke kanununda bu amaçlarla kamusal yetki kullanma hakkı ile donatılmış merciler olarak tanımlamaktadır. Dolayısıyla yetkili merciler, yargı kurumları, kolluk kuvvetleri, İçişleri Bakanlığı, İnfaz Kurumları, Adli Tıp Kurumu, Denetimli Serbestlik Kurumu gibi kurum ve kuruluşlardır. Bununla birlikte, uygulama alanının kümülatif iki şarta dayanması nedeniyle, örneğin kolluk görevlilerinin özlük hakları ve gelirlerine dair veriler, Direktifte sayılan amaçlarla veri işlenmesine girmeyeceğinden bu durumda yine GDPR uygulanacaktır[274]. Yine AB sınırlarına giriş, göç ve iltica alanlarında Direktif yerine GDPR uygulama alanı bulacaktır. Ancak sınır geçişleri sırasında kişinin hukuka aykırı şekilde giriş yaptığının tespiti ve bu durumun ilgili üye devlet mevzuatı uyarınca suç teşkil etmesi halinde soruşturmaya konu olacak verilerin

[274] Mark Leiser/Bart Custers, "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680,", **European Data Protection Law Review**, Cilt: 5, Sayı: 3, 2019, ss 367-378, s.370, 371.

işlenmesi, yine 2016/680 sayılı Direktif kapsamında ele alınacaktır. Görüldüğü gibi iki düzenlemenin uygulama arasında geçiş sıklıkla söz konusu olmakta, kimi zaman aynı yetkili kişi, bazı verileri işlerken GDPR diğer veriler açısından Direktife tabi olabilmektedir[275].

Son olarak Direktifin bünyesinde m.2/f. 3 ile Direktifin AB yetki alanı dışında kalan alanlarda ve AB kurum, kuruluş, büro ve dairelerinin kişisel veri işleyişi sürecinde uygulanmayacağı belirtilmiştir. Ufak bir hatırlatma ile Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın m. 4/f. 2 hükmü uyarınca da milli güvenliğe ilişkin hususlar üye devletlerin iç işleyişine ilişkin sorun olarak değerlendirilerek Avrupa Birliği mevzuatı ve yetki alanının dışında bırakılmıştır[276]. Ancak istihbarat örgütleri tarafından işlenen veriler dahi AİHM ve Adalet Divanı tarafından incelemeye konu edilebilmektedir. Özellikle bilgi toplama ve veri işlemenin kanuni zemini olmaması veya demokratik toplumda gereklilik, orantılılık gibi unsurlara aykırı olması halinde, AİHS kapsamında özel hayatın gizliliğini düzenleyen 8. madde kapsamında inceleme yapılmakta, milli güvenlik gerekçesiyle yapılan müdahalelerin denetim dışı bırakılmasına göz yumulmamaktadır[277]. İkinci istisna olan AB kurum ve kuruluşlarının veri işleme sürecinin Direktif kapsamı dışında bırakılması ise AB bünyesinde EUROPOL, Eurojust, OLAF, Schengen Bilgi Sistemi açısından Direktifin uygulanmayacağı anlamına gelmektedir. Bu durumda kişisel verilerin işlenmesi açısından öngörülen özel düzenlemeler uygulama alanı bulacaktır[278].

[275] Juraj Sajfert/Teresa Quintel, "Data Protection Directive (EU) 2016/680 For Police And Criminal Justice Authorities", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, 2019, Erişim Tarihi: 29.04.2021, s.3.
[276] Lynskey, Criminal Justice Profiling, s. 165.
[277] Bkz, AİHM, Klass ve Diğerleri/Almanya, Başvuru No. 5029/71, Karar Tarihi: 06.09.1978, Rotaru v. Romanya, Başvuru no: 28341/95, Karar Tarihi:04.05.2000, , www.hudoc.echr.coe.int, Erişim Tarihi: 29.04.2021.
[278] AB kurum ve kuruluşlarına uygulanacak düzenleme için bkz. Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data.

aa) Profillemenin İlk Aşamasına İlişkin Düzenlemeler: 2016/680 Sayılı Direktif Kapsamında Veri Toplama Sürecinin Hukukiliği ve Veri İşlenmesine İlişkin Temel İlkeler

Profilleme teknolojileri ile veri işlemenin ilk aşaması olan veri toplama süreci, Direktif kapsamındaki ilkelere uygun olmalıdır. GDPR bu kapsamda genel bir düzenlemedir. Ancak suçla mücadele ve yargılamanın amacına ulaşabilmesi için 2016/680 sayılı Direktif ile özel olarak ele alınan bazı ilkeler, GDPR bünyesindeki ilkelere göre farklılıklar içermektedir. Profillemenin ilk aşamasını oluşturan veri toplama sürecine ilişkin Direktif kapsamında öngörülen hükümler bu nedenle aşağıda ayrıca ele alınacaktır.

aaa) Veri İşlemenin Hukuki ve Adil Olması İlkesi

Veri işleme sürecinde temel ilkeler Direktif kapsamında 4. maddede gösterilmiştir. Madde 4/1 (a) veri işlemenin hukuki ve adil olmasının gerekliliğini vurgulamaktadır. Veri işlemenin hukukiliği ilkesi 8. maddede daha detaylandırılmış, GDPR kapsamından farklı olarak veriler yalnızca Direktif kapsamında sayılan amaçlara ulaşmak için gerekli ise ve yetkili mercilerce hukuki bir düzenlemeye dayanarak işlendiyse hukuka uygun veri işleme söz konusudur. Dolayısıyla meşru amaç, rıza gibi GDPR kapsamındaki meşru veri işleme zeminleri, Direktif kapsamında kabul edilmemiştir[279]. Nitekim bireylerin kolluk kuvvetleri ve yargı zemininde verilerinin işlenmesine "gerçek bir rıza" göstermesi mümkün olmayacağından veri işlemenin yalnızca kanuna dayandığı müddetçe meşru kabul edilmesi yerindedir. 8. maddenin 2. fıkrası, veri işlemeyi öngören kanunun veri işleme amacı, hangi verilerin işleneceği ve veri işlemenin kapsamını da belirtmesi gerektiğini vurgulamaktadır. Bununla birlikte veri işleme sürecinin hukuki olması için GDPR başlığında üzerinde durulduğu üzere verilerin meşru amaçla işlenmesinin yanı sıra Avrupa Birliği Temel Haklar Şartı madde 52/1 ve Avrupa İnsan Hakları Sözleşmesi m. 8/1 de dikkate alınarak, demokratik bir toplumda gerekli ve orantılı olması gerektiği de göz önünde

[279]Evik, "Avrupa Birliği Çerçevesinde Kişisel Verilerin Korunması", Sajfert/Quintel, s.6,

bulundurulmalıdır[280]. Veri işlemenin adil olması ilkesi, kişilerin verisinin hukuki iradeleri kırılarak veya kandırma gibi hukuka aykırı yollara başvurarak elde edilmemesini gerektirir. Kişilerin veri işleme sürecine ilişkin risklerden, güvencelerden ve bu süreçte sahip oldukları haklardan haberdar edilmeleri gereklidir[281]. Bununla birlikte 4/1(a) bendinde, GDPR düzenlemesinden farklı olarak "şeffaflık ilkesi" anılmamıştır. Nitekim suçun önlenmesi, kamu düzeninin tesisi ve soruşturmanın amacına ulaşabilmesi için şeffaflık ilkesinin kısıtlanması mümkündür. Bu durum ilgili kişinin bilgilendirilmesine ilişkin Direktif kapsamındaki 13. ve 14. maddelere ve ilgili kişinin verilerine erişimini düzenleyen 15. maddeye de yansımış, bu maddelerde sayılan hakların demokratik bir toplumda gerekli olduğu takdirde, belli bir süre boyunca kısıtlanabileceği belirtilmiştir[282]. Kuşkusuz ki bu kısıtlamalar kanunla öngörülmüş olmalı, bunun yanı sıra geçici bir süre için uygulanmalıdır. Bu kısıtlamaların "açık çek" şeklinde düzenlenmemesi ve AİHS, AİHM ve Adalet Divanı kararlarında belirtildiği üzere ilgili kişi açısından belirli güvenceler öngörmesi gereklidir. Kişi kısıtlanan hakları hususunda hukuki başvuru yollarına sahip olabilmeli ve bu kararlar gözden geçirilmelidir[283].

bbb) Belirli, Açık, Meşru Amaçla Sınırlı Veri İşleme İlkesi

Direktif kapsamında 4/1(b) maddesinde verilerin, özel, açık ve meşru amaçlara yönelik olarak toplanması gerektiği vurgulamıştır. Nitekim özellikle suça ilişkin olarak muğlak amaçlarla veri toplanması, herkesin "olağan şüpheli" olarak kabul edildiği ve tüm verilerin sınırsızca işlendiği bir topluma dönüşme tehlikesi barındıracaktır[284]. 9. maddede amaç sınırına ilişkin daha ayrıntılı bir düzenleme öngörülerek, kişisel verilerin yalnızca Direktif kapsamındaki yetkili mercilerce ve 1. maddede sayılan amaçlarla sınırlı şekilde toplanabileceği, ancak bu amaçların yanı sıra

---

[280] European Union Agency for Fundamental Rights, **Handbook on European Data Protection Law**, ss.64-67.

[281] European Data Protection Board, **Recommendations 01/2021 on the Adequacy Referential under the Law Enforcement Directive**, 02.02.2021, https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf, Erişim Tarihi: 30.04.2021, s.12.

[282] Volkan Dülger/Onur Özkan, "Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: 'Unutulan' Direktifin Kapsamlı ve Karşılaştırmalı Analizi", **Ceza Hukuku Derneği**, Sayı:42, Nisan 2020, ss.85-149, s.100.

[283] European Data Protection Board, **Recommendations 01/2021 on the Adequacy Referential under the Law Enforcement Directive**, s.12.

[284] Dülger/Özkan, s.101.

üye devlet ya da AB mevzuatında başka bir amacın açıkça öngörülmesi halinde, bu amaçla da kişisel veri toplamanın mümkün olduğu belirtilmiştir. Ancak mevzuat gereği Direktifin kapsamı alanına giren amaçlardan başka bir amaçla kişisel verilerin işlenmesi hususunda ana düzenleme olan GDPR hükümleri uygulanacaktır. Yine 9. maddenin 2. fıkrası gereği, GDPR kapsamında amaç ilkesine bir istisna olarak öngörülmüş olan kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veri işlenmesi durumunda yine Direktif'teki amaçların dışına çıkıldığından GDPR hükümleri uygulanmalıdır. Bununla birlikte Direktif 4. maddenin 2. fıkrasında, Direktif kapsamında öngörülen amaçların dışında, yetkili merci veya diğer bir yetkili merciin örneğin "milli güvenlik" gibi bir amaçla veri işlemesine imkân tanınmış, yine bu durumun AB mevzuatı veya üye devletlerin iç mevzuatı ile öngörülmüş olması, gerekli ve orantılı olması aranmıştır.

Dolayısıyla kişisel verilerin yetkili merci tarafından toplanması halinde, bu veri başka amaçlarla veya başka merciler tarafından sınırsız şekilde kullanılamayacaktır. Bu nedenle, amaç sınırlaması uyarınca veriler daha toplanmadan önce, önleyici amaç veya adli amaç şeklinde hangi amaçla işlendikleri açıkça belirlenmiş olmalı ve veriler yalnızca toplanma amaçlarına hizmet edecek şekilde kullanılmalıdır. Suçu önleme amaçlı toplanan veriler, ardından suçu aydınlatma amacına yönelik kullanılmamalıdır[285]. Direktif kapsamında bunun tek istisnası farklı amaçlarla toplanan verilerin kullanılmasına açıkça izin veren kanuni düzenlemelerdir.

ccc) Asgari Veri İşleme İlkesi

Direktif kapsamında 4/1 (c) bendinde düzenlenen ilke gereği, ancak, belirlenen amaca uygun ve bu amacı aşmayacak ölçüde veri işlenmelidir. Bu ilke işlenen kişisel verilerin yalnız niceliğini değil niteliğini de ilgilendirir. Bu hususta GDPR kapsamında yapılan açıklamalar Direktif açısından da geçerlidir. Bununla birlikte, Direktif bünyesinde "amaçla sınırlı" ifadesi yerine "bu amacı aşırı ölçüde aşmayacak ("not excessive") ifadesinin tercih edildiğinin altı çizilmelidir. Doktrinde GDPR lafzından

[285] Kızılırmak, Baran, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", **Kadir Has Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:2, Aralık 2019, ss. 225-261, s.232.

farklı olan bu ifadeye, kolluk kuvvetlerine daha fazla esneklik sağlamak amacıyla yer verildiği belirtilmektedir[286].

ddd) Doğru Veri İşleme İlkesi

Direktif m. 4/1 (d) bendinde ele alınan bu ilkeye göre yetkili merciler işlenen verilerin doğru, eksiksiz ve güncel olduğunu kontrol etmeli ve bu verileri işlemeden önce veri kalitesinden emin olmalıdır. Doğru olmayan verilerin derhal silinmesi yükümlülüğü de bu ilkeden kaynaklanmaktadır. Yine Direktifin 7. maddesinin 2. fıkrası, verilerin aktarılmadan önce doğruluğunun mutlaka kontrol edilmesi gerektiğini belirtmektedir. Direktif bünyesindeki bir diğer fark ise m.7/1 bünyesinde ceza hukuku alanında işlenen verilerin özel niteliği dikkate alınarak, "olgulara dayanan" verilerin "kişisel görüş" veya "değerlendirmelere dayanan" verilerden ayrı şekilde işlenmesi yükümlülüğüdür. Olgular doğrudan gözlemlenebilir ve gerçekliği bizzat kontrol edilebilirken, değerlendirmeler şahsidir ve veri olarak görecelilikleri dikkate alınmalıdır. Şahsi değerlendirme içeren verilerin güvenilir veri olup olmadıkları daha detaylı değerlendirmeye muhtaçtır. Kural olarak doğrudan olgulara dayanmayan tüm veri türler "görüş" olarak kaydedilmelidir. Örneğin bir radar tarafından yapılan hız tespitine ilişkin veri olguya dayalı veri olarak kaydedilir, ancak o sırada bölgede bulunan kolluk görevlisinin "araç gittikçe hızlanıyordu" ifadesi yine olgulardan yola çıkmakla birlikte şahsi gözlem içerdiğinden, görüş olarak işlenmelidir. Benzer şekilde, tanık veya mağdur ifadeleri de görüş şeklinde kaydedilmelidir. Bu bağlamda profilleme sonucu elde edilen bilgilerin ne şekilde kaydedileceği üzerinde durulmalıdır. Bu bilgiler "tekerrür riski", "kaçma şüphesi" gibi tahminler içermektedir. Bu nedenle, profilleme ile varılan sonuçların bir olgu olmadığı kolaylıkla söylenebilir. Direktifin ikili kayıt sistemi gereği, profilleme sonucu türetilen veriler, her ne kadar insan tarafından mantık süzgecinden geçirilmiş gerçek bir görüş olarak nitelendirilemese de Direktifte olgu ve görüş ayrımı dışında bir seçenek tanınmadığından, görüş kapsamında kaydedilecektir[287]. Direktif'te öngörülen olgu ve görüş ayrımı, ceza yargılamalarında soruşturma sırasında dayanılan verilerin gerçeğe uygunluk ve güvenilirliğini test ederken veri sorumlularına yol göstermek açısından büyük önem arz etmektedir.

---

[286] Sajfert/Quintel, s.6

[287] Leiser/ Custers, "The Law Enforcement Directive", s.377.

eee) Sınırlı Süre Veri İşleme İlkesi

Direktif 4/1 (e) bendi gereği toplanan kişisel verilerin veri işlemek ile güdülen amaca ulaşıldığında silinmesi gerekir. Bu madde yine Direktif kapsamındaki 5. madde ile birlikte okunmalıdır. 5. madde veri sorumluları açısından verilere hâlâ ihtiyaç duyup duyulmadığına ilişkin periyodik şekilde denetim yapılması ve GDPR düzenlemesinden daha keskin bir şekilde verilerin silinmesi için belirli zaman aralıklarının öngörülmesini zorunlu tutmaktadır. Yine 20. maddenin 2. fıkrası verilerin silinmesine ilişkin teknik ve örgütsel önlemlerin alınması yükümlülüğünü tekrar vurgulamaktadır[288]. Bununla birlikte saklama süresi Direktif kapsamında açıkça gösterilmemiştir. Bu konuda 29. Çalışma Grubu, saklama süresinin toplanan verinin niteliğine göre değerlendirilmesi gerektiğini belirtmektedir. Her veri kategorisi, varılmak istenen amaca ulaşmada katkılarına göre farklı sürelerde saklanabilir. Bu bağlamda Direktifin 6. maddesi de dikkate alınmalıdır. İlgili madde, mağdur, şüpheli, hükümlü, tanık, bilirkişi gibi kişisel verisi işlenen kişilerin niteliğine göre bir veri kategorisi yapılmasını öngörmektedir. Bunun yanı sıra çocuklara ilişkin verilerin daha kısa süre saklanması hususunda ayrıca özen gösterilmelidir. Veri saklama süreleri, verinin niteliği ve ait olduğu kişilere göre değişebileceği gibi, süre saklamaya ilişkin unsurlar ayrıca objektif kıstaslara göre de belirlenebilir. Örneğin ağır suçları tespit için daha uzun süreli veri saklanması, objektif niteliktedir[289]. Bununla birlikte önleyici amaçla veri toplanması halinde, istenilen amaca ulaşmak için verilerin ne kadar süre saklanması gerektiğini tespit daha güçtür. Suç öncesi alanda soruşturma sürecinde olduğu gibi örneğin kovuşturmaya yer olmadığı kararı gibi bir kararın alınması ve ardından sürecin tamamlanarak verilerin silinmesi söz konusu olmamaktadır. Bu bağlamda suçu önleme amacıyla saklanan verilerin periyodik bir şekilde denetlenmesi zorunluluğu ayrıca önem taşımaktadır. Verilerin saklanmasının devamlılığına karar verildiği takdirde, bu durumun gerekçeleri mutlaka ortaya konulmalı, bu gerekçeler Kişisel Verileri Koruma Kuruluna sunulmaya hazır bir şekilde kaydedilmelidir. 29. Madde Çalışma grubu verilerin saklanmasının gerekli olup olmadığının

[288] Kuner/Bygrave/Docksey, s. 318.
[289] Article 29 Working Party, **Opinion on Some Key Issues of the Law Enforcement Directive**, 17/EN WP 258, 29.11.2017, s.5.

değerlendirilmesi ve denetlenmesinde, kişisel verileri korumakla yetkili kurul görevlilerinin de sürece katılmasını tavsiye etmektedir[290].

bb) Profillemenin Analiz ve Karar Alma Aşamasına İlişkin 2016/680 Sayılı Direktif Kapsamındaki Düzenlemeler

aaa) Direktif m. 11 Kapsamında Yalnızca Otomatik İşleme Faaliyetine Dayalı Karara Tabi Olmama

Otomatik veri işleme ve karar vermeye ilişkin Direktif ile GDPR kapsamında paralellik gösteren düzenlemeler bulunmaktadır. Bu bölümde örtüşen düzenlemeler açısından GDPR başlığında yapılan açıklamalara göndermekle yapılmakla yetinilecek, iki düzenleme açısından farklılık arz eden durumlar üzerinde durulacaktır.

Öncelikle profillemenin tanımı Direktif m. 3/4'te GDPR ile aynı şekilde yapılmıştır. Profilleme de dâhil olmak üzere yalnızca otomatik yollarla karar almaya ilişkin düzenleme ise Direktif'in 11. maddesinde düzenlenmiş olup bu madde lafzı gereği, bir hak olarak değil, münhasıran otomatik karar alma yasağı olarak düzenlenmiştir. Nitekim maddede, kişi üzerinde olumsuz hukuki sonuç doğuran veya kişiyi ciddi şekilde etkileyen salt otomatik veri işlemeye dayalı karar almanın ilgili üye devlet ve AB mevzuatı uyarınca açıkça aksi öngörülmediği müddetçe yasak olduğu belirtilmektedir. Bu madde kapsamına giren bir uygulamanın söz konusu olması için, kişisel verilerin işlenmesi, insani müdahale söz konusu olmadan, salt otomatik şekilde karar alınması, bu kararın kişinin hukuki statüsü ve haklarını olumsuz yönde etkilemesi veya ciddi sonuçlar doğurması aranmaktadır. Bu şartlar GDPR kapsamında düzenlenen m. 22 ile paralellik gösterdiğinden, GDPR kapsamında yapılan açıklamalar Direktif açısından da geçerlidir.

---

[290] **Ibid**, s.4.

aaaa) Direktif m. 11 Kapsamında Otomatik İşleme Dayalı Karar Almanın Meşruiyet Zemini

Diretif m. 11 kapsamında GDPR m.22 f. 2'de otomatik karar almayı meşru kılan sözleşme kurulması ve ifası için gerekli olma ve kişinin açık rızasına dayanma sebeplerine yer verilmemiştir. Nitekim özellikle veri sorumlusu ile ilgili kişi arasındaki güç dengesizliğinin daha belirgin olduğu suçla mücadele veya ceza muhakemesi alanında, rızanın bir hukuka uygunluk zemini olarak kabul edilmemesi yerindedir[291]. Yine kolluk kuvvetleri veya yargı kurumları ile kişi arasında bir sözleşme ilişkisi bulunması da söz konusu olmadığından, sözleşmenin kurulması ve ifası, otomatik karar alma sürecini meşru kılan nedenler arasında sayılmamıştır.

İlgili maddede tek hukuka uygunluk sebebi olarak üye devlet veya AB mevzuatında münhasıran otomatik profillemeyi mümkün kılan açık düzenleme bulunması aranmakta, bunun yanı sıra ilgili düzenlemenin ilgili kişilerin hak ve özgürlüklerini garanti altına alması gerektiği, en azından insani müdahale talep etme hakkını içermesi gerektiği belirtilmektedir[292].

bbbb) Direktif m. 11 Kapsamında İlgili Kişiye Tanınan Haklar

Son olarak Direktifin 11. maddesi kişilerin salt otomatik veri işlemeye dayalı bir karara tabi tutulması halinde kararın gerçek kişi tarafından incelenmesi hakkını tanımakla birlikte, GDPR 22. maddede olduğu gibi ayrıca ilgili kişinin kendi görüşünü açıklama ve karara itiraz etme hakkını öngörmemiştir. Bununla birlikte 38. gerekçe maddesi salt otomatik veri işleme sürecinin belli güvenceler içermesi gerektiğini belirtmekte, bu güvenceler arasında kişinin insan müdahalesi talep edebilmesinin yanı sıra, karara ilişkin kendisine bir açıklama yapılmasını, görüşünü açıklayabilmesini ve karara karşı çıkabilmesini saymaktadır. Böylelikle kişi pek çok hata ve ön yargı içermesi mümkün olan algoritmaların kararına karşı gerçek bir itiraz ileri sürebilecektir[293]. Bununla birlikte ilgili hakların metin içerisinde değil, bağlayıcı

[291] Article 29 Working Party, **Opinion on Some Key Issues of the Law Enforcement Directive**, s.12.
[292] Kuner/Bygrave/Docksey, s.539.
[293] Article 29 Working Party, **Opinion on some key issues of the Law Enforcement Directive**, s.15.

olmayan gerekçe kapsamında ele alınması, üye devletlerin farklı düzenlemeler yapmasına imkân tanımış, hakların korunması açısından GDPR düzenlemesine kıyasla daha güvencesiz bir zemin oluşturmuştur[294].

cccc) Direktif m.11 Kapsamında Özel Nitelikli Veri İşleyen ve Ayrımcılığa Yol Açan Profilleme Uygulamalarına Karşı Önlemler

GDPR m. 22 kapsamında olduğu gibi Direktif m. 11'de de ayrımcılığa yol açma potansiyeline sahip özel nitelikli verilere dayanarak otomatik karar alınması yasaklanmıştır. Bunun tek istisnası, üye devletler tarafından özel nitelikli veri işlemeye izin veren düzenlemeler yapıldığı hallerdir. Bu düzenlemeler uyarınca kişi hak ve özgürlükleri güvence altına alınmalı, özel nitelikli veri işleme için meşru bir amaç gösterilmelidir. Bununla birlikte GDPR düzenlemesi özel nitelikli verilerin işlenmesi için 9. maddedeki açık rıza hukuki meşruiyet sebebine referans vermekte iken, Direktif kapsamında açık rıza özel nitelikli veriye dayanarak profilleme yapılmasında hukuka uygunluk nedeni olarak sayılmamıştır. Burada yine güç eşitsizliğinin söz konusu olduğu idari ve ceza hukuku alanında, özel nitelikli veri işlenmesine gösterilen rızanın gerçek bir rıza olmayacağı kabul edilmiştir. Nitekim Adalet Divanı, Schwarz v. Bochum kararında, AB vatandaşlarının pasaport alımı sırasında parmak izlerinin alınmasına ilişkin yaptığı incelemede, parmak izi vermeyen kişilerin seyahat etmeleri engellendiğinden, gerçek anlamda rızadan bahsedilemeyeceğini, rızanın bu tür durumlarda hukuka uygunluk sebebi teşkil etmeyeceğini belirtmiştir[295].

Yine GDPR düzenlemesinden farklı olarak 11. maddede ayrımcılık yasağına ilişkin özel bir düzenleme daha öngörülmüştür. Direktif'in m. 11/3 hükmü uyarınca gerçek kişilere yönelik özel nitelikli verilere dayanarak ayrımcılık yapılmasına yol açan profillemenin yasak olduğu tekrar vurgulanmıştır[296]. Bu düzenleme, yalnız özel nitelikli veri kullanılmasını yasaklamamakta, ayrıca profillemenin sonucunu da

---

[294] Sajfert/Quintel, s.10.

[295] AB Adalet Divanı, Michael Schwarz v. Stadt Bochum, Case C-291/12, EU:C:2013:670, 17.11.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0291&from=EN, Para 32, Erişim Tarihi: 30.04.2021.

[296] Article 29 Working Party, **Opinion on Some Key Issues of the Law Enforcement Directive**, s.13.

dikkate almaktadır. Profilleme sonucunda özel nitelikli verilere dayalı bir ayrımcılığın doğması halinde, söz konusu uygulama hukuka aykırı kabul edilecektir.

Ceza hukuku alanında kullanılan profilleme teknolojileri açısından en önemli hukuki sorunlardan biri bu teknolojilerin ilgili kişileri bireysel özelliklerini gözetmeksizin belli gruplar ile ilişkilendirmesi ve gruba aidiyetleri nedeniyle otomatik olarak tehlikeli kişi olarak addetmeleridir. Nitekim COMPAS teknolojisi örneğinde, Amerika'da pek çok siyahi kökenli kişi bu durumdan olumsuz yönde etkilenmiş ve siyahi kişiler için öngörülen yüksek risk puanlarına otomatik olarak tabi olmuşlardır. Bu nedenle hatalı şekilde "mükerrer olma riski yüksek" kişiler olarak değerlendirilmeleri söz konusu olmuştur. Bu durumun profilleme algoritmalarını eğitmede kullanılan veri setinin ayrımcı veriler içermesi sebebiyle mi yoksa algoritma yapısının öngörülemez şekilde ayrımcı bağlantılar kurması sebebiyle mi gerçekleştiği, kullanılan teknolojilerin derin öğrenme modeline dayanan karmaşık yapısı nedeniyle tespit edilememiştir[297]. Gruba aidiyet üzerinden kolektif sorumluluk yaratan bu tür profilleme teknolojileri, kuşkusuz ki ceza hukukunda temel ilke olan kusur ilkesi ve ceza sorumluluğunun şahsiliği ilkelerini de ihlal etmektedir. Ayrımcılık yasağına ilişkin düzenlemeler, bu tür ihlallere yol açan profilleme teknolojilerinin işleyişine yönelik kesin bir çözüm sunmamaktadır. Ancak yine de profilleme teknolojilerinin dayandığı verilerin ve vardıkları sonucun kontrol edilmelerini gerektirmeleri nedeniyle Direktif kapsamında öngörülen bu hükümler büyük önem taşımaktadır.

bbb) Direktif Kapsamında Şeffaflık Hakları

Direktifin suçla mücadele ve ceza muhakemesi sürecini düzenlemesi nedeniyle şeffaflık hakları olarak nitelendirilen bilgi edinme ve verilere erişebilme hakları GDPR kapsamından farklı şekilde ele alınmıştır. GDPR 13/2 (f) bendi ve 14/2 (g) bendi ve son olarak 15/1 (h) bendinde açıkça öngörülen, salt otomatik karar alma kapsamında alınan kararın varlığı, bu teknolojilerin işleme mantığı ve otomatik veri işleme sürecinin ilgili kişiler açısından önemi ve öngörülen sonuçları hakkında "anlamlı" bilgi edinebilme haklarına, Direktif kapsamında yer verilmemiştir.

---

[297] Sascha van Schendel, "The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI", İçinde **Regulating New Technologies in Uncertain Times**, Ed. Leonie Reins, Springer: The Hague, Mart 2019, s.225-240, s.237.

aaaa) İlgili Kişiyi Bilgilendirme Yükümlülüğü

Direktif kapsamında bilgilendirme yükümlülüğü m. 13 kapsamında düzenlenmektedir. Bilgilendirme yükümlülüğü çerçevesinde özellikle 13/2 (d) bendi dikkate alınmalıdır. Bu bent uyarınca, veri toplama süreci, ilgili kişinin bilgisi olmaksızın gerçekleştirildiği takdirde, kişiye veri işlemenin hukuki zemini, hangi veri kategorilerinin toplandığı, verilerin ne kadar süreyle saklanacağının yanı sıra ek bilgiler sunulması zorunludur. Bununla birlikte aynı maddenin 3. fıkrası üye devletlere bilgi sağlama yükümlülüğünü erteleyen, kısıtlayan hatta tamamen engelleyen düzenlemeler yapma hususunda takdir yetkisi tanımıştır. Bu sınırlamalar, demokratik bir toplumda gerekli ve orantılı olmalı, maddede sınırlı şekilde sayılan soruşturma ve kovuşturmanın işleyişi, suçu önleme, suçu tespit etme gibi amaçlara ulaşmak için öngörülmelidir. Bunun yanı sıra söz konusu sınırlamalar yalnızca m. 13/2 kapsamında öngörülen bilgiler açısından söz konusudur. Buna göre kişinin verilerini işlemeyi mümkün kılan meşru sebep, verilerinin ne kadar süreyle saklanacağı, bu verilerin paylaşıldığı kişi ve kurumlara dair bilgilerin paylaşılması kısmen veya tamamen kısıtlanabilir. Ancak m.13/1 kapsamında sayılan veri sorumlusuna ilişkin bilgilerin ve iletişim verilerinin, veri işlemenin amacının, kişisel verileri koruma kurumuna şikâyet hakkının, kişinin verilere erişim ve verilerini silmeye ilişkin haklarının ilgili kişiye her hâlükârda mutlaka açıklanması gereklidir[298]. Son olarak üye devletler bilgilendirme yükümlülüğünü kısıtlayabilse de m. 24/1(e) gereği profilleme faaliyetlerine ilişkin mutlaka kayıt tutmak zorundadır[299]. Bu düzenleme özellikle temel haklara yoğun müdahale içeren profilleme teknolojilerine dayalı işlemlerin kayıt altında olması, takip edilebilmesi ve hesap verilebilirlik ilkesinin tesis edilmesi açısından büyük önem taşımaktadır.

bbbb) İlgili Kişinin Verilere Erişim Hakkı

Kişilerin verilerine erişimini düzenleyen 14. madde ise kural olarak verilerin işlenme amacı, meşru zemini, hangi veri kategorilerinin işlendiği ve bu verilere hangi kaynaktan erişildiği ve verilerin kimlerle paylaşıldığı gibi hususlara erişimi mümkün

[298] Ibid, s.16, 17.
[299] Article 29 Working Party, **Opinion on Some Key issues of the Law Enforcement Directive**, s.15.

kılmaktadır. Bununla birlikte erişim hakkı 15. maddede sınırlanmış ve 13. maddeye paralel şekilde belli amaçlarla ve kanuna dayanarak kısıtlama ve tamamen engellemeye ilişkin bir düzenleme öngörülmüştür. 15. maddeye dayanılarak alınan erişim hakkına sınırlama ve engelleme kararlarının maddi ve hukuki gerekçelerinin kaydedilmesi gereklidir. Yine m. 15/3 gereği ilgili kişilere verilerine erişim hakkının engellendiği veya kısıtlandığını ve bunun nedenlerini açıklama yükümlülüğü getirmektedir. Ancak örneğin soruşturma ve kovuşturmanın amacına ulaşmasına engel teşkil edecekse bu tür bir açıklamadan imtina edilebilir. Son olarak 15. madde gereği kişilere söz konusu kararlara karşı hukuki yola başvurma hakları veya kişisel verileri koruma kurumlarına şikâyet hakları bulunduğunu hatırlatma yükümlülüğü öngörülmüştür.

Söz konusu kısıtlama ve engellemelere ilişkin maddeler, sınırsız ve genel bir yasak düzenlenme yetkisi tanımamaktadır. Bu yöndeki kararlar, kanunda öngörülen düzenlemeye dayanılarak, olayın şartları dikkate alınarak ve gerekçeli şekilde alınmalıdır. Nitekim verilere erişim hakkını tamamen kısıtlayan kararlar, hakkın özünü ihlal etmektedir. Bu nedenle, veriye erişimi ve bilgilendirme hakkını kısıtlamayı içeren kararlar, bu kararın alınmasındaki tehlike geçer geçmez, örneğin soruşturmanın ilerlemesinin tehlikeye düşme ihtimali ortadan kalkar kalkmaz ilgili kişi tarafından kullanılabilmelidir[300].

cccc) Yeni Bir Kanun Yolu Olarak Sınırlandırma Rejimine Karşı Kişisel Verileri Koruma Kurullarına Başvuru Hakkı

Direktif kapsamında 13. ve 15. maddelerde öngörülen engelleme ve kısıtlamalara karşı, bu hakların dolaylı olarak kullanılabilmesi için üye devletler 17. madde kapsamında Kişisel Verileri Koruma Kurullarına başvuru hakkını düzenlemek zorundadır. 17. maddede sayılan bu hak, Kişisel Verileri Koruma Kurullarına yapılacak genel şikâyet hakkından ayrı bir başvuru yolu olup bu kurullar aracılığıyla özel olarak kısıtlama kararlarının tekrar gözden geçirilmesini mümkün kılmaktadır[301].

[300]AB Adalet Divanı, Tele2 Sverige and Watson and Others, C 203/15 and C 698/15, EU:C:2016:970, 21.12.2016, para. 121. Verilere erişim hakkına ilişkin diğer kararlar için bkz Adalet Divanı, Rijkeboer, C-553/07, EU:C:2009:293, 07.05.2009, paras.69-70, Schrems, C-362/14, EU:C:2015:650, 06.10.2015, para. 95, https://eur-lex.europa.eu, Erişim tarihi: 01.05.2021.

[301] Article 29 Working Party, **Opinion on Some Key Issues of Law Enforcement Directive**, s.23.

Direktifin getirdiği en yenilikçi düzenlemelerden biri olan bu düzenleme, ikili bir koruma mekanizması öngörerek, ilkin veri sorumlularını doğrudan bilgilendirme ve erişim hakkını tanımakla yükümlü tutmaktadır. Hakların kısıtlanması ya da reddedilmesi halinde Kişisel Verileri Koruma Kurulları da sürece katılmaktadır. Böylelikle bağımsız bir kurum tarafından sürecin yeniden gözden geçirilmesi ve hakların doğrudan veya dolaylı şekilde garanti altına alınması mümkün kılınmıştır[302].

Bununla birlikte, kısıtlama kararlarının yargı yetkisi çerçevesinde bağımsız hâkimlikler ve mahkemeler tarafından verildiği durumlarda, Kurulların mahkeme kararlarını denetleme yetkisi olup olmadığı tartışmalıdır. Bu durumda Direktifin 45. maddesinin ikinci fıkrası dikkate alınmalıdır. İlgili hükümde, üye devletlere bu hususta takdir yetkisi tanınmış, bağımsız yargı organlarının yargısal faaliyetleri sırasında kişisel verilere ilişkin aldıkları kararları denetimin, Kurulların yetki alanı dışında bırakılabileceği belirtilmiştir. Bu durumda, yerel mevzuatlar gereğince, ceza muhakemesi sürecinde işlenen verilere erişim ve bilgilendirme hakları sınırlandırıldığı takdirde Kişisel Verileri Koruma Kurullarına, bu kararları inceleme yetkisi tanınmayabilir[303]. Ancak yargı organları dışında veri işlenmesi halinde Kurul her halukarda yetkili olacak ve Direktif kapsamındaki ikili inceleme ve değerlendirme mekanizması geçerli olacaktır.

Kolluk faaliyetleri ve yargı sürecinde kişisel verilerin işlenmesine dair detaylı düzenlemeler öngören 2016/680 sayılı Direktif, hukuk devletinin tesisi açısından oldukça önemli bir adımdır. Direktif kapsamında, gittikçe yaygınlaşan profilleme teknolojilerinin mekanik bir şekilde karar almasını yasaklayan 11. madde büyük bir önem taşımaktadır. İlgili madde, gerçek bir kişi tarafından denetimi zorunlu tutmaktadır. Yine Direktif kapsamında, verilere erişim ve bilgi edinme haklarının öngörülmesi, bu haklara ilişkin sınırlamalar ve tamamen kısıtlamalar mümkün kılınsa da, bu sınırların da sınırının çizilmesi çok önemli bir adımdır.

[302] Sajfert/ Quintel, s.13.
[303] **Ibid**, s.15.

d) Değerlendirme

Gerek GDPR, gerekse Direktif kapsamında ceza muhakemesinde adil yargılanma ilkesinin açık yargılama ilkesiyle paralellik gösteren şeffaflık hakları büyük önem taşımaktadır. Ancak şeffaflığın gerçek anlamda tesisi için profilleme teknolojilerinin kural temelli, takip edilebilir modellere dayanması gerekir. Bu teknolojiler eliyle varılan sonuçlara ne şekilde ulaşıldığının tespiti güç olan "kara kutu" modeline dayanması halinde, veri sorumluları, hâkimler veya Kişisel Verileri Koruma Kurulu tarafından yapılan denetim, şekli bir denetim olacaktır. Bu durumda, profilleme ile varılan sonuçların anlaşılmaksızın, de facto şekilde kabul edilmesi söz konusu olacak, insan tarafından gerçekleştirilen denetim anlamını yitirecektir.

GDPR m. 22 ve Direktif m. 11 kapsamındaki profilleme düzenlemeleri açısından diğer bir sorun, ilgili maddelere başvurmanın, ancak kişinin bireysel olarak süreçten etkilenmesi ve hakkında profillemeye dayanılarak ciddi etki doğuran hukuki veya benzer nitelikte kararların alınması halinde mümkün olmasıdır. Ancak, kimi profilleme türleri bizzat belirli kişileri değil, örneğin risk taşıyan mahalleleri tespit etmekte kullanılmakta, bu durumda, GDPR m. 22 veya 2016/680'de aranan ilgili kişiyi ciddi şekilde etkileyen bir kararın varlığı unsurunun karşılanıp karşılanmadığı tartışmalı hale gelmektedir. Bu durumda, ilgili kişilerin bölgeye çok sayıda kolluk görevlisi seferber edilmesinin, profilleme teknolojilerinin vardığı sonuca dayanılarak alınan bir karar olduğundan haberdar olmaları güçtür. Sürece ilişkin bilgi edinmenin güçlüğünün yanı sıra, bu durumun kişiler üzerinde doğan doğrudan ve dolaylı sonuçlarını kanıtlamak daha güçtür[304]. GDPR ve Direktif kapsamındaki düzenlemeler, belirli bir kişinin haklarına yönelik tehlikenin doğduğu aşamada uygulanmakta, kişilerin üzerinde ciddi bir etki veya hukuki statülerinde değişiklik oluşmasını beklemektedir. Bu nedenle, söz konusu hakların, grup ve bölge profillemelerine karşı bir koruma oluşturmadığı dikkate alınmalı[305], doğrudan ihlal beklenmeksizin bu teknolojilerin kullanımına ilişkin sınırlamalar öngören daha geniş kapsamlı düzenlemeler yapılmalıdır.

---

[304] Lynskey, Criminal Justice Profiling, s. 174.

[305] Maja Brkan, "Do Algorithms Rule the World? Algorithmic Decision-making in the Framework of the GDPR and Beyond", **International Journal of Law and Information Technology**, Cilt:27, Sayı:2, 2019, ss.91-121, s.100.

B. Türkiye Kişisel Verilerin Korunması Mevzuatında Profilleme Teknolojilerine İlişkin Düzenlemeler

Türk mevzuatında 2010 yılında yapılan Anayasa değişikliği ile Anayasanın özel hayatın gizliliğini düzenleyen 20. maddesinde kişisel verilerin korunması ayrıca güvence altına alınmıştır. Bu madde uyarınca herkes kişisel verileri hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve işlenme amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkında sahiptir. Kişisel verilerin korunmasına ilişkin Türkiye açısından diğer önemli kaynak, 02.05.2016 tarihinde onaylanan 108 Sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi"dir. Bu sözleşmenin ardından 7 Nisan 2016 tarihinde Kişisel Verilerin Korunması Kanunu[306] ("KVKK") ile bu hakkın nasıl kullanılacağına ilişkin usul ve esaslar daha detaylı şekilde düzenleme altına alınmıştır.

Kişisel verilerin korunmasına ilişkin önemli düzenlemeler içeren KVKK kapsamında bir korumanın söz konusu olması için, kuşkusuz ki bir verinin öncelikle kişisel veri olması gereklidir. Kişisel verinin tanımı KVKK m. 3/1 (d) bendinde GDPR ile benzer şekilde "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklinde yapılmıştır. Dolayısıyla yalnızca gerçek kişilere ait kişisel veriler açısından Kanun uygulanacaktır. Belirli ve belirlenebilir ifadeleri açısından GDPR kapsamında yapılan tartışmalar KVKK açısından da geçerlidir. Bununla birlikte, Kanun'da GDPR düzenlemesinden farklı olarak kişisel veriler tanımlanırken "knowledge" kavramına tekabül eden "bilgi" kavramına başvurulduğu görülmektedir. GDPR başlığı altında detaylı şekilde ele alındığı üzere bilgi ifadesi ham halde yer alan verilerden daha dar bir ifadedir. Bilgi, düşünme ve edinilen verileri rasyonel bir şekilde akıl süzgecinden geçirmeyi gerektirir[307]. Derhal dijital olarak kaydedilebilen veriden farklı olarak, bilgi neden ve niçin sorularına yanıt aramayı içerir. Bu nedenle henüz mantık süzgecinden geçirilmemiş veri kavramını bilgi ile eş değer tutmak yerinde değildir.

[306] Kanun No : 6698, Resmi Gazete T.: 07.04.2016, Sayı : 29677.
[307] Purtova, s. 51.

Bir verinin kişisel veri kabul edilmesi ile birlikte, verinin işlenmesinde uygulanacak temel ilkeler KVKK m. 4 kapsamında ele alınmıştır. Bu madde kapsamında ele alınan hukuka ve dürüstlük kurallarına uygun olma, amaca uygunluk, doğru ve asgari veri işleme ilkeleri açısından GDPR kapsamında yapılan açıklamalar KVKK açısından da geçerlidir. Dolayısıyla veri toplanma aşamasından, profillemenin uygulandığı ve sonuç verilerin işlendiği tüm aşamalarda bu ilkelere riayet edilmesi gerekir.

1. KVKK Kapsamında Profillemeye İlişkin Düzenlemeler ve Şeffaflık Hakları

İşlenen verilerin belirli ve belirlenebilir şekilde kişisel veri olduğunun tespit edilmesinin ardından, bu verilere dayanılarak profilleme yapılması üzerine KVKK kapsamında çeşitli hükümler devreye girecektir. Profillemeye ilişkin KVKK kapsamında ele alınan düzenlemeler, GDPR ve 2016/680 sayılı Direktif'e göre oldukça sınırlıdır. Örneğin, GDPR ve Direktif'ten farklı olarak KVKK bünyesinde profillemenin tanımına yer verilmemiştir. Profillemeye ilişkin temel düzenleme KVKK m. 11/ 1 (g) bendi ile sınırlıdır. Bu bende göre ilgili kişinin, "işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı bulunduğu görülmektedir.

a) KVKK m. 11 Kapsamında Otomatik Sistemler Vasıtasıyla Gerçekleştirilen Veri Analizinin Hukuki Zemini

KVKK m. 11 kapsamında yapılan düzenleme GDPR madde 22 ve 2016/680 sayılı Direktif m.11'e göre farklılıklar barındırmaktadır. Öncelikle bu maddenin kişisel verilerin münhasıran otomatik sistemler vasıtasıyla işlenmesine ilişkin yasaklayıcı bir madde olmadığı görülmektedir. GDPR ve Direktif kapsamında bu tür bir işleme için meşru amaçlar açıkça gösterilmişken ilgili maddede profilleme için meşruiyet koşulları gösterilmemiştir. Bu durumda, KVKK m. 5/2 çerçevesinde düzenlenmiş genel meşruiyet sebepleri olan açık rıza, kanunda açıkça öngörülmüş olma, sözleşmenin kurulması ve ifası için doğrudan doğruya ilgili ve gerekli olma, veri sorumlusunun hukuki sorumluluğu için gerekli olma, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, veri sorumlusunun meşru menfaati

için gerekli olma nedenlerinin profilleme açısından da geçerli olacağı söylenebilir. Bununla birlikte, meşruiyet sebepleri için AB mevzuatı çerçevesinde yapılan incelemede ele alınan çekinceler KVKK açısından da geçerlidir. Örneğin bir satım sözleşmesi sırasında işlenen verilerin, ardından aynı kişiye yönelik bireyselleştirilmiş reklamların gösterilmesi amacıyla kullanılması durumunda, artık "bir sözleşmenin ifası için gerekli olma" meşru sebebinin geçerli olmayacağı göz önüne alınmalıdır. Yine özellikle ürün veya hizmetin sunulmasında rızanın ön şart olduğu aksi halde hizmet vermenin reddedildiği durumlarda geçerli ve özgür bir rızanın söz konusu olamayacağı dikkate alınmalıdır[308]. Bunun yanı sıra tarafların eşit konumda olmadığı, işçi-işveren ilişkisi benzeri ilişkilerde, eşitsiz konumdaki kişiler üzerinde muhtemel olumsuz sonuçların doğabileceği dikkate alınarak, rızanın özgür bir iradeye dayanmayacağı dikkate alınmalıdır[309]. Suçla mücadele veya yargılama sırasında, kişi ile kolluk görevlileri veya yargı mercileri arasındaki ilişki açısından da eşitsiz bir güç ilişkisi söz konusu olduğu tartışmasızdır. Bu nedenle ceza muhakemesi alanında gerçekleştirilen profilleme açısından da açık rıza hukuki zeminine hiçbir şekilde dayanılamayacaktır.

b) KVKK m. 11 Kapsamında Münhasıran Otomatik Sistemler Vasıtasıyla Kişi Aleyhine Doğan Sonuca İtiraz etme Hakkı

Bu maddede GDPR ve Direktifteki düzenlemeden farklı olarak, maddenin uygulama alanı doğması için verileri otomatik olarak analiz edilen kişinin aleyhine bir sonuç doğması yeterli olacaktır. Bu bağlamda, KVKK m.11 düzenlemesinin kapsamının daha geniş olduğunu söylemek mümkündür. Bu maddede otomatik sistemler vasıtasıyla analiz yapılması yeterli görülmüş, bu analize dayanılarak ayrıca "karar alınması" aranmamıştır. Yine analiz sonucu kişinin aleyhine sonuç doğması yeterlidir, bu sonucun hukuki bir statü değişikliği veya benzer ağırlıkta bir etki doğurmasına gerek yoktur. Bu bağlamda örneğin kişisel verilerin analiz edilerek belli grupların oluşturulduğu ve kişinin bu gruba aidiyetinin tespiti edildiği anda dahi kişinin aleyhine bir sonuç doğduğunu iddia etmek mümkündür. Nitekim ceza

---

[308] Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf, Nisan 2018, Erişim Tarihi: 01.05.2021, s.27.

[309] Kişisel Verileri Koruma Kurumu, **Açık Rıza**, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf, Erişim Tarihi: 01.05.2021, s.7.

muhakemesi alanında "risk grubu" olarak görülen bir gruba aidiyetin belirlenmesi ile kişinin ayrımcı muameleye maruz kalma riski doğmaktadır. Bu durum "aleyhe sonuç" olarak kabul edilebilecek, ayrıca "tutuklamanın devamı", "arama kararı", "durdurma tedbirinin uygulanması" gibi kararların alınması gerekmeyecektir. Maddenin gerekçesinde de bir çalışanın performansının otomatik bir sistem vasıtasıyla analiz edilmesine itiraz hakkı bulunduğu gösterilmiş, kişinin ayrıca performans kriterine dayanarak iş sözleşmesinin sona erdirilmesi gibi bir kararın alınması aranmamıştır[310]. Bununla birlikte, maddenin kapsamının belirlenmesinde, elbette gelecekte Kişisel Verileri Koruma Kurulunun vereceği kararlar da etkili olacaktır.

c) KVKK m. 11 Kapsamında İnsan Müdahalesi Talep Etme Hakkı

KVKK m. 11 çerçevesindeki düzenlemede göze çarpan diğer bir fark, bu düzenlemenin salt otomatik sistemler vasıtasıyla analiz yapıldığı hallerde, ilgili kişilere "insan tarafından müdahale talep etme" hakkını tanınmamış olmasıdır. İlgili 11/1(g) maddesinin lafzı "İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı şeklinde düzenlenmiştir. Dolayısıyla kişi, hakkında salt otomatik sistemler vasıtasıyla aleyhine bir karar verildiğinde, bu karara itiraz edebilecektir. İtirazın ne şekilde inceleneceği açık şekilde düzenlenmemekle birlikte, maddenin konuluş amacından, itirazın tekrar otomatik olarak incelenmeyeceği, itirazın ardından, insani bir müdahalenin gerçekleşeceğini kabul etmek gerekir. Ancak bu durumda, insan müdahalesi yalnızca süreç sonunda, karar alındıktan sonra ve itiraz üzerine gerçekleşecektir.

d) KVKK Kapsamında Veri İşlemede Şeffaflığa İlişkin Düzenlemeler

KVKK kapsamında profillemeye ilişkin şeffaflık hakları açısından da farklar bulunmaktadır. GDPR 13/2 (f) bendi ve 14/2 (g) bendi ve 15/1 (h) bendinde, ilgili kişilere haklarında 22. madde kapsamında kalan otomatik yollarla verilen bir karar var ise bu kararın varlığı, kullanılan teknolojilerin işleme mantığı ve otomatik karar alma sürecinin kişiler açısından önemi ve öngörülen sonuçları hakkında "anlamlı" bilgi

[310] Volkan Dülger, Bilişim, **Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı**, Güncellenmiş 7. Baskı, Seçkin Yayınevi: Ankara, 2021, s.672.

verilmesinin öngörülmüşken, KVKK kapsamında bu tür açık düzenlemelere yer verilmemiştir. Ancak bu hakların açıkça düzenlenmemiş olması nedeniyle, KVKK kapsamında bu hakların talep edilemeyeceği sonucuna ulaşılmamalıdır. Nitekim KVKK m.10, veri sorumluları açısından ilgili kişilere kişisel verilerin hangi amaçla işleneceğini, kimlere ve hangi amaçla aktarılabileceğini, veri toplamanın hukuki nedenini ve metodunu açıklama yükümlülüğü getirmiştir[311]. Oysa somut olayın özelliğine göre, pek çok durumda bilgilendirmede yer alması gereken hususlar KVKK m. 10 ve 11'de belirtilenden daha fazla açıklama gerektirebilecektir[312]. Aydınlatma yükümlülüğünün yerine getirilmemesi halinde veri sorumluları açısından tazminat yükümlülüğünün de doğacağı dikkate alındığında, yükümlülüğün kapsamı daha geniş ve öngörülebilir şekilde düzenlenmelidir. Bu bağlamda, GDPR m.13 ve 14'te olduğu gibi kişinin verileri dayalı profilleme yapıldığı, profilin işleyiş modeli ve ilgili kişi üzerinde ne tür etkiler doğurabileceğinin açıklanması yükümlülüğünün açıkça öngörülmesi yerinde olacaktır.

Profilleme uygulamalarını besleyen verilerin, yalnızca ilgili kişi tarafından doğrudan paylaşılmadığı, genellikle pek çok ayrı kaynaktan veri edinildiği dikkate alınmalıdır. Nitekim GDPR m. 14 ile doğrudan ilgili kişi tarafından edinilmeyen, diğer kaynaklardan toplanan veriler açısından da veri sorumlularına bilgilendirme yükümlülüğü getirilmiştir. KVKK kapsamında ise doğrudan edinilmemiş kişisel verilere ilişkin bilgilendirme yükümlülüğü öngören özel bir düzenlemeye yer verilmemiştir[313]. Bununla birlikte, kanunda böyle bir ayrım açıkça görülmese de Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in[314] 6. maddesinde bu hususta bir düzenleme öngörüldüğü görülmektedir. "Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü" başlıklı bu madde uyarınca, veri sorumluları, kişisel verileri ilgili kişiden elde etmedikleri halde de ilgili kişiyi makul bir süre içerisinde aydınlatmakla yükümlüdür.

---

[311]Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü", **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı:2, 2019, ss. 41-65, s. 50.

[312] Nafiye Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXXV, Sayı: 2, 2017, ss. 765-790, s.274.

[313] Aşıkoğlu, "Aydınlatma Yükümlülüğü", s. 51.

[314] Resmi Gazete Sayı:30357, T.10.03.2018, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm, Erişim Tarihi: 05.05.2021.

Verilerin kaynağının ve profilleme teknolojilerine başvurulduğunun bilinmesi, verilerin şeffaflığı ve kontrol edilebilir olması açısından oldukça önemlidir. Aksi halde münhasıran otomatik karar verme sistemlerine itiraz etmek isteyen kişinin anlamlı bir itiraz hakkı söz konusu olamayacaktır. Bu nedenle, özel bir düzenleme olmasa dahi aydınlatma yükümlülüğü çerçevesinde, veri sorumluları işledikleri kişisel verinin kaynağını ve profillemenin yapılış usulünü açıklamalıdır. Kuşkusuz ki profilleme teknolojilerinin işleme mantığına dair yapılan açıklamanın anlamlı olabilmesi için kullanılan yazılımlar açıklanabilir bir modele dayanmalıdır. Bu nedenle GDPR ve Direktif kapsamında "kara kutu" şeklinde işleyen algoritmalara ilişkin açıklanan çekinceler, Türk mevzuatı açısından da geçerlidir. Özellikle Ceza Muhakemesi alanında adil yargılanmanın tesisi için, toplanan verilerden ulaşılan profillere nasıl varıldığının şüpheli veya sanık ile paylaşılması zorunludur. Derin öğrenme ve yapay sinir ağları ile öğrenmeye dayanan profilleme sonuçları yargılama sırasında kullanıldığı takdirde, profillemenin işleme mantığını açıklamak ve şeffaflık ilkesini tesis etmek mümkün olmayacaktır.

Profilleme süreci ana hatlarıyla özel şirketler tarafından toplanan verilere dayanılarak yapılmaktadır. Bu süreçte, özel şirketlere KVKK bünyesinde öngörülen profilleme ve şeffaflık haklarına ilişkin maddelerin uygulanacağı konusunda bir şüphe bulunmamaktadır. Ancak gerek veri toplama, gerekse profilleme sürecinin suçun önlenmesi ve ceza yargılaması sırasında yapılması durumunda KVKK kapsamında istisna hallerini düzenleyen 28. madde dikkate alınmalıdır. Aşağıda bu maddede öngörülen istisnalar detaylı şekilde ele alınacaktır.

2. KVKK Kapsamı Dışında Bırakılan veya Sınırlandırma Rejimi Öngörülen Haller

a) KVKK Kapsamı Dışında Bırakılan Haller

KVKK bünyesindeki 28. maddenin ilk fıkrası KVKK hükümlerinin uygulama alanı dışında bırakılan halleri düzenlemiştir. Bu fıkrada sayılan (ç) bendinde, kişisel verilerin milli savunma, milli güvenlik, kamu güvenliği ve ekonomik güvenliği sağlamaya yönelik ve kanun gereği görev ve yetkili kişi, kurum ve kuruluşlar

tarafından önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde KVKK hükümlerinin uygulanmayacağı belirtilmektedir.

Bu istisnanın kapsamına giren kamu güvenliği ve milli güvenlik kavramları geniş yorumlanmaya açıktır. Kamu güvenliğinin tesisi, kişilere veya mallara zarar verecek tehdit ve tehlikelerin engellenmesi şeklinde ele alınmalıdır[315]. Bununla birlikte, bu kavramın hatalı şekilde değerlendirildiği, örneğin şiddete başvurmanın söz konusu olmadığı çoğu toplantı ve gösteri yürüyüşünde dahi en sık başvurulan sınırlandırma gerekçesi olduğu görülmektedir. Hatta bu kavram daha da genişletilerek her türlü eylem ve hareketlilik "bir iç güvenlik tehditi" olarak algılanmaktadır[316]. Bu nedenle kamu güvenliği ile iç içe geçen ancak oldukça farklı anlama sahip iç güvenlik kavramı da değerlendirilmelidir. İç güvenlik, bir ülkenin iç ve dış güvenliği kapsayan milli güvenliğine ilişkin bir kavram olup, devletin bir bütün olarak varlığını, siyasi, sosyal ve ekonomik düzenini ortadan kaldırmaya yönelik ve buna elverişli olan tehditlere karşı mücadeleyi içerir. Dolayısıyla gündelik hayatta kamu düzeni ile ilişkili faaliyetlerin ulusal güvenliği ve devlet bütünlüğünü etkilemeye elverişli olduğunu söylemek mümkün değildir. Elbette iç ve dış güvenliğe yönelik tehditlerin söz konusu olması kamu düzenini de etkiyecektir, ancak gündelik hayatta kamu düzeni ve kamu güvenliğini etkileyen her olayın, devletin birliği ve bütünlüğünü ihlal etmeye elverişli olduğunu söylemek kavramın içeriğini boşaltarak çok daha yoğun ve orantısız müdahalelere yol açmaktadır[317]. Dolayısıyla kamu güvenliği, kişilerin can ve mal güvenliğinin tehlikeye düşeceği ihtimalleri, milli güvenlik ise ülkenin varlığını ve bütünlüğünü tehdit etmeye elverişli faaliyetleri kapsayacak şekilde algılanmalı, bu kavramlar geniş yorumlanmamalıdır. Bu kavramların sınırlarının doğru çizilmesi, kişisel verilerin korunma rejimi açısından 23. maddede öngörülen bu istisnaya sıklıkla başvurulmasını engellemek adına önem taşımaktadır.

İlgili bentte ikincil olarak önleyici, koruyucu ve istihbari faaliyetlerin gerçekleştirilmesi halinde KVKK hükümlerinin uygulanmayacağı belirtilmiştir.

---

[315] Gözler, Kemal, **İdare Hukuku**, Cilt:2, Ekin Kitabevi: Bursa, 2003, s.419.

[316] Örneğin Fransa'da sarı yelekliler hareketi milli güvenlik kapsamında değerlendirilmiş, OHAL hükümlerine başvurulması dahi gündeme gelmiştir, Richard, Werly, "Macron face aux risques d'un 'état d'urgence' anti-gilets jaunes", https://www.letemps.ch/monde/macron-face-aux-risques-dun-durgence-antigilets-jaunes, 08.01.2019, Erişim Tarihi: 06.05.2021.

[317] Atakan, Arda, "Kamu Düzeni Kavramı", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:13, Sayı:1-2, 2007, ss. 59-166, s.101,102.

Burada sayılan faaliyetler, suç işlenmesinden önceki alana ilişkin faaliyetlerdir. Suç öncesi alan, henüz suç teşkil eden hareketin gerçekleşmediği, suç işlendiğine dair şüphenin ortaya çıkmadığı bir alandır. Dolayısıyla kamu düzeni ve güvenliğine yönelik bir zarar gerçekleşmeden önce müdahalenin amaçlandığı bu alanda, tehlikelerin zarara dönüşmeden ortadan kaldırılması amaçlanır. Bununla birlikte, suç öncesi alanda yetkili merciler tarafından gerçekleştirilen her faaliyet önleyici faaliyet değildir[318]. Suç öncesi alanda, yalnız idari kolluk faaliyetleri değil, devletlerin ulusal güvenliğine, anayasal düzenine ve bağımsızlığına yönelik tehditleri ortadan kaldırmak için bilgi edinme amaçlı istihbarata başvurması, dolayısıyla istihbarat faaliyetlerinin gerçekleştirilmesi de söz konusu olmaktadır[319]. Kural olarak istihbarat teşkilatının görevi, demokratik hukuk devletinin varlığı, devamlılığı ve güvenliğini tesis etmek, bu amaçla demokratik sisteme yönelik tehlikeler için "erken alarm sistemi" oluşturmaktır. Bu amaca ulaşabilmek için veri toplayan ve risk analizi yapan istihbarat örgütü, bir nevi soyut tehlike kavramına dayanarak faaliyet yürütmekte[320] ve tespit ettiği riskleri yürütmeye bildirmektedir. Kolluk faaliyetleri ise tespitten ziyade, icrai faaliyetler içerir. Bu faaliyetler, kamu düzenini ihlal etmeye elverişli somut tehlikelerin fiili olarak önlenmesine yöneliktir. Bu nedenle kolluk istihbarattan farklı olarak durdurma, yakalama gibi icrai yetkilerle donatılmıştır[321]. Bununla birlikte günümüzde istihbarat ve kolluk arası sınırlar bulanıklaşmakta, bu durum kanunların lafzına da yansımaktadır[322]. KVKK ise önleyici veya istihbari nitelik taşıyan faaliyetleri tanımlamaksızın, bu tür faaliyetlerin tamamını uygulama alanı dışında bırakmıştır.

KVKK m.28 f.1 uyarınca tamamen kanun kapsamı dışında bırakılan diğer bir istisna hali, (d) bendinde öngörülen kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri

---

[318] Kızılırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", s.234.
[319] Ibid, s. 236.
[320] Michael Lysander Fremuth, "Wächst zusammen, was zusammengehört? Das Trennungsgebot Zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsarchitektur", **Archiv des öffentlichen Rechts**, Cilt: 139, Sayı:1, 2014, s.37.
[321] European Union Agency for Fundemantal Rights, **Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU**, Imprimerie Centrale: Lüksemburg, 2017, s.28.
[322] Örneğin PVSK ek madde 7, polise, ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunma, bu amaçla bilgi toplama, değerlendirme ve devletin diğer istihbarat kuruluşlarıyla işbirliği yapma yetkisi tanımaktadır.

tarafından işlenmesi halidir. İlgili bentte, soruşturma, yargılama ve infaz sürecinde, yalnızca yargı makamları ve infaz kurumlarınca gerçekleştirilen veri işleme süreci KVKK dışında tutulmuştur. Bu durumda adli amaçla kolluk tarafından işlenen veriler, m.28/1 (d) ile öngörülen bu istisna kapsamında değerlendirilmeyecek, KVKK rejimi adli kolluk açısından uygulanmaya devam edecektir. Nitekim adli kolluk bir yargı veya infaz makamı değildir. Anayasa'nın 9. maddesinde belirtilen "Yargı yetkisi, Türk Milleti adına bağımsız ve tarafsız mahkemelerce kullanılır" ifadesi ışığında cumhuriyet savcısı da bir yargı makamı olarak nitelendirilemeyecektir[323]. Anayasa ve CMK hükümleri uyarınca, savcıların suç teşkil ettiği iddia edilen fiili yargılamak ve çözüme kavuşturmak yetkisi bulunmamaktadır. Savcı kural olarak doğan uyuşmazlıkları çözmesi için yargı makamı önüne götürmekte, ön ödeme ve uzlaşma gibi alternatif çözüm yollarında ise kanunda kendisine tanınan yetki uyarınca davaya konu fiili ve faile ilişkin bir yargılama yapmaksızın muhakemeyi sona erdirmektedir[324]. Bu nedenle savcılık nezdinde işlenen kişisel veriler de KVKK m.28/1 (d) kapsamındaki mutlak istisna hükmü kapsamında değerlendirilemeyecektir.

b) Sınırlandırma Rejimi Öngörülen Haller

Savcılık ve kolluk mercileri açısından önem taşıyan hüküm KVKK m. 28/2 hükmüdür. Bu hükme göre suç işlenmesini önleme veya suç soruşturması için kişisel veri işlendiği takdirde, KVKK tamamen devre dışı kalmayacak, ancak aydınlatma yükümlülüğünü düzenleyen m. 10, ilgili kişilerin haklarını düzenleyen m. 11[325] ile Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen m. 16 veri işleyen merciler açısından bağlayıcı olmayacaktır. KVKK m. 28/2 ile kapsam dışı bırakılan bu haklardan 11. madde, münhasıran otomatik karar alınmaya karşı itiraz hakkını da içermektedir. Bu durumda suçu önleme ve soruşturma amacıyla, salt profilleme teknolojileri ile kişi aleyhine karar alındığında, kişiye itiraz hakkı tanınmayabilecektir. Yine profillemeye ilişkin şeffaflık hakları açısından önem taşıyan aydınlatma yükümlülüğüne ilişkin m. 10, m.28/2'de sayılan koşullar doğduğunda uygulama alanı

[323] Kızılırmak, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", s.255

[324]Hakan Karakehya/Murat Arabacı, "Cumhuriyet Savcısının Hukuki Statüsü, Muhakemedeki Taraf Pozisyonu ve İspat Yükünün Bulunması Üzerine", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:65, Sayı: 4, 2016, ss. 2059-2081,s.2066.

[325] 11. maddedeki zararın giderilmesini talep etme hakkı ise istisna kapsamının dışında bırakılmıştır. Başka bir deyişle, ilgili kişi her halde uğradığı zararı talep etme hakkına sahiptir.

bulamayacaktır. Bununla birlikte ilgili maddelerin uygulanmaması, ancak KVKK'nin amacına ve temel ilkelerine uygun ve orantılı olduğu takdirde mümkündür. KVKK m.28/2'nin söz konusu olduğu hallerde KVKK'nin diğer hükümleri her hâlükârda uygulanmalıdır. Bu bağlamda, dürüstlük, güncellik, belirli ve sınırlı amaçlarla veri işleme, sınırlılık ve ölçülülük temel ilkeleri düzenleyen m. 4, veri işlemenin hukuka uygun olma zeminlerini düzenleyen m. 5 ve özel nitelikli veri işlemeye yönelik m.6, verilerin silinmesi, yok edilmesi, anonim hale getirilmesini gerektiren m. 7 gibi diğer tüm hükümler her hâlükârda dikkate alınmalıdır. Bu maddeler, istisnaların sınırını çizmektedir.

Altı çizilmesi gereken diğer husus, hem m.28/2 (a) hem de 28/1 (d) bendinde kişisel verilerin soruşturma amaçlı işlenmesi ifadesine yer verilmesidir. İki fıkra arasındaki fark, soruşturma amaçlı verileri işleyen makamlardır. Kişisel verilerin yargı makamları veya infaz mercileri tarafından soruşturma amaçlı işlenmesi halinde m. 28/1 (d) devreye girecek ve KVKK hükümleri tamamen devre dışı kalacaktır. Bu merciler dışındaki mercilerin soruşturma amaçlı veri işlemesi halinde ise m.28/2 uygulanacak ve yalnızca bu fıkra kapsamında sayılan bazı hakların uygulanmaması söz konusu olacaktır. Bu nedenle, örneğin savcı ve kolluk kuvvetlerinin soruşturma için gerekli kişisel verileri işlediği haller m. 28/2'in kapsamındadır.

c) Değerlendirme

KVKK hükümlerin kısmen veya tamamen uygulanmayacağı haller oldukça karmaşık bir yapıda düzenlenmiş, tamamen istisna hallerinde kişisel verilerin korumasına ilişkin ek güvenceler öngörülmemiştir. Özellikle kişisel verilerin yargı makamları veya infaz mercileri tarafından işlenmesi sürecinin KVKK hükümlerinin tamamen kapsam dışı kalması yerinde olmamıştır. Nitekim kişisel verilerin korunması mevzuatlarının en temel hedeflerinden biri, devletlerin veri işleme etkinliklerinin ivme kazanmasıyla bireyler aleyhine bozulan dengeyi yeniden kurmaktır[326]. Bu nedenle veri işlemeye ilişkin temel ilkelerin hukuk devletinin istisnasız tüm işlem ve eylemlerine uygulanması gerekir. Suçu önleme, tespit ve infaz gibi amaçlar nedeniyle özel koşullar gerektiren veri işleme sürecinin ise bu koşullar dikkate alınarak ve bireyler için uygun

[326] Küzeci, s.383.

güvenceler öngörülerek detaylı şekilde düzenlenmesi gerekir. Nitekim GDPR bünyesinde istisna halleri bulunmakla birlikte, bu boşluk 2016/680 sayılı Direktif ile doldurulmuştur. Ancak Türk mevzuatında, istisna hallerini düzenleyen, yargı ve infaz mercileri ile kolluk ve savcılığın kişisel veri işlemesini sınırlandıran ayrı bir kişisel verileri koruma mevzuatı bulunmamaktadır. Bununla birlikte bir yargılama mercii olmayan kolluk görevlileri veya savcıların adli amaçla veri işleme süreçlerinin tamamen KVKK kapsamı dışında bırakılmadığı tekrar vurgulanmalıdır. Her ne kadar bu mercilere kişisel verilere ilişkin belirli hakları kısıtlama veya kullandırmama imkânı tanınsa da söz konusu mercilerin KVKK'nin diğer hükümleri çerçevesindeki yükümlülükleri devam etmektedir. Ancak, KVKK kapsamında, örneğin 2016/680 sayılı Direktif kapsamında olduğu gibi soruşturma sırasında işlenen kişisel verilerin kısıtlandığı veya tamamen engellendiği durumlarda, bu mercilerin kararlarına ilişkin Kişisel Veriler Kurulu'na başvuru yolu öngörülmemiş veya söz konusu hakların kısıtlanmasına ilişkin kararların otomatik olarak Kurul tarafından değerlendirebilmesini mümkün kılan düzenlemeler yapılmamıştır. Bu bağlamda, 2016/680 sayılı Direktif hem kişisel verilerin yargı makamları ve infaz mercilerince işlendiği halleri kapsaması, hem de kolluk, savcı tarafından ilgilinin haklarının kısıtlandığı hallerde güvenceler barındırması açısından örnek teşkil etmektedir. Benzer şekilde, KVKK ile açık bırakılan bu alanları düzenleyen normlara acil ihtiyaç duyulmaktadır. Bu ihtiyaç KVKK kapsamında istisna hükmü olan 28. maddenin yeniden düzenlemesi ile karşılanabileceği gibi daha da yerinde olan, AB Kişisel Verileri Koruma mevzuatına paralel şekilde suçla mücadele ve suç işlendikten sonraki soruşturma, kovuşturma ve infaz aşamalarının özel niteliklerini göz önünde bulunduran ayrı bir kişisel verileri koruma düzenlemesi yapılmasıdır.

İKİNCİ BÖLÜM

CEZA MUHAKEMESİ MEVZUATI KAPSAMINDA PROFİLLEME TEKNOLOJİLERİ

Bir önceki bölümde profilleme teknolojileri kişisel verileri koruma mevzuatı çerçevesinde ele alınmıştır. Bununla birlikte, profilleme teknolojilerinin ceza muhakemesi alanında kullanımı, bu teknolojilerin ceza muhakemesinin ilke ve kuralları açısından değerlendirilmesini de gerektirir.

Bu bölümde ilk olarak profilleme teknolojilerinin, ceza adaletinde kullanılmasına ilişkin karşılaştırmalı hukuktaki düzenlemeler ele alınacaktır. Ardından profilleme uygulamalarının ceza muhakemesindeki yeri tespit edilmeye çalışılacaktır. Bu bağlamda, profilleme teknolojilerinin koruma tedbirleri kapsamında değerlendirilip değerlendirilemeyeceği, ceza muhakemesinde benzerlik gösterdikleri koruma tedbirleri de dikkate alınarak tartışılacaktır. Ardından, profilleme teknolojileri geleneksel koruma tedbirlerinin ortak özellikleri olan kanunilik, geçici olma, belirli bir şüphe derecesi gerektirme ve ölçülü olma unsurları kapsamında incelenecektir.

Profilleme teknolojileri amaçları ve sonuçları bakımından pozitivist ekolün ceza hukukuna mirası olan güvenlik tedbirleri ile de benzerlik göstermektedir. Bu nedenle koruma tedbirleri ile yapılan karşılaştırmanın ardından, bir sonraki başlıkta profilleme teknolojilerinin güvenlik tedbirleri ile benzerlikleri ve farkları ele alınacaktır.

Son olarak mevcut koşullar altında bu tür teknolojilerin ceza muhakemesinde kullanımının hukuka uygunluğu ve delil değeri tespit edilecektir. Bu başlık altında delillerin ve delil araçlarının taşıması gereken nitelikler açıklanacak, ardından profilleme ile varılan sonuçların bu nitelikleri barındırıp barındırmadığı üzerinde durulacaktır.

I. BAZI HUKUK SİSTEMLERİNDE YER ALAN ÖZEL DÜZENLEMELER

GDPR bir tüzük olduğu ve tüzüklerin, AB kurumlarını, tüm üye devletleri ve bu devletlerin vatandaşlarını doğrudan bağlayıcı nitelikleri göz önüne alındığında, AB devletlerinde GDPR bünyesindeki profilleme düzenlemeleri yeknesak bir şekilde uygulama alanı bulmuştur. Bunun yanı sıra üye devletler Kolluk Direktifindeki profilleme düzenlemelerini, Direktif'teki amaç ve ilkeler doğrultusunda öngördükleri kanunlarla iç hukuklarında yürürlüğe koymuşlardır. Ancak bu düzenlemeler, profilleme teknolojilerini salt kişisel verilerin korunması hakkı çerçevesinde değerlendirmiştir. Bu düzenlemeler ile ilgili kişilere profilleme ile toplanan veriler ve sonuçları hakkında bilgi edinme, insan müdahalesi talep etme ve otomatik kararlara itiraz etme hakları gibi sınırlı haklar tanınmıştır. Bununla birlikte profilleme teknolojilerinin ceza muhakemesindeki yerini teknik şekilde ele alınmamış, ceza muhakemesinde bu tür teknolojilerin ne şekilde kullanılacağı, ne şekilde sınırlandırılacağı ve vardıkları sonucun delil olarak kabul edilip edilemeyeceği düzenlememiştir.

Avrupa'da çeşitli devletlerin idare, vergi ve ceza kanunlarında bizzat profilleme düzenlemeleri yer almasa da profillemeye benzer bir uygulama olan veri madenciliğine ilişkin çeşitli düzenlemelere rastlanılmaktadır.

A. Almanya

Almanya'da 11 Eylül sonrasında olası terör saldırılarına karşı otomatik veri taraması tedbirine ("Rasterfahndung") başvurulması yeniden gündeme gelmiştir. Otomatik veri taraması, elektronik ortamda işlenmiş veri tabanlarındaki bilgilerin taranması ve birbiriyle karşılaştırılmasından ibarettir. Özel ve kamusal kurumlar bünyesindeki bilgiler mukayese edilerek suçun arkasındaki kişi ve örgütsel yapılar keşfedilmeye çalışılır. Bu tedbirin daha basit haline ilkin 70'li yıllarda Rote Armee

Fraktion (RAF) örgütüne karşı başvurulmuştur[327]. RAF örneğinde, ilkin kolluk görevlileri örgütün hücre evlerine ait elektrik faturalarının elden ve sahte isimlerle ödendiğini tespit etmiştir. Ardından Hamburg'daki elektrik kurumu abone kayıtları, nüfus müdürlüğü ve sigorta müdürlüğü gibi başka kurumlardaki kayıtlarla otomatik veri taraması yoluyla karşılaştırılmıştır. Bunun üzerine gerçek olduğu tespit edilen isimler elenmiş, sahte isim kullananlar arasında ise elden fatura verenler tespit edilerek şüpheli kişilere ulaşılmıştır[328]. Almanya'da bu tür uygulamaların hukuki zeminine Alman Ceza Muhakemesi Kanunu'nun (StPO) 98 a ve b maddelerinde yer verilmiştir. Bu düzenlemeler gereği, veri taraması ancak ilgili maddede sayılan katalog suçlar işlendiği ve şüpheliyi tespit için başka tedbirlere başvurmanın mümkün olmadığı hallerde uygulanabilir. Tedbire başvurmak için mahkeme kararı gerekir, gecikmesinde sakınca bulunan hallerde ise savcı tarafından üç gün içinde mahkeme tarafından onaylanmak koşuluyla talimat verilebilir. Bu tedbir risk analizi yapan profilleme yöntemlerinden farklılık göstermektedir. Otomatik veri taraması, yalnızca büyük veri içerisinde ilişkili olabilecek verilerin anahtar kelimelerle veya belirli talimatlarla aranmasından ibarettir. Profilleme yapabilmek için de öncelikle bu şekilde veri madenciliğinin yapılması zorunludur. Ancak profillemede bir adım ileriye gidilerek yazılımlar aracılılığıyla belirli veri grupları ilişkilendirilir, kişilere ilişkin genellemeler yapılarak "tehlikeli kişiler", "tehlikeli mahalleler", "terörist örgütlerle bağı olan kişiler" şeklinde genel profiller çıkartılır. Almanya özelinde uygulanan veri madenciliği tedbirinde ise sınırsız sayıda verinin birleştirilerek grupların ve kişilerin istatistiki şekilde kategorize edilmesi ve gelecek hareketlerinin bu genellemelerden yola çıkarak tahmin edilmesi söz konusu değildir. Otomatik veri taramasında, daha ziyade fiili işlediğinden şüphelenilen kişinin profili, soruşturmanın en başında yetkili kişiler tarafından oluşturulmakta ve bu profile uygun verileri sistemde taramak üzere soruşturma talebi oluşturulmaktadır. Bu soruşturma talebine dayanılarak elektronik veri tabanlarında, arama kriterlerine uygun kayıtlar ve fotoğraf gibi dijital veriler taranır. Bu verilerden talep çerçevesinde kalanlar ayrı bir dosyaya ayrılarak kaydedilir. Diğer veriler ayrıca soruşturma kapsamında kaydedilmez. Ayrıştırılan veriler savcılık

[327] Rainer W. Gerling/Cordula Langer/Ray Roßmann, "Rechtsgrundlagen zur Rasterfahndung: Einführung und Auszüge aus den einschlägigen Gesetzen", **Datenschutz und Daten Sicherheit**, Cilt: 25, Sayı:12, 2001, ss.746-749, s.746.

[328] Çiler Damla Bayraktar, "Ceza Muhakemesi Hukukunda Bir Koruma Tedbiri Olarak Otomatik Veri Taraması (Rasterfahndung): İnsan Hakları Bağlamında Bir Analiz", **Ceza Hukuku Dergisi**, Cilt: 13, Sayı:38, Aralık 2018, ss. 25-64, s.28.

makamına iletilir[329]. Dolayısıyla Alman mevzuatında, ceza muhakemesinde otomatik sistemler aracılığıyla profilleme yapılarak karar alınması düzenlenmemiş, yalnızca veri tabanlarında soruşturma konusu kişilere işaret eden verilerin aranması mümkün kılınmıştır. Bu tedbiri klasik anlamda koruma tedbirlerinden ayıran, henüz belli bir kişi üzerinde şüphe yoğunlaşmamışken, şüphelilerin tespiti için sevk edilmeleridir[330]. Bu hedefe ulaşabilmek için gerektiğinde özel kurumların veri tabanlarında, ceza muhakemesi makamlarından gelen talep üzerine veri taraması ve karşılaştırması yapılabilir ve soruşturma için gerekli veriler ayıklanarak ilgili makamlara iletilir. Bununla birlikte bu tedbir ile veri taraması sırasında kullanılacak ölçütlere tesadüfen uyan ve şüpheli olmayan pek çok kişinin hareket ve alışkanlıklarına dair bilgilerin elde edilmesi riski de doğmaktadır. Bu nedenle tedbir katalog suçların işlenmesi halinde uygulanma ve mahkeme denetimine tabi olma unsurları ile sınırlandırılmıştır[331].

B. Hollanda

Hollanda'da Hollanda Polis Veri Kanunu (de Wet Politiegegevens) [332] m. 9, 10 ve 11. ile belli verilerin ve veri dosyalarının otomatik şekilde analiz edilmesi mümkün kılınmıştır. Uygulamada Hollanda polisinin veri madenciliği yapma yetkisini kullanırken kolluğa soruşturma sırasında genel araştırma yetkisi veren Polis Veri Kanunu'nun 3. maddesine dayandığı görülmektedir. Genel bir yetki tanıyan bu düzenlemede, kişisel verilerin korunmasına ilişkin herhangi bir sınırlandırma öngörülmemiştir. Buna rağmen, Hollanda Yüksek Mahkemesi, polisin genel yetkilerini düzenleyen 3. maddeye dayanarak veri madenciliği yapmasını, "temel hak ve özgürlüklere yoğun bir müdahale içermediği müddetçe" hukuka uygun kabul etmiştir[333]. Oysa veri madenciliği tedbiri, kuşkusuz ki sınırsız sayıda ve tüm vatandaşlara ait verileri araştırmayı ve bu verileri paylaşmayı mümkün kılarak kişisel verilerin korunması hakkına yoğun bir müdahale içermektedir. Bu yetkiyi suç tipleri, saklama süresi, mahkeme kararı gibi unsurlarla sınırlamaksızın genel bir hüküm

[329] Bayraktar, s. 42, 43.
[330] Bayraktar, s.49.
[331] Bayraktar, s. 43.
[332] De Wet Politiegegevens, 21.07.2007, https://wetten.overheid.nl/BWBR0022463/2020-01-01, Erişim Tarihi: 10.09.2021.
[333] Hoge Raad, 19 Aralık 1995, NJ 1996, 249 ve Hoge Raad 1Temmuz 2014, NJ 2015, 114, 115, aktaran Sven Brinkhoff, "Big Data Data Mining by the Dutch Police: Criteria for a Future Method of Investigation", **European Journal for Security Research**, Cilt:2, 2017, ss. 57–69, s. 61.

kapsamında değerlendirmek, AİHM standartları ile çelişmektedir. Örneğin Hollanda'da sıklıkla başvurulan iColumbo sistemi, belli anahtar sözcük ve profillere dayanarak internetteki tüm veriler arasında arama yapmak ve bu verileri analiz etmek üzere kullanılmaktadır. Ancak Hollanda'da bu tedbir ile hangi tür verilerin işleneceğini sınırlayan, şüphe derecesi belirleyen veya hâkim kararı gerektiren bir norm bulunmamaktadır. Oysa iColumbo aracılığıyla şüpheli statüsünde olmayan kişilerin ırk, din, cinsiyet gibi hassas verilerine dahi ulaşmak mümkündür. Öte yandan, Hollanda'da yine sıklıkla başvurulan otomatik araba plakası tanıma sistemini (ANPR system) düzenlemek için kanun tasarısı sunulmuştur. Bu sistemde, otobandan geçen tüm taşıtların plakaları kaydedilmekte, ardından sistemdeki verilerin kolluk elindeki verilerle kıyaslanarak araba hırsızlığı ve uyuşturucu ticareti gibi suçlarda kullanılan araçların tespiti amaçlanmaktadır. İki sistemdeki verilerin uyuşması, soruşturma başlatılması veya koruma tedbirlerinin uygulanmasına zemin hazırlamaktadır. Hatta kimi davalarda eşleşme sonuçları ceza muhakemesinde delil olarak değerlendirilmektedir. Bu nedenle veri eşleştirme sistemi açısından Hollanda Ceza Muhakemesi Kanunu'na 126 jj maddesi eklenmesi ve ANPR sisteminin ceza muhakemesinde hangi şartlar altında kullanılabileceğinin düzenlenmesi yönünde kanun teklifinde bulunulmuştur[334]. Ancak bu uygulama da yalnızca tarama ve eşleştirmeden ibaret olup, henüz risk analizi yapan ve geleceğe yönelik kişilerin riskini hesaplayan profilleme teknolojilerine ilişkin bir düzenleme yapılmadığı görülmektedir.

C. Avusturya

Avusturya'da da profilleme teknolojilerine ilişkin düzenleme bulunmamakta, ancak Almanya'ya benzer şekilde otomatik olarak veri arama ve karşılaştırması yapan sistemlere yönelik düzenleme yapıldığı görülmektedir. Avusturya Ceza Muhakemesi Kanunu'nun[335] 141. maddesinde suç örgütü veya terör örgütü faaliyeti çerçevesinde 10 yıldan daha fazla hapis ceza gerektiren bir suç işlendiğine dair şüphe oluştuğu takdirde, kişisel veri ve hükümet verileri üzerinden tarama ve veri madenciliği işlemleri mümkün kılınmıştır. Ancak bu suçlar için yapılan soruşturma ve kovuşturmalarda ilgili maddenin dördüncü fıkrası gereği kişilerin ırkı, etnik kökeni,

[334] Brinkhoff, s. 61, 62.
[335] Strafprozeßordnung 1975 (StPO) StF: BGBl. Nr. 631/1975 (WV).

politik ve dini görüşleri, sağlıkları ve cinsel hayatlarına ilişkin özel veriler üzerinden veri arama ve eşleştirme yapılamayacaktır. 142. maddede veri madenciliği işleminin mahkeme kararına dayanan savcılık talimatı üzerine gerçekleştirilebileceğini belirtmektedir. 143. madde ise bu süreci daha da sınırlandırarak, verileri talep ederken, yapılacak işlemin nedeninin, uygulanacağı kişilerin ve tedbir ile elde edilmek istenen verilerin belirtilmesini zorunlu kılmaktadır. Diğer bir hüküm ise kamu düzeni ve güvenliğini tesis etmeyi amaçlayan kolluk faaliyetlerini düzenleyen Sicherheitspolizeigesetz[336] ("SPG") 53a maddesinin ikinci fıkrasıdır. İlgili fıkra ile suç işlemek üzere kurulan bağlantıları tespit etmek veya kamu düzenini tehlikeye sokan saldırı ve hareketleri engellemek amacıyla operasyonel ve stratejik analiz tekniklerinin kullanımı mümkün kılınmıştır. Başka deyişle önleyici amaçlarla veri analizi yapılması hâkim kontrolü olmaksızın gerçekleştirilebilir. Ancak Avusturya kolluk sisteminde önleyici ve adli faaliyetler duvar ilkesi gereği net bir şekilde ayrılmış ve SPG m. 13/2 uyarınca, önleyici amaçla yapılacak veri tarama ve madenciliği işlemlerinde farklı amaçlarla toplanmış verilere başvurulması yasaklanmıştır. Dolayısıyla kolluğun adli ve önleyici amaçlarla topladığı veriler birleştirilemeyecek, farklı amaçla toplanmış verilerin saklandığı dosyalara erişim hukuka aykırı kabul edilecektir. Veri tarama ve analizi yetkisi, tüm adli, idari, ticari veri tabanlarına erişimi mümkün kılmamaktadır[337].

D. Belçika

Belçika'da veri tarama yetkisinin yanı sıra profilleme teşkil eden uygulamalara sınırlı şekilde izin verildiği görülmektedir. "3 Ağustos 2012 Kanunu" şeklinde bilinen Kanun'un[338] 5/1 hükmü uyarınca Maliye Bakanlığı'na görev tanımı çerçevesinde topladığı verileri depolama ve bunlar üzerinden belli risk faktörleri belirleyerek denetim yapma, verileri ilişkilendirme ve analiz yapma yetkisi verilmiştir. Ancak bu

[336] İlgili Kanun'un uzun adı Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei, StF: BGBl. Nr. 566/1991 idF BGBl. Nr. 662/1992 (DFB), https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792, Erişim Tarihi: 12.09.2021.

[337] Salimi Farsam, **National Report for Austria**, 19th International AIDP-Congress on Information Society and Penal Law, Eylül 2013, https://www.combattingcybercrime.org/files/virtual-library/national-laws/preparatory-colloquium-section-iii-national-report-for-austria.pdf, Erişim Tarihi: 12.09.2021, s. 6, 7.

[338] Loi Portant Dispositions Relatives aux Traitements de Données à Caractère Personnel Réalisés par le Service Public Fédéral Finances dans le Cadre de ses Missions, T. 24.08.2012, https://www.etaamb.be/fr/loi-du-03-aout-2012_n2012003257.html, Erişim Tarihi: 12.09.2021.

yetki, görüldüğü üzere yalnızca Bakanlık kapsamında ve finansal hareketleri analiz etmek için tanınmış olup ceza muhakemesi alanında veri madenciliği veya profilleme açısından özel bir norm sevk edilmediği görülmektedir.

E. Fransa

Avrupa ülkeleri arasında yargı sürecinde profilleme teknolojilerine ilişkin yasak öngören nadir bir düzenlemeye Fransa'da rastlanılmaktadır. Bilişim ve Özgürlükler Kanunu[339] m.47/1'de bir kişinin "davranışının değerlendirilmesini" içeren hiçbir mahkeme kararının, o kişinin karakterinin belirli yönlerini analiz etmek amacıyla gerçekleştirilen otomatik şekilde kişisel veri işlenmesine dayanamayacağını belirtmektedir. Bu fıkrada, yargı kararlarında kişilerin davranışları irdelenirken, kişiliklerini analiz eden profilleme teknolojilerine başvurulamayacağı belirtilmiştir. Bu bağlamda, ceza muhakemesinde bir kişinin suç teşkil eden davranışı, onun iç dünyasına ilişkin profilleme yapan teknolojilerden yararlanarak tespit edilemeyecektir. Bu açık hükme rağmen doktrinde, m. 47/1 hükmünün yargı kararlarında profilleme teknolojilerinden yararlanmayı tamamen yasaklamadığı, karar alırken salt profillemeye dayanılmadığı, başka delillerle hükmün desteklendiği hallerde profillemeye başvurulabileceğini savunan görüşler bulunmaktadır[340]. Oysa maddenin lafzı "yalnızca kişisel verilerin otomatik olarak işlenmesine dayanılamayacağı" şeklinde ifade edilmemiştir. Aksine fiilleri tespit eden kararların, otomatik şekilde kişilik analizi yapan teknolojilere hiçbir şekilde dayanamayacağı belirtilmiştir. Bu madde, profilleme teknolojilerinin kullanılmasını yasaklamamakla birlikte, bunların yargılamada delil olarak değerlendirilmesini yasaklamaktadır. Aynı maddenin ikinci fıkrası ise bir kişiyle ilgili olarak yasal sonuçlar doğuran veya o kişiyi önemli ölçüde etkileyen kararların, "yalnızca" profil çıkarma dahil olmak üzere kişisel verilerin otomatik olarak işlenmesine dayanamayacağını düzenlemektedir. İkinci fıkra GDPR m. 22'nin yansıması olup GDPR m. 22'de olduğu gibi hukuki statü değişikliği yaratan veya benzer nitelikte önemli sonuçlar doğuran kararları ele alınmış, bunlar

[339] Kanun'un orijinal adı Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés olup kısaca Loi Informatique et Libertés şeklinde bilinmektedir. Kanun için bkz. https://www.cnil.fr/fr/la-loi-informatique-et-libertes#:~:text=L'informatique%20doit%20%C3%AAtre%20au,aux%20libert%C3%A9s%20individuelles%20ou%20publiques , Erişim Tarihi: 25.10.2021.

[340] Florence G'sell, "Les Progrès à petits pas de la 'Justice Prédictive' en France", **Europäische Rechtsakademie**, Cilt: 21, 2020, ss.299–310, s.303.

açısından "salt" otomatik sistemlere başvurulamayacağı belirtilmiştir. İlk fıkra yargı kararları açısından net bir delil değerlendirme yasağı çizdiği, iki fıkra da yine hukuki etki doğuran kararların otomatik yollar dışında elde edilmiş veri ve delillerle desteklenmesini gerektirdiği için önem taşımaktadır. Fransa'da yaşanan diğer bir gelişme ise tüm yargı kararların ücretsiz bir şekilde herkesin erişimine açılmasıdır. Yargı Örgütlenmesi Kanunu'nun[341] L111-13. maddesi gereği adli mahkemelerce verilen kararlar kamuoyuna elektronik ortamda açıklanacaktır. Bu durum dijital ortama aktarılan kararların, analiz edilmesini ve gelecekte alınacak kararları öngörmek üzere profilleme teknolojilerine başvurulmasını mümkün kılmaktadır[342]. Bu hususta Fransa, yine diğer ülkelerden farklı olarak L111-13. maddesi ile hâkimlerin kimlik bilgilerinin, gerçek veya varsayılan mesleki uygulamalarını değerlendirmek, analiz etmek, karşılaştırmak veya tahmin etmek amacıyla yeniden kullanılamayacağını düzenlemiştir. Bu hüküm, belli bir hâkimin kararlarını profilleyerek benzer bir olaya ne şekilde karar vereceğini tahmin eden modellemelere başvurmayı hukuka aykırı kılmaktadır. Dolayısıyla Fransa'da profilleme teknolojilerinin ceza muhakemesinde sanık veya hâkim davranışlarını tahmin etmek üzere kullanılması mümkün değildir.

F. Değerlendirme

Avrupa özelinde ele alınan hukuk sistemlerinde profilleme teknolojilerinin ceza muhakemesi alanında kullanılmasına ilişkin özel bir düzenlemeye Fransa örneği haricinde yer verilmediği görülmektedir. Daha ziyade farklı veri tabanları arasındaki verilerin taranması ve kimi hallerde eşleştirilerek karşılaştırılmasını sağlayan veri madenciliği tekniklerinin düzenlendiği görülmektedir. Ancak profilleme, verilerin bu şekilde taranması ve diğer verilerden ayrılarak yorumlanmaya hazır hale getirilmesinden ibaret değildir. Veri grupları üzerinde algoritmalar aracılığıyla daha detaylı bağlar kurulmasını sağlar. Yalnızca şüpheli bir kişi ya da gruba dair verileri işaretleyerek ilgili mercilere iletmenin ötesinde, bu verilerin gruplandırılması, ilişkilendirilmesi ve aralarında bağ kurularak otomatik sonuçlara varılmasını gerektirir. Örneğin karşılaştırmalı hukukta düzenlenen veri madenciliği teknikleri ile belli bölgede oturan ve belli isme sahip kişiler veri tabanı üzerinden eşleştirilerek tespit

[341] Kanunun orijinal adı Code de l'organisation judiciaire şeklindedir, bkz. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071164/LEGISCTA000006151759/?anchor=LEGIARTI000038311162#LEGIARTI000038311162, Erişim Tarihi: 20.09.2021.
[342] G'sell, s.303, 304.

edilebilmektedir. Oysa profilleme ile bir bölgede oturan ve belli niteliklere sahip kişilerin kimlik bilgilerine erişmek temel amaç değildir, bu veriler belli suçları işleme eğilimini tespit etmek üzere analiz edilir. Dolayısıyla yukarıda bahsedilen Almanya'daki RAF üyelerine karşı uygulanan yöntemlerden Hollanda'da kişilerin plaka ve kimlik bilgilerini karşılaştırmaya kadar uzanan uygulamalar daha ziyade tanımlayıcı veri madenciliği uygulamalarıdır. Bunların amacı, henüz şüpheli tespit edilmemişken veya şüpheliye ait belli ipuçları söz konusu iken, belli kriterler uyarınca veri tabanlarında arama yapmaktır. Böylelikle hedef kitlesi küçültülür veya kimi durumlarda veriler arasındaki çelişkiler ortaya çıkarılarak soruşturmalar derinleştirilir. Kuşkusuz profilleme teknolojileri açısından da ilkin verilerin taranması ve karşılaştırılması zorunludur. Ancak profillemede bir adım daha öteye gidilerek bu veriler arası bağlantılar kurularak veriler sınıflandırılır, ardından bu sınıflara uygun olduğu varsayılan yeni veriler gruplanır[343]. Bu bağlamda potansiyel tehlikeli kişi grupları oluşturularak benzer nitelikte olan kişilerin bu gruplar altında toplanması, salt veri sistemlerinin taranmasından daha yoğun bir müdahale içermektedir. Bu tür sınıflandırmalara dayalı sonuçların ceza muhakemesindeki akıbeti, karşılaştırmalı hukukta ve Türkiye'de açıkça düzenlenilmeye muhtaçtır.

Uygulamada, profilleme teknolojilerinin kullanımı, özel hukuk ve idari hukuk alanlarında olduğu kadar ceza muhakemesi alanında da yaygınlaşmaktadır. Bu teknolojilerin sevk amacı, çalışma şekli, ne tür verileri elde ettiği ve vardıkları sonuçların delil değerinin tartışılmadan ceza muhakemesine sızması, ceza muhakemesi ilkelerinin aşınmasına yol açmaktadır. Profilleme uygulamalarının ceza muhakemesindeki konumlarını irdelemek adına aşağıdaki bölümlerde bu teknolojiler öncelikle ceza muhakemesindeki geleneksel koruma tedbirleri ve bu tedbirleri sınırlandıran ilke ve kurallar çerçevesinde değerlendirilecektir. Ardından bu teknolojilerin bir nevi güvenlik tedbirine dönüşen boyutu ele alınacaktır. Son olarak bu teknolojilerle varılan sonuçların delil değerleri tartışmaya açılacaktır.

[343] Bart W. Schermer, "The Limits of Privacy in Automated Profiling and Data Mining", **Computer, Law and Security Review**, Cilt: 27, Sayı:1, 2011, ss. 45-52, s. 46.

II. TÜRK MEVZUATINDA PROFİLLEME TEKNOLOJİLERİNİN HUKUKİ NİTELİĞİ

Profillemenin ceza muhakemesinde kullanılmasına ilişkin yerel mevzuatta herhangi bir düzenlemeye yer verilmemiştir. Karşılaştırmalı hukukta ise profillemeye benzerlik gösteren ancak hak ve özgürlüklere daha az müdahale içeren veri madenciliği uygulamalarının kullanımına ilişkin düzenlemeler yapıldığı görülmektedir. Türk mevzuatında, adli amaçlı veri madenciliği ve veri eşleştirmeye ilişkin bu tür düzenlemelere de yer verilmediği görülmektedir.

Profilleme teknolojilerine ilişkin bir düzenleme boşluğu olduğu açık olmakla birlikte, öncelikle profilleme teknolojilerinin ceza muhakemesinde hangi tedbir veya yaptırım türü kapsamında ele alınması gerektiği değerlendirilmelidir. Bu amaçla, aşağıda ilk olarak profilleme teknolojileri, koruma tedbirleri çerçevesinde ele alınacak, bu tedbirlerle örtüşen ve farklılaşan yanları üzerinde durulacaktır. Ardından, bu tedbirlerin bir yaptırım türü olan güvenlik tedbiri olara ele alınıp alınamayacağı değerlendirilecektir.

A. Koruma Tedbirleri Kapsamında Profilleme Teknolojileri

Koruma tedbirleri, kişilerin hak ve özgürlüklerini sınırlamaları sebebiyle açıkça düzenlenmekte, bu düzenlemeler insan onurunu ve temel hakları korumayı gözetecek belirli güvenceler içermektedir. Demokratik toplumlarda, bir suçun ortaya çıkarılması ve failin tespit edilmesi amacıyla kişilerin haklarını sınırlamanın belirli sınırları vardır. Nitekim bireylerin öngörülemez kısıtlamalara tabi olma ihtimali olduğu bir toplumda özgür olmaları mümkün değildir. Bu nedenle, amacı maddi gerçeğin tespit edilmesi olan ceza muhakemesi hukukunda, toplumsal düzenin korunması ve temel hak ve özgürlüklerin teminat altına alınması birlikte gözetilmelidir. Devletin güç kullanma ve cezalandırma yetkisi sınırsız olduğu takdirde, bireylerin kendilerini gerçekleştirebildiği bir toplum düzeninin tesis edilmesi de mümkün değildir. Bu nedenle ceza muhakemesinde gerçeğin her ne pahasına olursa olsun değil, hukuk

düzeni içinde kalınarak ve failin onuru korunarak araştırılması gerekir[344]. Profilleme teknolojileri, kişilerin özel hayatının gizliliği ve verilerinin korunması kadar, seyahat özgürlükleri ve kişi güvenlikleri ile de yakından ilintilidir. Kişiler hakkında "potansiyel suçlu" kimliği oluşturulurken toplanan ve birleştirilen veriler, klasik koruma tedbirleri ile toplanan verilerden çok daha kapsamlı veriye ulaşımı mümkün kılmaktadır. Bu tespitler, kişilerin seyahat özgürlükleri ve kimi zaman kişi güvenliklerine ilişkin kararlar alınması ile sonuçlanmaktadır. Dolayısıyla profillleme, ceza muhakemesi sürecinde koruma tedbirleri ile benzeşmekte, kimi zaman hak ve özgürlüklere bu tedbirlerden çok daha fazla müdahale teşkil etmektedir.

Aşağıda profilleme teknolojileri, koruma tedbirleri kapsamında değerlendirilirken, öncelikle benzer nitelikteki arama ve fiziksel kimlik tespiti tedbirleri kapsamında ele alınacaktır. Ardından profilleme tedbirlerinin, koruma tedbirlerinde ortak olarak görülen nitelikleri barındırıp barındırmadığı değerlendirilecektir.

1. Profilleme Teknolojilerinin Arama Tedbiri İle Karşılaştırılması

Arama, bir kişi veya gizli ve saklı tutulan bir eşyanın, önleme veya adli amaçlarla meydana çıkarılması için yapılan ve özel hayatın gizliliğine müdahale içeren bir koruma tedbiridir[345]. Aşağıda adli arama ve önleme araması tedbirlerindeki temel unsurlar belirtilerek, bu tedbirler ile profilleme teknolojileri arasındaki benzerlikler ve farklar ele alınacaktır.

a) Adli Arama ile Profilleme Teknolojilerinin Karşılaştırılması

Adli arama, bir suçun işlendiği şüphesi üzerine başlatılan ceza soruşturması veya kovuşturması sürecinde şüpheli veya sanığın veya suç delillerinin ele geçirilmesi için kişilerin üstü, konutu veya iş yerinde gerçekleştirilir[346]. Dolayısıyla arama ile şüpheli

---

[344] Kahan Onur Arslan, "İnsan Onuru Kavramı ve Koruma Tedbirleri Bağlamında Temel Bir İlke Olarak İnsan Onurunun Korunması", **Türkiye Barolar Birliği Dergisi**, Eylül Ekim 2015, Sayı:120, ss.155-172, s. 170, 171.

[345] Kadir Can Özel, "Bir Koruma Tedbiri Olarak Arama", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Durmuş Tezcan'a Armağan, Cilt:21, Özel Sayı, 2019, s. 1217-1266, s.1219, 1230.

[346] Bahri Öztürk/Durmuş Tezcan/Mustafa Ruhan Erdem/Özge Sırma Gezer/Yasemin Saygılar Kırıt/Esra Alan Akcan/Özdem Özaydın/Efser Erden Tütüncü/Derya Altınok Villemin/Mehmet Can Tok, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, 2021, s.503.

veya sanığın yakalanması ve kişinin veya üçüncü kişilerin zilyedliğindeki suç delillerinin elde edilmesi amaçlanmaktadır[347].

Risk analizi yapan profilleme ise kişinin kamu düzenine tehlike oluşturup oluşturmadığı, yeniden bir suçu işleyip işlemeyeceğine dair tespitte bulunmak üzere başvurulan bir yöntemdir. Ancak profilleme ile muhakeme sürecinin işlemeye devam etmesine ve davaya konu maddi olayın çözümlenmesine yardımcı olmak amaçlanmamaktadır. Profilleme geleceğe yönelik, topluma risk teşkil eden grupların ve kişilerin tespit edilmesini amaçlar. Profilleme milyonlarca veri arasında bağ kurarak ve çıkarım yaparak gruplar oluşturma ve bu gruba ait olduğu iddia edilen bireyleri belirlemek üzere kullanılır. Kişiye ait banka işlemleri, internet hareketleri, kişinin sosyal çevresi ve bulunduğu yerleri içeren pek çok verinin birleştirilerek yorumlanması şeklinde "kişiye özgü" uygulanabileceği gibi[348], şüpheli sıfatını taşımayan milyonlarca vatandaşın verilerinden yola çıkarak belirli grupları belirlemek şeklinde "gruba özgü" de uygulanmaktadır[349]. Profilleme teknolojilerine başvuran kolluk görevlileri, çoğu durumda veri tabanlarında araştırma yaparak, yazılım tarafından tespit edilen örüntülere, tekrarlara uyan kişileri hedef almaktadır. Ancak bu veri tabanları, tüm vatandaşları hedef aldığından, profilleme teknolojilerinin adli aramadan farklı olarak hakkında soruşturma dahi başlatılmamış kişilere karşı uygulanması söz konusu olmaktadır.

Dolayısıyla arama tedbirinde olduğu gibi suça ilişkin delilleri bulmak veya işlenmiş bir suçun failini yakalamak profillemenin amaçları arasında yer almamaktadır. Bu teknolojiler ile pozitivist ceza hukuku teorisyenlerine paralel şekilde "suçlu karaktere sahip" kişiler henüz suç teşkil eden fiilleri bulunmasa dahi belli listelere dâhil edilerek gruplandırılır. Kimi zaman profilleme teknolojileri ile kişilerin gerçekleştirmesi muhtemel kanuna aykırı davranışları tespit edilmeye çalışılır ve bunu engellemek amacıyla belirli gruplar altında kategorize edilen kişiler toplumdan uzaklaştırılır. Kimi zaman ise profilleme teknolojileri ile bir soruşturma veya kovuşturma sırasında bu tür kişilerin kaçma riski tayin edilmeye çalışılır. Son olarak

---

[347] Özel, s.1222.

[348] Ira Rubinstein/Ronald D. Lee/Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", **University of Chicago Law Review**, Cilt:75, Sayı:1, 2008, ss. 261-285, s.263.

[349] Hildebrandt, "Defining Profiling: A New Type of Knowledge?", s. 20.

hükmün belirlenmesi aşamasında, kişilerin karakteri ve yeniden suç işleme risklerini değerlendiren profilleme teknolojilerine başvurulduğu görülmektedir. Ancak hepsinin ortak özelliği, temelde bu kişiler toplumda serbest dolaştığı takdirde doğacak riskleri hesaplamaktır. Dolayısıyla işlenmiş bir suç ile fail arası bağı gösteren delilleri elde etme amacı bulunmamaktadır. Aksine kişilerin geçmişlerinden yola çıkarak geleceklerine dair bir nevi "niyet okuma"[350] söz konusudur. Dolayısıyla profilleme teknolojileri kişi grupları hakkında "dijital bir günlük" tutmakta ve kişilerin bir suç işleyip işlemediklerini belirlemekten ziyade karakter analizlerini yapmaktadır[351].

Adli arama ile kişinin hak ve özgürlüklerine müdahale edilebilmesi için ön koşul, suç şüphesinin gerek soruşturma gerekse kovuşturma evresinde belirli bir kişi üzerinde yoğunlaşmış olmasıdır. İlgili kişinin yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe bulunmalıdır. Şüpheli kişiyi veya delili bulmayı "umma", arama tedbirine başvurmak için yetersizdir. Nitekim umma sübjektif bir kavram olup, bir hipoteze dayanırken, makul şüphe için objektif olgu ve emarelerin bulunması gerekir[352]. Arama tedbiri, istisnaen şüpheli veya sanık sıfatını taşımayan kişilere yöneltilmekte, ancak bu durumda daha da sıkı koşullara tabi tutulmaktadır[353].

Oysa milyonlarca kişiye dair veri üzerinden gerçekleştirilen profilleme teknolojileri, bir kişi üzerine yoğunlaşmış şüpheden yola çıkmamakta, yine şüpheyi destekleyecek verilerin bulunacağına dair herhangi bir belge ya da olguya dayanmamaktadır. Profilleme teknolojilerinde, kişi ve grupların profili çıkartılırken başvurulan verilerin, çoğu durumda işlenmiş suç ile bir ilişkisi bulunmamaktadır. Örneğin kişinin borcunu zamanında ödeyip ödemediği, güvenilir olup olmadığı, çevresinde suç işlemiş kişilerin bulunup bulunmadığına dair bilgilerin kişinin bir suç işlediğine dair makul şüpheye işaret ettiğini söylemek mümkün değildir[354]. Aramayı mümkün kılan makul şüphe, gözlemlenebilen icrai hareketler üzerinden

---

[350] Bu terim John Battelle tarafından İngilizce'de "database of intentions" şeklinde ifade edilmiştir, bkz. John Battelle, **How Google and its Rivals Rewrote the Rules of Businesses and Transformed Our Culture**, Nicholas Brealey Publishing: London, 2005, s.6.

[351] Joseph T. Thai, "Is Data Mining Ever Search Under Justice Stevens's Fourth Amendment", **Fordham Law Review**, Cilt:74, Sayı:4, 2006, ss.1731-1758, s.1756.

[352] Özbek, Veli Özer/ Doğan, Koray/ Bacaksız, Pınar, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, Eylül 2021, s.293.

[353] CMK m.117 gereği bu tür durumlarda, aranılan kişinin veya delillerin belirtilen yerde bulunduğunu gösteren olayların varlığı gereklidir, Yener Ünver/Hakan Hakeri, **Ceza Muhakemesi Hukuku**, Adalet Yayınevi: Ankara, Mayıs 2019, s.383, 384.

[354] Tien, s.403, 404.

değerlendirilir. Profilleme teknolojileri ise geçmişe dair dijital veriler üzerinden otomatikleşmiş bir şüphe kavramı yaratmaktadır[355]. Dolayısıyla, profilleme teknolojileri, adli aramadan farklı olarak bireyselleşmiş şüphe ve şüpheli kavramlarına dayanmamaktadır.

Bunun yanı sıra arama tedbiri, aramanın konusuna göre alt gruplara ayrılır. Üst araması, eşyada arama, konut araması konusuna göre farklı arama türlerine örnektir. Kimi zaman aramanın konusu özel düzenlemelere başvurulmasını gerektirir. Örneğin avukatlık büroları savunma hakkının dokunulmazlığı gözetilerek CMK m. 130 ve Avukatlık Kanunu m. 58 ile ayrıca düzenleme altına alınmıştır[356]. Son olarak CMK m. 134'te bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemleri düzenlenmiş bulunmaktadır.

Profilleme teknolojileri, sevk amaçları kadar konuları bakımından da geleneksel adli arama tedbirinden ayrılmaktadır. Arama tedbiri, en baştan belirlenmiş ve sınırlanmış bir kişi, eşya, konut veya bilgisayar içerisindeki belirli verilere yöneliktir. En fazla veri ve bilgiye erişime imkân sağlayan bilgisayarda arama işleminde dahi, kişinin her dosyası, görüşme kayıtları ve fotoğrafları aranmamakta, yalnızca suça ilişkin deliller elde edilmeye çalışılmaktadır. Profilleme teknolojilerinde ise işlenen bir suça ilişkin veya önceden belirlenen bir konuyla sınırlı bir arama söz konusu değildir. Şüpheli sıfatı taşıyan ve taşımayan milyonlarca kişinin hayatına dair tüm verilerinin panoraması çıkartılmakta, bunlar arasında ilişkiler kurulmaktadır. Veri havuzlarının birleştirilerek süzülmesi ile geleneksel arama tedbirlerine nazaran kişiler hakkında çok daha kapsamlı bilgi edinilmektedir. Bu durum aranılan kişinin şüpheli veya üçüncü kişi olması halinde farklı güvenceler öngören, yine arama konusunun üst araması, bilgisayar veya konut olmasına göre ayrı düzenlemeler öngören hükümleri anlamsız hale getirmektedir. Dolayısıyla arama ile öngörülen usule uyulmadan ve herhangi bir denetim öngörülmeden, çok daha fazla bilginin elde edilmesi mümkün hale gelmiştir.

Arama için kural olarak hâkim kararı alınması gerekir ve bu kararda ceza soruşturmasına konu olan eylem, aranılacak kişi, konut veya diğer yerin adresi, eşya

---

[355] Tien, s. 405.

[356] Serap Keskin Kiziroğlu, "5271 Sayılı Ceza Muhakemesi Kanunu'nda Basit Arama (Adli Arama)", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:58, Sayı:1, 2009, ss.139-168, s. 146-148.

aranacak ise hangi eşyanın aranacağı, ayrıca arama kararının ne zamana kadar geçerli olduğu belirtilmelidir[357]. Dolayısıyla aramaya başlanmadan önce verilen karar veya emirde, aramanın amacı ve sınırları çizilmekte, kapsamı belirsiz bir arama hukuka aykırı kabul edilmektedir.

Profilleme teknolojileri ise zaman ve mekân kısıtlaması gözetilmeksizin uygulanmakta; oluşturulan profiller, adeta hayalet bir kimlik gibi, sürekli kişilerin karşısına çıkmaktadır. Kişi ve gruplara dair yeni veriler, profilleme algoritmalarının daha iyi eğitileceği ve geliştirileceği iddia edilerek sınırsızca işlenmektedir. Bu bağlamda, profilleme teknolojileri, kişisel verilerin artışı ve yeni teknolojik gelişmelerle sınırsız ve süresiz bir müdahaleyi mümkün kılmıştır. Kişinin doğumundan itibaren tüm verilerine ulaşılması, klasik anlamda koruma tedbirleri düzenlendiği sırada hayal dahi edilemeyen bir olgudur. Oysa artık adli arama tedbirinin çok ötesinde, ancak adli arama için öngörülen güvencelerden yoksun şekilde verilere erişmek mümkün hale gelmiştir[358]. Dolayısıyla profilleme teknolojileri, coğrafi veya zamansal bir sınır tanımaksızın tüm verileri elde edilebilir ve incelenebilir hale getirmiştir[359].

Bunun yanı sıra arama tedbiri şeffaf şekilde uygulanan bir tedbirdir. Örneğin arama tedbirinde, soruşturma veya kovuşturma konusu fiil kişiye açıklanır, arama kapsamını belirten bir belge de istemi halinde CMK m. 121 gereği kişiye temin edilir. Yine konut aramasında arama tanıklarının süreci gözlemlemesi büyük önem taşımakta ve sürecin denetimini mümkün kılmaktadır[360]. Ceza muhakemesinde uygulanan profilleme teknolojileri ise yazılımın karmaşıklığına bağlı olarak kimi zaman taradığı veriler arasında açıklanamayan sonuçlara varmaktadır. Ayrıca ilgili kişiyi etkileyen

---

[357] Feridun Yenisey/Ayşe Nuhoğlu, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, Eylül 2021, s.419, Özbek, Veli Özer/ Doğan, Koray/ Bacaksız, Pınar, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, Eylül 2021, s.310, 311, Ünver, Yener/ Hakeri, Hakan**, Ceza Muhakemesi Hukuku**, Adalet Yayınevi: Ankara, Mayıs 2019, s.887.

[358] Forcese, Craig, "The Limits of Reasonableness: The Failures of the Conventional Search and Seizure Paradigm In Information-Rich Environments", Temmuz 2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1945269, Erişim Tarihi: 20.06.2021, s.6.

[359] Lee Tien, "Privacy, technology and Data mining", **Ohio Northern University Law Review**, Cilt:30, Sayı:3, 2004, ss. 389-416, s.402.

[360] Her ne kadar Yargıtay'ın aksi yönde kararları bulunsa da objektif gözlemci olmaları nedeniyle oldukça önemli olan arama tanıklarının bulunmaması halinde, aramayı hukuka aykırı kabul ettiği kararlar da bulunmaktadır. Bkz. 11. Ceza Dairesi, E.2017/3773, K.2021/2260,T.8.03.2012, Yargıtay 9. Ceza Dairesi, E. 2020/669,K. 2020/2006,T. 17.11.2020, https://lib.kazanci.com.tr/, Erişim Tarihi: 12.06.2021.

hukuki veya ciddi nitelikte bir karar alınana kadar kişi süreçten haberdar olmamakta, bu teknolojilerin işleyişini ve dayandıkları verileri inceleyememektedir. İnceleyebildiği ihtimalde dahi, ilgili kişinin veya müdafiinin bu mekanik süreci yorumlayabilmesi makine öğrenmesinin karmaşıklığı karşısında mümkün değildir. Yine profilleme sürecine arama tanıkları gibi üçüncü kişi gözlemcilerin katılması söz konusu değildir, süreç otomatik olarak denetimsiz şekilde işlemektedir. Dolayısıyla profilleme süreci, "kapalı kutu" şeklinde işlemesi, ilgililere her durumda bildirilmemesi ve objektif gözlemciler tarafından denetime tabii tutulmaması nedeniyle arama usulünden farklıdır.

Sonuç olarak profilleme teknolojileri, yargılamada maddi olayı gösteren delil elde etme veya faili yakalama amacından ziyade failin gelecekteki tehlikeli davranışlarını veya yeniden suç işleme ihtimalini tespit etmek üzere kullanılmakta[361], amaç, konu ve usul bakımından adli arama tedbirinden ayrışmaktadır.

Bununla birlikte amaçları bakımından ele alındığında, profilleme teknolojileri, geleceğe yönelik tehlikeleri önlemek ve suç işlenmeden önce müdahale etmeyi hedefleyen önleme araması ile birtakım benzerlikler barındırmaktadır. Bu nedenle aşağıdaki başlıkta önleme araması tedbirine ilişkin usul ve kurallar vurgulanacak ve bunlar profilleme teknolojileri ile karşılaştırılacaktır.

b) Önleme Araması ile Profilleme Teknolojilerinin Karşılaştırılması

Kolluk yalnızca suç işlendikten sonra müdahale etmekle görevli değildir, bir tehlikenin zararlı bir netice doğurmasını önlemek ve suç işlenmesini engellemekle de yükümlüdür. Bu nedenle kolluğa suç işlenmeden önce müdahalede bulunabilmek ve tehlikeleri ortadan kaldırmak amacıyla ayrıca önleyici yetkiler tanınmıştır. Önleme araması yapma yetkisi de bu kapsamdadır[362].

Önleme araması tehlikenin veya suçun önlenmesi amacıyla, kolluk görevlileri tarafından gerçekleştirilmektedir. Profilleme teknolojileri de gelecekte kamu düzenine

[361] Rik Peeters/Marc Schuilenburg, "Machine Justice: Governing Security Through the Bureaucracy of Algorithms", **Information Polity**, Cilt:23, Sayı:1, 2018, ss. 267–280, s.272, 273.
[362] Zeliha Alpsoy, **Önleme Araması**, Adalet Yayınevi: Ankara, Kasım 2019, s. 98.

tehlike oluşturabilecek veya suç işleyebilecek kişileri tespit etmek ve suç işlenmesini önlemek amacıyla kullanılabilmektedir. Bu nedenle amaç unsuru bakımından profilleme teknolojileri, adli aramalara nazaran önleme aramalarına daha yakındır.

Önleme araması yapılan yerler arasında ulaşım araçları, toplantı ve gösteri yürüyüşlerinin yapıldığı yerler ve umuma açık diğer yerler bulunmaktadır. Amaç kalabalık yerlerde somut tehlikelerin bertaraf edilmesidir. Profilleme teknolojileri de bu amaçla, toplantı ve gösteri yürüyüşleri öncesinde, bunlara katılması tehlikeli bulunan kişilere gösteri öncesi müdahale etmek[363], bazı kişilerin yine topluma karşı tehlike arz ettikleri gerekçesiyle ulaşım araçlarına erişimini ve seyahat etmelerini engellemek[364] için sevk edilebilmektedir.

Önleme araması kararı makul sebebe dayanmalıdır. Kolluk öncelikle tehlike veya suçun önlenmesi için aramanın sebebini gerekçeli şekilde açıklamalıdır[365]. Hukuk devletinde kişi hak ve özgürlüklerine yoğun bir müdahale içeren arama, kolluğun yalın sezisi üzerine gerçekleştirilemez, bu nedenle arama sebebinin somut veri ve olgulara dayanması gerekir[366]. Dolayısıyla önleme aramasına ancak somut ve öngörülebilir bir tehlike bulunması halinde başvurulabilir. PVSK kapsamında bu nitelikteki tehlike hal, "makul sebep" olarak ifade edilmektedir. Makul sebep konunun uzmanları tarafından ortak şekilde anlamlandırılıp değerlendirilen bir olgudur[367]. Her ne kadar makul sebep, kolluğun kişisel tecrübe ve bilgisinden yola çıkarak olayı değerlendirmesi itibariyle makul şüpheye göre daha sübjektif bir nitelik taşısa da[368],

---

[363] Göstericilerin online takibinin ve göstericilere ait profil oluşturulmasının, hukuki denetime tabi tutulmaksızın ve öngörülemez şekilde yapıldığı takdirde, toplantı ve gösteri hakkının kullanılmasında caydırıcı etki uyandırdığına dair bkz. The University of Oxford, **The Law on Policing Peaceful Protests**, September 2020, https://www.law.ox.ac.uk/sites/files/oxlaw/opbp_report_on_the_law_on_policing_peaceful_protests_0.pdf, Erişim Tarihi: 29.06.2021, s.6, 25.

[364] CAPPS II (Computer Assisted Passenger Pre-screening System) programı ve bu programın takipçisi Secure Flight Programı ile kişiler, hangi verilere dayanarak oluşturulduğu şeffaf şekilde paylaşılmayan "izleme listeleri"ne kaydedilebilmekte ve bu listede yer alan kişilerin seyahat hakları kısıtlanmakta veya güçleştirilmektedir, bu yönde bkz. Florence, s.2156, 2157.

[365] Nitekim PVSK m. 9/2 de arama talep yazısında, arama için makul sebeplerin oluştuğunun gerekçelendirilerek belirtilmesi gerektiğini düzenlemektedir, bkz. Yenisey/Nuhoğlu, s.302, 303.

[366] Şemsettin Aksoy, **Önleme ve Koruma Tedbiri Olarak Arama**, İstanbul Üniversitesi Kamu Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul 2006, s.103.

[367] Makul sebep makul şüphe kavramıyla karıştırılmamalıdır. Makul şüphede çok sayıda ve sıradan kişilerin somut bir olguyu aynı yönde değerlendirmeleri beklenir, bkz. Yargıtay Ceza Genel Kurulu, E. 2016/20-800 K. 2017/120, T. 28.2.2017, https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=ycgk-k.-2017_120-c.-savcinin-emri-olmadan-adli-arama-uyus%CC%A7turucu.pdf, Erişim Tarihi: 21.06.2021.

[368] Alpsoy, s.116, 117.

kolluğun gözlem üzerine önlenmek istediği tehlike soyut değil, somut ve öngörülebilir olmalıdır[369].

Bununla birlikte profilleme teknolojileri, çoğu durumda henüz makul bir sebep oluşmadan uygulamaya konulmaktadır. Günümüzde kamu düzenini tesis etmek ve toplumları potansiyel terör saldırılarından korumak, adeta tek başına bir makul sebep haline gelmiştir. Dolayısıyla bu teknolojiler, somut bir tehlike söz konusu olmadan dahi suç işlenmesi ihtimalini azaltacakları iddiasıyla sınırsız bir şekilde sevk edilmektedir. Bununla birlikte, herhangi bir makul sebebe bağlı olmaksızın başvurulan bu sistemlerin vardıkları sonuçlar, kişiler hakkında idari veya adli kararlara dönüşebilmekte veya en azından kişiler üzerinde gözetimin arttırılması veya haklarında soruşturma başlatılmasına yol açabilmektedir[370].

Önleme aramasının dayandığı makul sebep, makul şüpheye benzer şekilde kişilerin mevcut davranışlarının somut olayın koşulları altında değerlendirilmesini ve bulunulan yer, zaman gibi unsurların da gözetilerek tehlike veya suç ihtimalinin somutlaştırılmasını gerektirir. Makul sebep, kolluğun bireysel tecrübe ve bilgisini kullanmasını, dolayısıyla sübjektif bir gözlem yapmasını da gerektirir. Profilleme teknolojileri ise mevcut davranışın gözlenmesine ve işin uzmanı bir kişi tarafından değerlendirilmesine dayanmaz. Daha ziyade, determinist bir şekilde benzer nitelikte geçmişe, alışkanlıklara, aile yapısına sahip kişilerin topluma tehlike oluşturacakları varsayımına dayanır ve bu varsayımın tek kaynağı veriler ve veriler arasında makinelerce kurulan bağlardır. Dolayısıyla bireysel gözlem yerini insanların iradi hareketlerinin reddedildiği ve istatistiki verilere indirgenerek neredeyse kimliksizleştirildiği matematiksel bir modele terk eder[371]. Ancak genellemelere dayalı ve gerçek hayatta teyit edilmemiş bu çıkarımlar, makul sebep teşkil etmemektedir.

---

[369] Kılıç, Ergin, **Türk Hukukunda Adli ve İdari Aramalar**, İstanbul Üniversitesi Kamu Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, Ankara 2004, s.110. Örneğin, makul sebep için bir yerde her yıl önemli günlerde olaylar çıktığı iddiası genel ve yetersiz olup, yapılan istihbari çalışmalar, çevre araştırmaları, olağan olmayan hareketlilikler belgelerle gösterilerek, tehlikenin belirtilen zamanda somut bir şekilde oluştuğu ispatlanmalıdır.

[370] Daniel J. Steinbock, "Data Matching, Data Mining, and Due Process," **Georgia Law Review**, Cilt: 40, Sayı:1, Güz 2005, ss. 1-84, s. 17.

[371] Yves Cartuyvels, "Profilage et Datamining dans le Monde de la Pénalité: Vers Une Sortie Du Droit?", https://dial.uclouvain.be/pr/boreal/object/boreal%3A203248/datastream/PDF_01/view, ErişimTarihi:29.06.2021.

Profilleme teknolojilerinde önleme aramasında olduğu gibi gerçek bir kişi tarafından değerlendirme söz konusu değildir. Başka bir deyişle önleme araması için makul sebebin oluşup oluşmadığı takdir edilirken veya önleme araması kararı alınırken tedbirin gerekliliği daha tedbir uygulanmadan önce gerçek bir kişi tarafından değerlendirilmektedir. Profillemede ise kolluk görevlisi veya diğer mercilerin müdahalesi ancak profilleme teknolojilerinin bir sonuca varmasının ardından gerçekleşmektedir. Oysa algoritmalar, pek çok suça tanıklık etmiş, pek çok kişiyi daha önce gözlemlemiş uzmanlara nazaran kişinin davranışlarını bağlamı içerisinde değerlendirmekten yoksundur[372]. Örneğin, önleme aramasında kolluk kişinin hareketleri ve ortamı gözlemleyerek, bu gözleme dayalı müdahalede bulunmaktadır. Elbette idari aramalarda da kişilerin hatalı şekilde durdurulması, durdurma ya da arama sırasında belirli ön yargıların devreye girmesi mümkündür. Ancak aramanın yerinde olmadığı anlaşıldığında tedbir sona erdirilecek, kişi arama sebebi ve sonucu konusunda bilgilendirilmiş olarak olay yerinden ayrılabilecektir. Dolayısıyla önleme araması geçici nitelikte olup kişinin hak ve özgürlüklerini uzun süreli kısıtlayıcı bir etki doğuramaz. Bunun yanı sıra hukuka aykırı şekilde yapılan aramalara karşı hukuki sonuç ve yaptırımlar öngörülmüştür. Oysa profilleme teknolojilerinin sürecin en başında hatalı verilere dayanması veya mantığa aykırı sonuçlara yol açması halinde, bu hatalı durum tedbirin sonlandırılmasına yol açmamaktadır. Aksine varılan bu sonuçlar başka kararlar için "girdi" olarak değerlendirilmekte ve kişinin türetilen verilerinin yeniden kullanımı ile hatalı verilerin sonuçları katlanarak ağırlaşabilmektedir[373]. Örneğin kişinin hatalı şekilde "terörist izleme" listelerine kaydedilmesi veya bu listelerin çok geniş kriterlerle düzenlenmesi halinde, listeye giren kişilerin uçuş izinleri iptal edilecek, vize başvuruları reddedilebilecek, aranmaları ve adli soruşturmaya konu olmaları söz konusu olabilecektir. Dolayısıyla bu listeler, kişilerin yeni listelere girmesine, adli, idari, ticari yaptırımlara maruz kalmasına yol açmakta ve kişiler üzerinde kalıcı bir damga bırakmakta, buna rağmen gerçek bir değerlendirilmeden geçirilmemektedirler.

Önleme araması ile profilleme, konuları itibariyle de oldukça farklıdır. Önleme araması suç yoluna girilmeden önce kişilerin üst ve eşyalarında arama yapmayı mümkün kılmaktadır. PVSK m. 9/5 gereği konutta, yerleşim yerinde ve kamuya açık

[372] Steinbock, s.42.
[373] Steinbock, s.18.

olmayan işyerlerinde ve eklentilerinde önleme araması yapılması yasaklanmıştır. Nitekim henüz suç şüphesinin dahi söz konusu bulunmadığı durumlarda, kişilerin özel hayatına yoğun müdahale içeren konut araması yapılamaması yerinde bir düzenlemedir[374].

Bununla birlikte profilleme teknolojilerinin dayandığı veriler bugün hayatın her alanını kapsamaktadır. Akıllı fırın, bilgisayar, mutfak gibi pek çok eşya ile konut içi alan dahi bir "veri fabrikası"na dönüşmüştür. Google, Amazon gibi firmaların ev içinden edindikleri verileri bu verileri profillemeyerek belli sonuçlara varmakta[375], gerektiğinde bu bilgiler kolluk görevlileri ile paylaşılmaktadır. Yine önleme aramasında Arama Yönetmeliği m. 28 gereği, kişinin üstünde veya eşyasında rastlanan özel kâğıt ve zarflar dahi açılamaz, açıksa yazılı bilgiler okunamaz. Profilleme açısından kapalı kapılar ardında kalan hiçbir veri söz konusu değildir. Veri tabanlarındaki tüm veriler, değerlendirmeye tabidir. Dolayısıyla profillemenin konusu, önleyici aramada olduğu gibi sınırlandırılarak çizilmemiştir. Profilleme, yalnız umuma açık alanlar ve kişilerin belirli bir zaman diliminde üzerinde bulundurdukları eşyalar ile sınırlı kalmaksızın gerçekleştirilmektedir.

Diğer bir fark, profilleme teknolojileri kullanılırken, suç şüphesinin doğması üzerine ayrı bir rejimin devreye girmemesidir. Ancak önleme araması suç şüphesi doğması ile birlikte sona erecek, suça işaret eden delil elde etme veya şüpheliyi yakalama amacı söz konusu olduğu anda artık CMK kapsamında adli arama kuralları uygulanacaktır. Başka bir deyişle basit suç şüphesinin oluşmasının ardından adli arama kuralları devreye girmelidir[376]. Profillemede ise suç şüphesi oluştuğu takdirde, ilgili kişilere yönelik şüpheli haklarını garanti altına alan ayrı bir rejim uygulanmamaktadır.

PVSK m. 9/2 gereği arama kararında veya emrinde, aramanın sebebi, konusu, kapsamı, yapılacağı yer, zaman ve geçerli olacağı süre gösterilmek zorundadır. Kural olarak arama işlemi, tehlike veya suçun önlenmesi amacına ulaşılması ya da aranan

[374] Bu durumun tek istisnası PVSK m. 20'de öngörülen büyük tehlike ve suçların önlenmesine ilişkin istisnai durumlardır, bkz. Alpsoy, s. 103.
[375] Sophia Maalsen/Jathan Sadowski, "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance", **Surveillance and Society**, Cilt:17, Sayı:1/2, 2019, ss.118-124, s.118.
[376] Eşref Barış Börekçi, "Yeni Düzenlemeler Işığında Önleme Aramaları", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 17, Özel Sayı, 2020, ss.89-113, s.95.

şeyin bulunamayacağının anlaşılmasıyla sona erer. Amaca ulaşıldığı takdirde kararda belirtilen sürenin dolması beklenmeyecektir[377].

Oysa "toplumu tehlikelerden koruma" iddiası ile sevk edilen profilleme teknolojileri açısından herhangi bir süre öngörülmemiştir. Bu amaca ne zaman ulaşılacağını tespit etmek ise mümkün değildir. Örneğin tehlikeli kişiler listesine giren bir kişi suç işlerse, profilleme amacına ulaşmış sayılacak mıdır? Aksi halde, bir kişi tahmin edildiğinin aksine suç işlemezse, ne kadar yıl içinde bir listeden silinmelidir? Bu sorulara yanıt veren düzenlemeler henüz öngörülmediğinden, profilleme teknolojileri özelinde gerçekleştirilen işlemin nedeni, sınırları ve süresi belirsizdir.

Sonuç olarak, profilleme teknolojileri ile kişinin konut içerisinde ve kamusal alanlarda bıraktıkları izlere dair sınırsız sayıda verinin işlenmekte, bu veriler istatistiksel şekilde gruplandırılmakta ve bunlardan yola çıkarak kişinin karakteri ve gelecek davranışları su yüzüne çıkarılmaya çalışılmaktadır. Ancak geleneksel anlamda önleme araması tedbirinden farklı olarak profilleme teknolojileri gözlemden yola çıkan makul bir sebebe değil, belli kişilerin karakterlerinden veya ait oldukları grup ve sınıflarından ötürü suçlu oldukları veya suç işlemelerinin an meselesi olduğu varsayımına dayanmaktadır. Bu bağlamıyla daha ziyade pozitivist akımın yeniden doğuşu olan profilleme teknolojileri, klasik ekolden farklı olarak kişinin iradesi olduğu ve suç teşkil eden bir eylemi gerçekleştirmemeyi seçebileceği ihtimalini reddetmektedir. Dolayısıyla kişiler, bizatihi varoluşlarından ötürü risk olarak kategorize edilmektedir[378]. Bu nedenle profilleme teknolojileri sadece amaçları, konuları ve usulleri bakımından değil, dayandıkları düşünsel zemin bakımından da gerek adli arama gerekse önleme araması tedbiri kapsamında ele alınamayacaktır.

2. Profilleme Teknolojilerinin Fizik Kimlik Tespiti ile Karşılaştırılması

Fizik kimliğin tespiti, bireyi diğerlerinden ayırmayı sağlayan, beden ölçüleri, parmak izi, avuç izi, ayak izi, sesi gibi fiziksel özelliklerinin belirlenmesi ve kayda

---

[377] Alpsoy, s. 168.

[378] Failin tehlikeliliği anlayışının ceza hukukunu yeniden ele geçirmesi üzerine bkz Michel Foucault, "About the Concept of the 'Dangerous Individual' in 19th Century Legal Psychiatry", **International Journal of Law and Psychiatry**, Cilt: 1, ss. 1-18, 1978, s.16 vd.

alınmasıdır[379]. Profillemede ise fizik tespitinde olduğu gibi bedensel nitelikler ve biyometrik verilerin ötesinde kişinin geçmiş tüm hareketleri, mesleği, banka verileri, nüfus verileri, eğitim durumu, sosyal statüsü, sabıka kaydı gibi verileri esas alınır. Dolayısıyla kişinin kimliği fiziki nitelikleri üzerinden değil, siyasi, sosyal hayatıyla birlikte bir bütün olarak tanımlanmaya çalışılır.

Kişinin karakter analizi ve gelecek faaliyetlerini tespit etme iddiasındaki profilleme teknolojileri, salt failin kimliğinin tespitini amaçlayan fizik kimlik tespitinden oldukça farklıdır. Fizik kimlik tespiti, daha ziyade veri eşleştirme tedbiri ile yakından ilişkilidir. Veri eşleştirme, dijital olarak işlenmiş biyometrik verilerin ve parmak izlerinin veri tabanında aranarak şüphelininkiyle eşleştirilmesini içerir. PVSK m. 5 kapsamında yapılan düzenleme gereği kolluk görevlileri tarafından CMK fizik tespiti sırasına alınan fotoğraf ve parmak izlerinin yanı sıra suç ile ilişkili olmayan ruhsat, sürücü belgesi, pasaport alımı için başvuranların ve gönüllü olanların parmak izi ve fotoğraf kaydının alınması öngörülmüştür. Bu veriler AFIS[380] sisteminde saklanacak, sonradan örneğin olay yerinde bulunan izler, sistemde bulunan veriler ile karşılaştırılacaktır. Dolayısıyla farklı kişi gruplarına ait parmak izi ve fotoğraflar sonradan kullanılmak üzere saklanmaktadır[381]. Veri eşleştirme, günümüzde, yalnızca AFIS veri sisteminde toplanan veriler üzerinden yapılmamaktadır. Kolluk, internet servis ve erişim sağlayıcıları ve özel şirketlerin verilerine de erişebilmektedir. Bununla birlikte PVSK m. 5, kolluğun AFIS dışındaki veri tabanlarına hangi şartlar altında erişebileceğini ve hangi hallerde bu veri tabanlarındaki verilerle şüphelinin verisini eşleştirme yetkisi olduğunu düzenlememiştir. Dolayısıyla günümüzde ceza muhakemesi özneleri ve idari kurumların dışında, özel şirketler çok daha fazla veri işlemekte ve kolluk görevlileri bu verilere bilgi toplama gerekçesiyle sınırsız şekilde erişebilmektedir[382]. Dolayısıyla veri toplamaya ilişkin PVSK ve CMK kapsamında öngörülen sınırların etrafından dolanmak mümkün hale gelmiş, veri eşleştirme tedbiri, profillemeye benzer şekilde sınırsızca uygulanma zemini bulmuştur.

.

---

[379] Özbek/Doğan/Bacaksız, s.444.

[380] AFIS, Automated Finger Identification System (Otomatik Parmak İzi Tanımlama Sistemi) ifadesinin kısaltmasıdır.

[381] Centel/Zafer, s.362, 363, Erdoğan Tetik, "Kimlik Tespitinde Parmak İzi Arşivlerinin Gerekliliği ve Ülkemizdeki Durumun Değerlendirilmesi, https://www.caginpolisi.com.tr/eski_sitemiz/35/42-43-44-45-46-47.htm, Erişim Tarihi: 30.06.2021.

[382]Michael Isaac, "Privatizing Surveillance: The Use of Data Mining in Federal Law Enforcement", **Rutgers Law Review**, Cilt: 58, Sayı: 4, Yaz 2006, ss. 1057-1090, s.1058.

Verilerin çokluğu ve teknolojinin sağladığı imkân ile profilleme teknolojileri, şüpheli olan ve olmayan ayrımı yapmaksızın tüm kişilerin verilerinden yola çıkabilmektedir. Ancak profillemenin asıl amacı, bu verilerle soruşturma sırasında elde edilen verileri eşleştirmek değil, benzer şekilde davranış sergileyen kişileri belli kategoriler altında gruplandırmaktadır. Gruplandırma, belli nitelikleri taşıyan insanların gelecekte de benzer şekilde davranacağına dair duyulan inanca dayanmaktadır. Otomatik profilleme teknolojileri ile varılan sonuçlar ile gelecekte suç işleme riski barındıran kişiler tespit edilmeye çalışılmaktadır[383]. Bu kişilere benzer karakteristik ya da davranış biçimi gösteren herkes grup içinde listelenmekte ve bu yolla risk listeleri oluşturulmaktadır. Ancak bu uygulama, kişilerin fiziki verilerinin alınarak polis veri tabanındaki fiziki kimliğine ilişkin verilerle eşleştirilmesinden çok daha farklı ve haklara daha yoğun müdahale içeren bir uygulamadır[384]. Kişilerin yalnız fiziksel biyometrik verileri değil, yaş, cinsiyet ve davranış kalıpları ele alınmakta ve suç işleme riski arasında yazılımlar eliyle tekrarlayan özellikler tespit edilmektedir. Ancak kimi durumda makineler eliyle, riskli kişiler arasında insan muhakemesi ile anlaşılamayan bağlantılar kurulmaktadır[385]. Profilleme, milyonlarca kişiyi belli istatistiklere indirgemekte ve hayatın olağan akışında bir bağlam içerisinde ele alınmayan bu istatistiklere göre öngörülerde bulunmaktadır. Bu süreç, belli bir şüphelinin nüfus kimliğini tespit etmekten ziyade, "topluma uyumlu" veya "zararlı" bir insan olup olmadığını tespit etmeyi içerir. Henüz suç teşkil eden bir hareketin işlenmesi söz konusu olmadan kişilerin önceden davranışlarını kestirebilme ve buna göre önlem alabilme amaçlanır. Dolayısıyla profillemede belirli bir suç isnat edilmiş bir şüphelinin ferden tespit edilmesi ve yargılama ve ardından cezanın infazının gerçekleştirilebilmesi amacı bulunmamaktadır. Genel olarak "tehlikeli kişiler", "kaçma riski bulunan kişiler", "tekrar suç işleme ihtimali yüksek" kişiler listesi oluşturulması ve bunlara dair uzun vadeli bir politikanın belirlenmesi söz konusudur[386].

Sonuç olarak profillemenin kişiler hakkında dijital bir kimlik öngördüğünü ancak bu kimlik öngörülürken toplanan verilerin fiziksel nitelikler ve biyometrik

---

[383] Katja de Vries,"Identity, Profiling Algorithms and a World of Ambient Intelligence", **Ethics and Information Technology**, 2010, Cilt:12, Ocak 2010, ss. 71–85, s.77.
[384] Lothar Fritsch, "Profiling and Location-Based Services (LBS)", içinde **Profiling the European Citizens**, Ed. Mireille Hildebrandt/Serge Gutwirth, Springer: Dodrecht, 2008, ss.147-168, s. 150.
[385] Steinbock, s.9, 10.
[386] Kehl/Priscilla/Kessler, s. 9, 13.

verilerle sınırlı olmadığını söylemek mümkündür. Yine bu kimlik, kişinin biyometrik verileri ile kıyaslanarak kim olduğunu tespit etmek üzere kullanılmamaktadır. Aksine, kişinin kim olduğu, bağlamından koparılan verilerle, bireyselleştirilmeden tanımlanmakta, benzer bulunduğu gruptaki diğer üyelerle aynı nitelikleri taşıdığı varsayılmaktadır. Dolayısıyla kişilerin sanal ve otomatik şekilde belirlenen bir grup kimliği içerisine hapsedilmesi söz konusudur.

Haklara daha yoğun müdahale içermesine rağmen, profilleme teknolojilerine maruz kalan kişiler açısından usuli güvenceler öngörülmemiştir. Örneğin CMK m. 81 kapsamında fizik kimlik tespitinin gerçekleştirilebilmesi için öncelikle üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı soruşturma başlatılmış olması aranmıştır. Söz konusu tedbir yalnızca şüpheli ve sanık sıfatını taşıyan kişilere uygulanabilecektir[387]. Fizik kimliğin tespiti için basit şüphe yeterli değildir. Nitekim insan bedenine müdahale içeren ve insan onuru ile ilintili fiziksel tespit, her basit kuşku düzeyinde yapılamamalıdır[388]. Bu güvenceler aynı zamanda susma hakkı ve kişinin aleyhine delil vermeye zorlanmama hakkıyla da ilişkilidir. Profilleme teknolojileri ise, salt fiziksel verilerin değil, kişilere ait tüm verilerin analiz edilmesini içermektedir. Kişilerin bir gün cezai ve idari yaptırıma konu olacaklarını bilmeden bıraktıkları tüm izlerin ve şirketler tarafından paylaşılan verilerin toplanması, analiz edilmesi ve yargılama sırasında kullanılması, susma veya aleyhe delil göstermeme hakları işlevsiz kalmaktadır.

Fizik kimlik tespiti otomatik olarak yakalanan veya gözaltına alınan herkese uygulanabilecek bir tedbir değildir. İşlenmiş suça ilişkin şüpheli veya sanığın kimliğinin tespitinde tek elverişli araç olması halinde uygulanmalıdır. Bu durumda sanığın fizik kimliğinin tespiti, ancak suç şüphesi altındaki kişinin kimliğinin doğru olmadığı yönündeki kuşkunun giderilememesi halinde gerekli olacaktır[389]. Bu nedenle ileride işlenecek suçlarda kullanılmak üzere ihtiyaten CMK m. 81 kapsamında kimlik tespiti yapılması hukuka aykırıdır[390]. Oysa risk analizi yapan profilleme teknolojileri,

---

[387] Ünver/Hakeri, s. 609. Ancak iddianamenin düzenlenmesi için kişinin birey olarak belli olmasının yeterli olduğu, kimliğinin tereddüde yer bırakmayacak şekilde tespitin ancak yargılama sürecinde gerekli olduğunu ileri süren görüşler de bulunmaktadır, bkz. Centel/Zafer, s. 571.

[388] Ömeroğlu, Ömer, "Ceza Muhakemesinde Şüpheli ve Sanığın Fizik Kimlik Tespiti", **Türkiye Barolar Birliği Dergisi**, Cilt: 27, Sayı: 115, Kasım 2014, ss.61-102, s.76.

[389] Ömeroğlu, s.74.

[390] Ünver/Hakeri, s.639.

"tehlikeli kişi" kimliği oluştururken, kamu düzenini sağlama adına geleceğe yönelik bir önlem almakta, dolayısıyla suç teşkil eden ve daha önce işlenmiş bir fiilin failini tespit için zorunlu olma koşulunu karşılamamaktadır.

Dolayısıyla profilleme teknolojileri, amaçları, usulleri ve sonuçları bakımından fizik kimlik tespiti tedbiri kapsamında değerlendirilemeyecektir.

3. Koruma Tedbirlerinin Temel Nitelikleri Çerçevesinde Profilleme Teknolojileri

a) Amaç Unsuru Bakımından Değerlendirme

Koruma tedbirleri ceza muhakemesinin gerçekleştirilmesini mümkün kılan ve muhakeme sonucunda verilerin kararın uygulanabilmesini sağlayan tedbirlerdir. Ceza muhakemesinde maddi gerçeğe ulaşılmasına, delillere ulaşarak, ulaşılan delilleri güvence altına alarak ve kişinin yargılama sırasında hazır bulunmasını sağlayarak hizmet ederler[391]. Adil yargılanma hakkının temellerinden biri olan yargılamanın mümkün olduğunca kısa sürede yapılması ilkesinin gerçekleştirilmesinde, en önemli araçlardan biri de koruma tedbirleridir[392].

Koruma tedbirleri, her ne kadar belli bir şüphenin oluşması üzerine uygulansa da uygulandıkları sırada henüz şüpheli veya sanığın suçu sabit olmamıştır. Bu tedbirlerin henüz herhangi bir hükme varılmadan kişi özgürlüğü, konut dokunulmazlığı, özel hayatın gizliliğine yönelik ağır müdahaleler teşkil ettikleri açıktır. Bu nedenle ilgili tedbirlerin "peşin bir ceza mahiyetine" dönüşme olasılığına karşı sıkı şartlara bağlanmaları gerekir[393].

Profilleme teknolojileri ise suç işlediğinden şüphelenilen kişinin topluma tehlike oluşturup oluşturmadığı, kaçma riski ve yeniden suç işleme ihtimalini tespit etmekte ve bu tespitler Amerika, İngiltere gibi ülkelerde kişinin gözetime tabi tutulması, hakkında tutuklama kararı verilmesi veya hüküm verilmesi sırasında dikkate

---

[391] Ünver/Hakeri, s.679.
[392] Özbek/Doğan/Bacaksız, s.222.
[393] Faruk Yasin Türinay, "Ceza Muhakemesi Hukukunda Koruma Tedbirlerinin Sınıflandırılması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:70, Sayı:2, 2021, ss. 475-541, s. 480.

alınmaktadır. Birinci bölümde "Yapay Zekâ Teknolojilerinin Ceza Muhakemesi Alanında Kullanılması" başlığı altında tartışıldığı üzere bu teknolojilerin bir kısmı suç işlenecek yerin ve suç işleyecek kişinin tespit edilmesi için sevk edilmektedir. Bu bağlamda suç işlendikten sonra delil elde etme ve failin kaçmasını engellemekten ziyade suçu önleme amacı taşıdığından idari tedbirlere yaklaşmaktadırlar. Nitekim adli koruma tedbirlerinden farklı olarak idari ya da önleyici tedbirler, henüz ortada suç teşkil eden bir hareket yokken, suç ve tehlikeleri önleme amaçlı sevk edilirler. Asıl amaçları muhakemenin işleyişini mümkün kılmak ve kararın infazını sağlamak değildir, kişileri suç yoluna girmeden önce engellemek üzere idari tedbirlere başvurulur. Durdurma, önleme araması ve önleyici amaçla iletişimin denetlenmesi gibi idari tedbirler de hak ve özgürlüklere müdahale içerir. Bu nedenle önlenmek istenen tehlike, hakların kısıtlanmasını haklı kılmak adına somut bir tehlike olmalıdır[394].

Örneğin Precobs yazılımı daha önce hırsızlık suçunun işlendiği bölgelerde, suçun ne zaman, nerede, ne şekilde işlendiği ve hangi eşyaların çalındığını tespit etmekte, bu şekilde toplanan veriler arasında analiz yaparak bir sonraki suçun nerede işleneceğini öngörmeye çalışmaktadır[395]. Bu amaç kuşkusuz ki koruma tedbirlerinin amacından farklıdır. Benzer şekilde ihbarda bulunulan veya re'sen tespit edilen suç oranlarını öncelikli olarak dikkate alarak analiz yapan Predpol ve CommandCentral gibi yazılımlar da suç mahallini suç işlenmeden veya kişilerin hakları bir tehlike altına girmeden önce tespit etmek amacıyla kullanılmaktadır. Bununla birlikte, Los Angeles ve Santa Cruz polisi tarafından başvurulan Predpol'ün sonuçlarından biri özellikle kolluk devriye araçlarının ağırlıklı olarak gönderildiği bu yerlerde daha fazla durdurma ve arama yapılması, daha çok suç tespit edilmesi olmuş, sonuçta sıklıkla kolluk müdahalesi ile karşılaşan bu bölgelerin risk oranı sistemde daha yüksek gözükmüştür. Dolayısıyla yazılımların işaret ettiği belli bölgeler sistemde sürekli "temiz" bölge gözükürken, diğerleri kısır döngü şeklinde "kırmızı bölge" ilan edilmiştir[396].

Potansiyel faillere yoğunlaşan ve yeniden suç işleme riski bulunanları tespit eden profilleme teknolojileri ise tehlikeli kişilik analizi yapmakta ve kimi zaman suç işlenmesini önleme amacıyla idari tedbirler alınmasına kimi zaman ise ceza

---

[394] Ünver/Hakeri, s. 681.
[395] Lundschien, "Predictive Policing: Wie Algorithmen bei der Verbrechensbekämpfung Helfen".
[396] Keith Kirkpatrick, "It's not Algorithm, It's the Data", **Communications of Association for Computing Machinary**, Cilt:60, Sayı:2, Şubat 2017 pp. 21-23, s. 23.

muhakemesi aşamasında örneğin tutuklama kararı veya şartlı salıvermenin reddedilmesine temel oluşturmaktadır. Suç öncesi alanda profilleme teknolojileri idari tedbirlere benzemekle birlikte, ceza muhakemesi alanında bunlara başvuruldukları takdirde bu teknolojilerin hukuki nitelikleri tartışmaya açılmalıdır. Nitekim kişilerin yeniden suç işleme ihtimali ya da tehlikeliliklerinin tespit eden profilleme teknolojilerine, yalnızca şüpheli veya sanıklara ilişkin delillerin elde edilmesi veya muhakeme sürecinde hazır bulundurulmalarını sağlamak amacıyla başvurulmamaktadır. Daha ziyade bu teknolojiler, toplum için tehlike arz eden kişileri toplumdan ayırmak amacıyla kullanılmaktadır.

Profilleme teknolojileri aslında suçun kişisel veya toplumsal nedenlerle meydana geldiğini ve belli profile sahip suçluların determinist şekilde yeniden suç işleyeceği varsayımına dayanmaktadır. Nitekim bu teknolojiler, dava konusu fiille ile fail arasında bağ kurmamakta, failin fiili gerçekleştirdiği sıradaki kusurlu iradesi ile ilgilenmemektedir. Daha ziyade topluma zarar verme potansiyeli barındıran kişilere karşı toplumsal savunmanın gerçekleştirme, dolayısıyla bu kişileri toplumdan uzaklaştırma mantığına dayanmaktadırlar. Dolayısıyla, ceza hukukunda yeniden doğan pozitivist anlayışa göre, "kötü" yaşayış tarzı, fizyolojik veya düşünsel özellikleri nedeniyle kimi şahıslar daha önce hiçbir suç işlememiş olsa dahi tehlikeli olduklarını ortaya koyabilirler[397]. Bu durum profilleme teknolojilerini ceza muhakemesine bir nevi "idari" ve "önleyici" amaçları dâhil eden güvenlik tedbirlerine yaklaştırmaktadır. Nitekim koruma tedbirleri bir ceza değildir, aşağıda tartışılacağı üzere maddi gerçeğe ulaşmak için geçici nitelik arz eden araçlardır. Bugün bu araçların pozitivist ekol etkisiyle kişileri toplumdan uzak tutmak için kullanılması, ilgili teknolojileri muhakemesi kapsamında sınıflandırılması oldukça güçleşmekte ve hümanist ceza hukuku anlayışını zedelemektedir. Bu durum, koruma tedbirlerinin bir nevi peşinen cezalandırma ve toplumdan uzaklaştırma mekanizması olarak kullanıldığı yeni ve tehlikeli bir ceza hukuku anlayışının kapılarını aralamaktadır.

[397] Mehmet Emin Artuk, "Güvenlik Tedbirleri", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:12, Sayı:1-2, 2008, ss.461-492, s.467.

b) Araç Olma Özelliği Bakımından Değerlendirme

Koruma tedbirleri, tedbir kavramının da ima ettiği üzere yargılamada maddi gerçeğe ulaşmak ve cezanın infazını sağlamak için yalnızca birer araçtır. Başka bir deyişle, koruma tedbirleri ceza muhakemesinde bizatihi bir amaç olamazlar. Amaca ulaşıldığı anda derhal sona erdirilmeleri gerekir. Bu nedenle kişi hakkında hüküm verilene kadar beklenilmeksizin, sevk edilme amaçlarına ulaşılıp ulaşılmadığı kontrol edilmelidir[398].

Tedbirler aynı zamanda birbirlerinin aracı da olabilir. Örneğin yakalama tedbiri, gözaltı ve tutuklamanın aracı, arama tedbiri ise el koyma tedbirine aracıdır. Bununla birlikte tüm tedbirler ceza muhakemesinin maddi gerçeğe ulaşması için muhakemenin işleyişine hizmet ederler[399].

Profilleme teknolojileri, yukarıda da açıklandığı üzere belirli tedbirler alınmasına aracılık etmektedir. Bu teknolojilerin belirledikleri tehlikelilik veya mükerrer suç işleme puanlamaları, arama veya tutuklama gibi kararlar alınmasına araç olabilmektedir. Bununla birlikte, profilleme teknolojilerinin genel amacının yargılamanın işleyişine hizmet etmek, fiilden yola çıkarak yoğunlaşmış şüpheyi güçlendirebilmek amacıyla somut deliller elde etmek olduğunu söylemek mümkün değildir. Bu yönüyle profilleme teknolojilerinin somut olaydaki maddi gerçeğe ulaşmaya hizmet etmemektedir. Profilleme teknolojileri daha ziyade, failin tehlikeliliğini amprik olmayan, genellemelere dayanan bir şekilde tespit etmeye çalışmaktadır.

c) Geçici Olma Özelliği Bakımından Değerlendirme

Koruma tedbirlerinin araç olmaları, aynı zamanda geçici olarak uygulanmalarını gerektirir. Koruma tedbirlerine yalnızca ceza muhakemesinin işleyişi ve cezanın infazını mümkün kılmak için ihtiyaç olduğu sürece başvurulur. Geçici olma aynı zamanda koruma tedbirlerinin yaptırım niteliğinde olmadığını gösterir ve belirli bir

---

[398] Bahri Öztürk/Behiye Eker Kazancı/Sesim Soyer Güleç, **Ceza Muhakemesi Hukukunda Koruma Tedbirleri**, Seçkin Yayınevi: Ankara, Mart 2021, s.34
[399] Ünver/Hakeri, s.683.

süre uygulanmalarını gerektirir[400]. Kimi koruma tedbirlerinde, tedbirlerin düzenlendiği maddelerde bu süre açıkça öngörülmüştür. Örneğin CMK m. 91'da gözaltı süresi, yakalama yerine en yakın hâkim veya mahkemeye gönderilmesi için zorunlu süre hariç, yakalama anından itibaren yirmi dört saati geçemez. Yine kural olarak teknik araçlarla izleme CMK m. 140/3 gereğince en çok üç haftalık süre için karar verilebilir. Bu süre gerektiği takdirde bir hafta daha uzatılabilecektir. Bunun yanı sıra, geçicilik ilkesi gereği, bir tedbir amacına ulaşmakla birlikte başka bir tedbirin uygulanmasıyla sona erebilir. Örneğin yakalama tedbiri, şartları oluştuğu takdirde cumhuriyet savcısının emriyle yerini gözaltı tedbirine bırakabilecektir[401].

Bununla birlikte geçicilik tüm koruma tedbirlerine içkin bir unsurdur. İlgili koruma tedbiri için kanunda belli bir süre öngörülmemiş olsa dahi tedbiri haklı gösteren sebep ortadan kaltığında tedbir sona erecektir. Bu durum hem masumiyet karinesi hem de ölçülülük ilkesinin bir gereğidir[402].

Profilleme teknolojileri ise koruma tedbirlerinden farklı olarak kişilerin veya mahallelerin tehlikeliliğini ölçmekte, gösterdikleri oranlarla kişiler hakkında neredeyse ömür boyu damgalayıcı bir etki doğurmaktadır. Bu profiller, bankalar, sigorta şirketleri, özel kurumlarca paylaşılmakta, ceza muhakemesinde yeniden kullanılmakta, ardından örneğin işveren kurumlarına aktarılabilmektedir. Dolayısıyla profilleme, amacına ulaşılması ile sonlanan bir tedbir olmaktan ziyade, elden ele aktarılan ve zaman içerisinde sürekli kişilerin karşısına çıkan sonuçlar doğurmaktadır[403]. Bu durum kişi hakkında neredeyse peşin bir hüküm niteliği taşımaktadır. Bir önceki bölümde üzerinde durulan kişiler verilerin korunması normları her ne kadar kişilere haklarında alınan otomatik kararların insan müdahalesi ile gözden geçirilmesini talep etme imkânı tanısa da profillemelerin vardığı sonuçların silinmesine ilişkin açık düzenlemeler bulunmamakta, toplanan veriler farklı amaçlarla sürekli yeniden kullanılmaktadır. Bu durum, profilleme teknolojilerini, ceza muhakemesine hizmet eden, geçici bir araç olmaktan çıkarmakta, daha ziyade "risk"

[400] Özbek/Doğan/Bacaksız, s.223, Yenisey/Nuhoğlu, s. 324.
[401] Caner Yenidünya,"Ceza Muhakemesinde Koruma Tedbirlerine İlişkin Temel Özellikler", 26.06.2019, https://caneryenidunya.medium.com/ceza-muhakemesinde-koruma-tedbirlerine-i%CC%87li%C5%9Fkin-temel-%C3%B6zellikler-f0f35107b92d, Erişim Tarihi: 01.07.2021.
[402] Ünver/Hakeri, s.684.
[403] Wachter/Mittelstadt, s.513

olarak kabul edilen kişilerin diğerlerinden kalıcı olarak ayrıştırılması ve farklı muameleye tabi tutulması sonucunu doğurmaktadır.

d) Kanunla Düzenlenme Zorunluluğu Açısından Değerlendirme

Koruma tedbirleri konut dokunulmazlığı, seyahat özgürlüğü, kişi güvenliği özel hayatın gizliliği de dâhil pek çok hakka müdahale içermektedir. Bu nedenle ilgili tedbirler, Anayasa m. 13'ün temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği ifadesi karşısında PVSK, CMK ve diğer kanunlar çerçevesinde düzenlenmiştir[404]. Koruma tedbirleri, Anayasa m.19 ve devamında düzenlenen temel hakların sınırlandırma sebeplerine bağlı şekilde, belirli ve öngörülebilir şekilde düzenlenmelidir. Nitekim bu nedenle CMK m.161 ve 164'te yer alan soruşturma ve kovuşturmaya dair genel yetkiler, temel hakları korumak açısından yetersiz olup, haklara müdahale içeren tüm tedbirlere ilişkin ayrı ve özel düzenleme yapılması yoluna gidilmiştir[405].

Koruma tedbirlerinin yasayla düzenlenmesi, özgürlükçü hukuk devletinde hak ve özgürlüklere sınırsız şekilde müdahale etmeden maddi gerçeğe ulaşmayı teminat altına almaktadır. Bu nedenle söz konusu tedbirlerin sınırları, idare tarafından düzenleyici işlemlerle değil, halkın temsil organı olan meclis tarafından çizilmektedir. Yönetmelikler, ancak kanuna aykırı olmamak şartıyla uygulamaya yön gösterir ve yetki kanunu olmaksızın yönetmeliklerle koruma tedbirlerinin düzenlenmesi hukuka aykırı olacaktır[406].

Profilleme teknolojilerin özel hayatın gizliliği ve kişisel verilerin korunması haklarına müdahale ettiği açık olmakla birlikte, Türk mevzuatında profilleme sürecini, amaç, yöntem ve denetim bakımından sınırlayan düzenlemelere ceza hukuku ve idare hukuku mevzuatında rastlanmamaktadır. Profilleme düzenlemelerine, daha ziyade karşılaştırmalı hukukta olduğu gibi Kişisel Verilerin Korunması Kanunu'nda yer verilmiştir. Ancak kişisel verilerin korunması kapsamındaki düzenlemeler

---

[404] Öztürk/Eker Kazancı/Soyer Güleç, s.29.
[405] Ünver/Hakeri, s.687.
[406] Yenidünya, "Ceza Muhakemesinde Koruma Tedbirlerine İlişkin Temel Özellikler", https://caneryenidunya.medium.com/ceza-muhakemesinde-koruma-tedbirlerine-i%CC%87li%C5%9Fkin-temel-%C3%B6zellikler-f0f35107b92d.

profillemenin uygulanma usulünü, hangi şüphe derecesinde ve ne kadar süre ile uygulanabileceklerini ve hâkim denetimini öngörmemektedir. Kişisel verilerin korunması mevzuatında, yalnızca ilgili kişi hakkında, hukuki ve benzer ağırlıkta kararlar alındığı takdirde, kişilerin münhasıran otomatik sistemler tarafından değerlendirilmelerine karşı itiraz hakları düzenlenmiştir. Dolayısıyla bu değerlendirmeler, temel hak ve özgürlüklere sınırsız şekilde müdahale ederek gerçekleştirildiği takdirde, bunu engelleyecek sınırlar çizilmemiş, profilleme gerçekleştirildikten sonra insan müdahalesini mümkün kılan bireysel bir itiraz hakkı tanınmıştır. Her ne kadar eşitlik ilkesi ve ayrımcılık yasağı gibi temel ilkeler profilleme teknolojilerinin sınırlarını gösterse de profillemenin din, ırk, mezhep gibi klasik kategorilerin ötesinde, "tehlikeli-tehlike teşkil etmeyen vatandaş" şeklinde yeni kategoriler doğuran sonuçları karşısında, ayrımcılık yasağı normlarına dayanmak güç olmaktadır[407]. Örneğin Amerika Birleşik Devletlerinde görülen 2013 yılında People v. Osman davasında sanık cinsel suçlarda tekerrüre ilişkin risk puanını hesaplayan Static 99 profilleme teknolojisinin daha önce kişinin partneri ile birlikte yaşayıp yaşamadığını dikkate almasına ve yaşamadıysa bu durumu yüksek risk faktörü olarak kabul etmesine itiraz etmiş, bununla birlikte Mahkeme "partner ile birlikte yaşama veya yaşamama" faktörünün ayrımcılık yasağı kapsamında ırk, din, cinsiyet gibi korunan faktörlerden biri olmadığına ve bu nedenle hukuka aykırı kabul edilemeyeceğine karar vermiştir[408]. Dolayısıyla yalnız yaşama gibi veriler bir tercih değil aksine toplumsal anomali olarak değerlendilebilmekte, kişiler bu tür yeni gerekçelerle toplumdan ayrıştırılabilmektedir.

Temel hak ve özgürlüklere geleneksel koruma tedbirlerinden çok daha yoğun müdahale içeren profilleme teknolojileri, sanık haklarını ve anayasal hakları güvence altına alan düzenlemeleri aşındırmaktadır. Bu nedenle bir an önce bu teknolojilere özgü kanuni düzenlemelerin yapılmasına ihtiyaç duyulmaktadır.

---

[407] Matthias Leese, "The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union", **Security Dialogue**, Cilt:45, Sayı:5, 2014, ss. 494–511, s.500, 506.

[408] People v. Osman, Esas: H037818, 2013 (Cal. Ct. App. Apr. 8, 2013), aktaran Melissa Hamilton, "Risk-needs Assessment: Constitutional and Ethical Challenges", **American Criminal Law Review**, Cilt:52, Sayı:2, ss. 231-291, s.245. Bununla birlikte kişi inancı gereği evlilik öncesi birlikte olduğu kişi ile yaşamıyorsa, ilgili yazılım her ne kadar dini görüşü doğrudan bir girdi ele almasa da dolaylı olarak ayrımcılığa yol açmaktadır. Ancak dolaylı ayrımcılık iddiaları genellikle yazılımın görünüşte tarafsız olması ve ayrımcılık içeren faktörleri doğrudan içermemesi nedeniyle reddedilebilmektedir, Hamilton, "Risk-needs Assessment", s.261.

e) Gecikmesinde Tehlike Bulunma Unsuru Bakımından Değerlendirme

Koruma tedbirleri muhakeme işlemlerine devam edilememesi tehlikesi doğduğunda uygulanır. Başka bir değişle, derhal başvurulmadıklarında muhakemenin işleyememesi, delillerin elde edilememesi veya failin kaçması tehlikesi bulunmadığı sürece kişi haklarına müdahale içeren koruma tedbirleri uygulanmayacaktır. İlgili koruma tedbirine başvurulmadığında meydana gelecek tehlikenin muhakemeyi güçleştirmesi, hatta olanaksız kılması gerekir. Bu durumda maddi gerçeğe ulaşılamayacak veya karar yerine getirilemeyecektir[409]. Bu tehlikenin bulunup bulunmadığı genel geçer gerekçelerle değil, her somut olayda olayın şartları değerlendirilerek tespit edilmelidir.

Koruma tedbirlerini düzenleyen maddelerde gecikmede tehlike unsuru açıkça düzenlenmemiş olsa dahi her koruma tedbiri açısından bu unsur mutlaka aranmalıdır. Tedbire zaruret olmaksızın başvurulması hukuka aykırı olacaktır. "Periculum in mora" şeklinde ifade edilen gecikmede tehlikeden bahsedebilmek için bu tehlikenin muhtemel ve soyut bir tehlike olması yeterli değildir. Ceza muhakemesi sırasında derhal koruma tedbirleriyle müdahale edilmezse zararın meydana gelme ihtimali, somut ve fiili unsurlarla belirlenebiliyor olmalıdır[410].

Örneğin tutuklamaya ilişkin 100. maddede suçu işlediği yönünde kuvvetli suç şüphesi bulunan şüpheli veya sanığın, ayrıca kaçacağına, delilleri yok edeceği veya değiştireceğine, tanık, mağdur ve diğer kişiler üzerinde baskı girişimde bulunacağına yönelik kuvvetli şüphe bulunması aranmaktadır. Dolayısıyla kaçma veya delil karartma şüphesinin somut olgularla gerekçelendirilmesi zorunludur. Örneğin, sanığın aile bağlarının kuvvetli olması, güvenceli ve düzenli bir işi olması, hep aynı yerde ikamet etmesi veya hasta olması halinde kaçma şüphesine işaret eden somut olgular bulunmamaktadır[411]. Yine beyanda bulunacak olan tanık, mağdur, bilirkişi gibi kişiler

[409] Öztürk/Eker Kazancı/Soyer Güleç, s.35, Özbek/Doğan/Bacaksız, s. 225, Ünver/Hakeri, s.688.
[410] Yenisey/Nuhoğlu, s.324, 325.
[411] Örneğin AİHM, Mamedova/Rusya kararında daimi adresi, iki küçük çocuğu, istikrarlı bir yaşam stili olan ve babası hasta olan sanığın kaçma riskini gösteren somut olgular bulunmadığını belirtmiştir, bkz. AİHM Mamedova/Rusya, Başvuru no:7064/05, Tarih:01.06.2006, aktaran Nur Centel,"İnsan Hakları

üzerinde baskı girişiminde bulunulduğu dayanaklarıyla gösterilmelidir. Şayet olay aydınlatılmış, tanık ve diğer kişilerin beyanları alınmışsa, artık delil karartma tehlikesine dayanılarak tutuklama tedbirine başvurulamaz[412].

Profilleme teknolojileri, ceza muhakemesinin amacına ulaşabilmesi tehlikeye düşmediğinde de sevk edilmektedir. Bu teknolojiler uzun vadeli bir ceza politikasına hizmet etmekte, tehlikeli kişileri kamu güveliği ve yeniden suç işlenmesini engelleme amacıyla ayırt etmeyi amaçlamaktadır. Bu tür genel amaçlar, risk değerlendirmesi yapan yazılımların sürekli uygulanmasında meşruiyet zemini olarak kullanılmaktadır[413]. Profilleme teknolojilerinin kullanımının acil ve somut bir tehlikeye yanıt verip vermediği değerlendirilmeksizin, soyut bir tehlike üzerinden kişileri sürekli gruplandırması ve puanlaması, ceza muhakemesi kapsamındaki koruma tedbirlerinden farklılık göstermektedir.

Bununla birlikte, kimi zaman bu teknolojilerin, çeşitli koruma tedbirlerine araç olarak kullanılması söz konusudur. Örneğin Amerika Birleşik Devletleri'nde kişilerin kaçma veya duruşmaya katılmama ihtimali, somut olgulara dayalı kuvvetli şüpheden ziyade algoritmaların belirlediği kaçma riski puanlarına dayanmaktadır. Kaçma şüphesini hesaplayan bu algoritmalar, kişinin ailevi durumu, toplumla bağı, iş durumu ve eğitiminin yanı sıra Amerikan vatandaşı olup olmadığı, sabıka kaydı, işlediği suçun ağırlığı, alkol veya uyuşturucu bağımlısı olup olmadığı gibi unsurları dikkate almaktadır[414]. Bunlara örnek olarak Ohio'da kullanılan Pre-trial Risk Assessment Tool ("PAT")[415] ve daha yaygın şekilde kullanılan Factors Rated Federal Pretrial Risk Assessment ("PTRA")[416] verilebilir. Oysa bu faktörler, kişinin kaçmak veya izini kaybettirmek üzere yaptığı planları, örneğin sürekli ikamet değiştirmesi, yıllar sonra ilk kez pasaport ve yurt dışı bileti alması gibi somut olguları göstermemektedir.

Avrupa Mahkemesi Kararları Işığında Tutuklama Hukukuna Eleştirel Yaklaşım", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:17, Sayı:1-2, s.49-93, s.53.

[412] Centel, İnsan Hakları Avrupa Mahkemesi Kararları Işığında Tutuklama Hukukuna Eleştirel Yaklaşım, s.54.

[413] Hamilton, "Risk-needs Assessment", s.244, 245.

[414] Lauryn P. Gouldirn, "Defining Flight Risk", **The University of Chicago Law Review**, Cilt:85, Sayı:3, Mayıs 2018, ss. 677-742, s. 710, 711.

[415] PAT üzerine ayrıntılı değerlendirme için Edward Latessa/Paula Smith/Richard Lemke/Matthew Makarios/Christopher Lowenkamp, **Creation and Validation of the Ohio Risk Assessment System: Final Report,** Temmuz 2009, https://university.pretrial.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=f99d46b1-4a98-23d2-48a8-99cbb94387f1, Erişim Tarihi: 01.07.2021, s.13, 14.

[416] Hamilton, "Risk-needs Assessment", s.287.

Ayrıca diğer koruma tedbirlerine araç olarak kullanılan profilleme teknolojileri, kaçma şüphesi ve failin tehlikeliliğini iç içe geçecek şekilde değerlendirmektedir. Kaçma şüphesi, şüpheli veya sanığın mevcut hareketlerine dayalı şekilde somut olgulara dayandırılmalıdır. Oysa bu tür teknolojiler, ceza muhakemesinin işleyişinden ziyade faillerin duruşmalara katılmadığı ve ceza muhakemesi sürecine dâhil olmadığı ihtimalde "topluma ne denli zarar verebileceğini" hesaplamaktadır[417]. Dolayısıyla profilleme teknolojileri, koruma tedbirleri gibi maddi gerçeğe ulaşmak için zorunluluk bulunması nedeniyle uygulanmamaktadır. Bu durum failin ceza muhakemesi işleyişini somut tehlike altına sokan bir hareketi bulunmaksızın koruma tedbirlerine başvurulması riskini doğurmaktadır.

f) Görünüşte Haklı Olma Unsuru Bakımından Değerlendirme

Koruma tedbirlerinin uygulanabilmesi için ceza muhakemesinin işleyişine yönelik bir tehlike bulunmalıdır. Bununla birlikte, henüz bir hüküm verilmemişken uygulanan koruma tedbirlerinin haklılığı ancak muhakeme sonunda belli olacaktır. Ancak koruma tedbirlerinin, muhtemel olumsuz sonucu engellemek için muhakeme sonucu beklenmeden uygulanmaları gerekir. Bu durumda koruma tedbirlerinin uygulandıkları sırada en azından haklı görünmeleri gerekir. Burada bahsedilen haklılık henüz suç şüphesi yenilmediği için esasa ilişkin bir haklılıktan ziyade görünüşte haklılıktır[418].

Koruma tedbirlerinin görünüşte haklı olması, tedbir uygulandığı anda, tedbirin uygulanma koşullarının mevcut olması anlamına gelir. Yargılamanın sonucunda sanık hakkında beraat kararı verilmesi, sanık aleyhine uygulanmış olan koruma tedbirlerinin haksız olduğunu göstermez. Koruma tedbirlerinin haklı olup olmadığı, ancak, tedbire başvurulduğu andaki koşullara göre değerlendirilmeli, o sırada tedbir için öngörülen şartların karşılanıp karşılanmadığı incelenmelidir[419]. Tedbir uygulandığı sırada, tedbirin engellemek istediği tehlikenin gerçekleşeceğinin muhtemel gözükmesi ve en

[417] Gouldirn, s.717, 721.
[418] Ünver/Hakeri, s.689.
[419] Yenidünya, "Ceza Muhakemesinde Koruma Tedbirlerine İlişkin Temel Özellikler".

azından belirli suç şüphesine işaret eden sebeplerin oluşmuş olması, tedbiri görünüşte haklı kılmaktadır[420].

Yargıtay Ceza Genel Kurulu da görünüşte haklılığı değerlendirirken, koruma tedbirlerinin bir tehlike tedbiri türü olduğunu, dolayısıyla ancak bir hakkın tehlikede olduğunu gösteren olayların bulunması halinde uygulanabileceğini belirtmiştir. Ancak sürecin nihayete ermesi zaman alacağından ve tehlike, gecikmeye müsaade etmediğinden, koruma tedbirlerinde haklı görünüşle yetinilmek zorunda olduğunu belirtmiştir. Bu nedenle koruma tedbirlerinde yanılma her zaman mümkündür ve koruma tedbirlerinin yöneltildiği kişiye yönelik haksızlık ihtimali her zaman bulunmaktadır. Bununla birlikte, en azından görünüşte haklılık şartı gereği, bu tedbirlere müracaat edilebilmesi için ilgili suçun işlendiğini ve tedbire müracaat edilmesinde yarar bulunduğunu gösteren bir şüphe bulunmalıdır. Bu şüphe tedbir türüne göre "makul" veya "kuvvetli" şüphe olabilecektir. Ancak Ceza Genel Kurulu, kişilerin temel hak ve özgürlüklerine müdahale edilmesinin dayanağını oluşturacak bu şüphenin, mutlaka başlangıç şüphesinden yoğun bir şüphe olmasının zorunlu olduğunun altını çizmektedir[421].

Profilleme teknolojileri ceza muhakemesi işleyişine tehlike oluşturacak somut durumlara değil, geleceğe yönelik soyut risklere yoğunlaşmaktadır. Nitekim profilleme teknolojileri suç işlenmesi üzerine gerçeği ortaya çıkarmaya hizmet eden koruma tedbirlerinden farklı olarak, geleceğe yönelik suç işlenmesini engelleme amacı güder. Dolayısıyla bu teknolojiler, toplumda suç işlenme oranını azaltmak ve kişilerin hareketlerini öngörülebilir kılarak toplumu kontrol etmek için kullanılmaktadır. Başka bir deyişle, belirli bir faili tespit edip ona bireyselleştirilmiş bir ceza verilmesi, profillemenin konusunu oluşturmaz. Daha bütüncül bakıldığında, profilleme teknolojileri, şüpheli/sanık hareketlerinin istatistiksel olarak kaydedilmesi ve verilerinin daha keskin ve daha öngörülebilir suçlu profili çıkarılması ile ilgilenirler. Bu durum bireysel cezalandırma ve topluma yeniden kazandırma amacıyla yola çıkan ceza hukuku anlayışından ayrışmakta, suç yoluna girmeden kişileri kontrol etme ve toplumdan ayırmayı hedefleyerek ceza hukukunun uygulama alanını

[420] Yenisey/Nuhoğlu, s.325, 326.
[421] Yargıtay Ceza Genel Kurulu, T. 25.11.2014, E. 2013/9-610, K. 2014/512, aktaran Ünver/Hakeri, s.686.

genişletmektedir[422]. Sonuç olarak profilleme teknolojileri, koruma hukuku tedbirleriyle farklı amaç güttüğünden, bu teknolojileri görünüşte haklı kılan sebepler de farklıdır.

Öncelikle profilleme teknolojileri sevk edilirken muhakemenin işleyişini tehlikeye düşüren bir olay aranmamaktadır. Nitekim ceza muhakemesi işleyişine risk kavramını dâhil eden bu teknolojilere başvurmak için soyut bir tehlikenin var olması yeterli olmaktadır. Bu teknolojilere başvurmak için belirli bir suç şüphesinin oluşması dahi aranmamaktadır. Bunun yanı sıra profilleme teknolojilerinin uygulanış şeklini düzenleyen kanunlar bulunmadığından, bu teknolojilerin sevk edildiği sırada kanunda öngörülen şartları karşılayıp karşılamadıkları tartışmaya açılamamaktadır. Anti sosyal kabul edilen veya topluma tehlike oluşturduğu iddia edilen davranışları engelleme ve kontrol altına almayı sağlamak üzere sevk edilen bu teknolojilerin tek meşruiyet gerekçesi öngörülebilir, güvenli bir toplum yaratmak ve kamu düzeninin sürekliliğini tesis etmektedir. Oysa bu amaçlar oldukça geniş ve belirsiz amaçlar olduğu gibi, bu amaçlara yönelik gerçek bir tehlike olup olmadığının değerlendirilmeden profillemeye başvurulabilmesi kişi hak ve özgürlüklerine sınırsız bir müdahaleye yol açmaktadır. Nitekim görünüşte haklılık unsuru aranmaksızın uygulanan profilleme teknolojilerinin ceza muhakemesinde kullanılması veya vardıkları sonuçlara dayanılarak ceza muhakemesi araçlarının sevk edilmesi, geleneksel koruma tedbirlerini sınırlayan düzenlemeleri anlamsız kılmaktadır.

g) Belirli Düzeyde Suç Şüphesine Dayanma Bakımından Değerlendirme

Koruma tedbirlerine başvurmak için öncelikle bir suç işlendiğine ilişkin şüphe bulunmalıdır. Aksi halde adli koruma tedbirlerine başvurulması, temel hak ve hürriyetlere haksız ve hukuka aykırı müdahale oluşturacaktır[423].

---

[422] Amber Marks/Ben Bowling/Colman Keenan,"Automatic Justice?: Technology, Crime, and Social Control", İçinde: **The Oxford Handbook of Law, Regulation and Technology**, Ed: Roger Brownsword/Eloise Scorford/Karen Yeung, Oxford Univerity Press: Oxford, 2017, ss. 705-730, s.708.
[423]Yenidünya, "Ceza Muhakemesinde Koruma Tedbirlerine İlişkin Temel Özellikler", Ünver/Hakeri s.685, Özbek/Doğan/Bacaksız, s.258.

CMK kapsamında tüm koruma tedbirleri için ortak bir şüphe derecesi öngörülmemiştir. İlgili koruma tedbirinin hak ve özgürlüklere yönelik müdahalesinin yoğunluğuna göre her bir tedbir bakımından ayrıca şüphe derecelerinin düzenlendiği görülmektedir. Örneğin arama ve elkoyma için makul şüphe gerekirken, tutuklama ve adli kontrol için kuvvetli suç şüphesinin varlığı aranır. Bilgisayarda arama ve teknik araçlarla izleme için ise kuvvetli şüphe sebeplerinin oluşmuş olması gereklidir[424].

Şüphe kavramı, delilden faile ulaşmayı sağlayan ve ceza muhakemesinde koruma tedbirleri dâhil pek çok işlemin keyfi şekilde uygulanmasını engelleyen önemli bir kavramdır. Bu nedenle daha detaylı şekilde ele alınmalıdır.

Ceza muhakemesi, iddia makamının ihbar, şikâyet, talep veya diğer yöntemlerle öğrendiği başlangıç şüphesi teşkil eden basit şüphe ile başlar. CMK m.160 gereği "suç işlendiği izlenimi veren bir hali" öğrenen savcı işin aslını soruşturmak zorundadır. Bununla birlikte başlangıç şüphesinin somut olgulara dayanması gerekir. Öncelikle suç teşkil eden bir fiilin gerçekleştiğine dair bir ihtimal bulunmalıdır. Savcı, suç işlendiği izlenimini veren halin gerçekten mevcut olup olmadığını denetleyecek ve buna göre soruşturma sürecini başlatacaktır[425]. Basit şüphenin oluşması için, kesin bir belge veya delil aranmamaktadır. Bununla birlikte yalnızca bir tahmin veya mantığa aykırı iddiaların ileri sürüldüğü durumlarda basit şüphenin oluştuğu ileri sürülemez. Soruşturma başlatabilmek için, başlangıç şüphesi fiili olay ve olgulara dayanmalıdır, aksi halde dedikodu ve söylentiler, keyfi şekilde soruşturma başlatılmasına yol açacaktır[426].

Dolayısıyla soruşturma için, en azından belirti delilleri ile suç işlendiğine dair şüphe desteklenmelidir. Olaylara dayanmayan, tahmin niteliğindeki umma, varsayımlar ve kriminalistik hipotezler basit şüphe teşkil etmez[427]. Nitekim bu hususta 15/08/2017 tarih ve 694 sayılı Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararnamenin 145 inci maddesiyle, CMK'nin

[424]Öztürk/Eker Kazancı/Soyer Güleç, s.30, Özbek/Doğan/Bacaksız, s. 258.
[425] Yenisey/Nuhoğlu, s.327, 328.
[426] Şahin, İlyas, "Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi", **Marmara Üniversitesi Hukuk Faültesi Hukuk Araştırmaları Dergisi**, Cilt:20, Sayı:3, 2014, ss.97-144, s.111, 112.
[427] Yılmaz, Zehra, **Ceza Muhakemesi Hukukunda Şüphe**, Selçuk Üniversitesi Kamu Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, Konya 2019, s.83.

158. maddesinin 6.fıkrasına eklenen yeni fıkra, 01/02/2018 tarihli ve 7078 sayılı Kanunun 140. maddesiyle kanun haline getirilmiş ve buna göre herhangi bir araştırma yapılmasını gerektirmeksizin bir fiilin suç teşkil etmediği açıkça anlaşılıyorsa veya ihbar ve şikâyet, soyut ve genel nitelikte ise soruşturma başlatılmayacaktır. Bu hallerde soruşturma yapılmasına yer olmadığına karar verilmesi gerekir. Bu düzenleme ile ihbar ve şikâyet, doğrudan soruşturma başlatmaya yeterli kabul edilmemiş, soyut ve genel nitelikli bildirimlerin basit şüphe teşkil etmeyeceğinin altı çizilmiştir[428].

Makul şüphe ise Adli ve Önleme Aramaları Yönetmeliği'nin 6. maddesinde tanımlandığı üzere, hayatın olağan akışı dikkate alınarak, somut olaylar karşısında genellikle duyulan şüphedir. Makul şüphe değerlendirilirken, ilgili zaman, yer ve kişinin veya bu kişiyle birlikte bulunan kişilerin davranış ve tutumları dikkate alınacaktır. Yönetmeliğin ilgili maddesi ihbar veya şikâyetin tek başına makul şüphe teşkil etmeyeceğini, bunları destekleyen emarelerin varlığını aramaktadır. Dolayısıyla makul şüphenin bilgi, belge, gözlem ve tecrübe ile desteklenmesi gereklidir. Basit şüphe, belli bir faili işaret etmiyor olabilir. Bununla birlikte makul şüphe için belirli bir failin suç işlemiş olabileceğine dair tarafsız bir kişiyi ikna edebilecek bilgi ve olguların mevcut olması gerekir[429]. Dolayısıyla, makul şüphenin, dışarıdan izleyen kişileri suç işlendiğine ikna edecek objektif bir yapısı bulunmalıdır. Örneğin, hırsızlık suçundan dolayı sabıkalı olmak, arama tedbiri için gerekli makul şüpheyi oluşturmaya yeterli değildir. İlgili kişilerin soruşturma konusu olaya karıştıklarına, evlerinde bu suçun delilerinin bulunduğuna dair somut bir olgu veya olay bulunması gerekir. Bu durumda örneğin bir kimsenin gece çok geç bir saatte, çalınan arabanın yakınında görülmüş olması gerekir[430]. Nitekim Yargıtay 2. Ceza Dairesi, şüphelinin gündüz elinde poşetle yürürken hırsızlık ithamıyla eşyasının arandığı olayda, arama gerekçesi olarak salt şüphelinin geçmiş sabıkalarının gösterilmesinin yetersiz olduğunu ve aramanın makul şüphe oluşmaksızın yapılması nedeniyle hukuka aykırı olduğunu belirtmiştir[431]. AİHM de içtihatlarında makul şüpheyi kolluğun mesleki tecrübesi ve teknik bilgisine dayanan sübjektif bir şüphe olarak değil, tarafsız bir gözlemciyi ilgili kimsenin bir suç işlediği konusunda ikna edecek objektif bir şüphe olarak

[428] Yılmaz, s.64.
[429] Yılmaz, s.91, 92.
[430] Yılmaz, s.94.
[431] Yargıtay 2. CD., E. 2012/29290, K. 2013/27219, T.20/11/2013, https://lib.kazanci.com.tr/, Erişim Tarihi: 01.07.2021.

tanımlamaktadır[432]. Şüphenin makul dereceye ulaşıp ulaşmadığı, elbette somut olayın şartları içerisinde değerlendirilmelidir[433].

Yeterli şüphe ise CMK m. 170 uyarınca soruşturma evresi sonunda toplanan delillerin suçun işlendiği hususunda iddianame düzenlemeye yetecek düzeye ulaşmasıdır. Aksi halde Cumhuriyet savcısı, kamu davasının açılmasına yer olmadığına karar verecektir. Soruşturma sürecinde toplanan deliller şüphelinin yargılanması halinde mahkûm olma ihtimalini, beraat etme ihtimalinden daha kuvvetli kılıyorsa, bu şüphe yeterli şüphe olarak tanımlanmaktadır[434]. Yeterli şüphe için elde edilen delillerin soruşturulan kişinin yüksek ihtimalle suçun faili olduğunu, akla ve mantığa uygun objektif bir şekilde göstermesi aranır. Toplanan delillerin kamu davası açmak üzere iddianame düzenlemek için yeterli olup olmadığını takdiri, yani delilleri değerlendirme yetkisi Cumhuriyet Savcısına aittir[435]. Bununla birlikte şüphelinin suçu işlediğini hiçbir kuşku bulunmaksızın gösterecek derecede araştırma yapılmış olması aranmamaktadır. Nitekim yeterli "şüphe" ifadesi hala olayın maddi içeriğine ilişkin kuşkuyu barındırmakta ve yalnızca mahkûmiyet ihtimalinin daha yüksek olduğunu göstermektedir[436].

Şüphe üzerine yapılan derecelendirmelerde en yüksek noktada kuvvetli şüphe bulunmaktadır. Kuvvetli şüphe, ceza soruşturmasına başlanması için aranan basit şüphe ve kamu davasının açılması için aranan yeterli şüpheye nazaran, suçun işlendiği hususunda "daha yoğun, acil ve zorlayıcı" bir şüphe derecesidir. Kuvvetli şüphede mahkûmiyet kararı verilebilecek kesinlikte bir kanı henüz oluşmasa bile, o ana kadar toplanan delil ve emareler tedbiri haklı kılacak yoğunluğa ulaşmış olmalıdır[437]. Doktrinde bu yoğunluk, şüphenin tamamen yenilip yüzde yüz oranına ulaşıldığı takdirde mahkûmiyet kararı verilmesi, yüzde elli bir mahkûmiyet oranından daha

---

[432]Bkz. AİHM, Fox, Campbell and Hartley/Birleşik Krallık, Başvuru No:12244/86, 12245/86, 12383/86, 30.08.1990, para. 32, Erdagöz/Türkiye, Başvuru No:21890/93, 22.10.1997, para. 51, aktaran Öznur Sevdiren, "Anayasa Mahkemesi'nin Tutuklama Kararının Maddi Şartları İçtihadına Eleştirel Bir Yaklaşım", **Anayasa Hukuku Dergisi**, Cilt:8, Sayı:16, 2019, ss. 295-358, s. 302.

[433] Sevdiren, s.302.

[434] Öztürk/Eker Kazancı/Soyer Güleç, s. 33; Centel/Zafer, s. 103, Özbek/Doğan/Bacaksız, s. 224.

[435] Erkut Güçlü Kahraman, "Yeterli Şüphe Kavramının İddianamenin İadesi Kurumu Bakımından Değerlendirilmesi", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 16, Sayı: 1, 2014, s. 123-150, s.142. Kahraman'a göre savcı şüphelinin fail olması ihtimalinin yüksek olduğunu değil, dava açıldığı takdirde mahkeme önünde suçun kişi tarafından işlendiğini tartışma zeminini mümkün kılacak delillerin toplanıp toplanmadığını değerlendirmelidir.

[436] Yılmaz, s.120.

[437] Şahin, s. 118, 119.

yüksek, ama yüzde yüze varmayan şüphe aralığında ise tutuklama kararı verilebileceği şeklinde ifade edilmektedir. Bununla birlikte tutuklama gibi kişiyi özgürlüğünden mahrum bırakan tedbirlere başvurmak için, şüphelinin o suçu işlediği konusunda yüzde doksan oranında yüksek mahkûmiyet olasılığı bulunması gerektiğinin altı çizilmektedir[438].

Dolayısıyla kuvvetli suç şüphesinden bahsedebilmek için, şüpheli veya sanığın, fail veya suç ortağı olarak bir suçu işlediği konusunda ihtimal yüksek olmalı ve bu ihtimal olgulara dayanmalıdır[439]. Suç şüphesinde olgu, isnadın ciddi olduğunu, objektif olarak kişinin üstüne atılan suçu işlediği hususunda toplanan verilerin dayanakları bulunduğunu ifade eder. Bununla birlikte uygulamada isnadın ciddiyeti, suçun ağır olması ile karıştırılmakta ve bazı davalarda kuvvetli suç şüphesini gösteren olgular bulunmadığı halde, salt dava konusu suç ağır bir suç olduğu için tutuklama tedbiri kararı verilmesi yanılgısına düşülmektedir. Şüphenin delillere dayanması ve koruma tedbirine ilişkin kararın gerekçelendirilmesi zorunludur. Elbette her koruma tedbiri için suçun işlendiğine dair kuvvetli şüphenin yanı sıra farklı koşulların da aranması gerekir. Örneğin tutuklama kararı verilebilmesi için kişinin ilgili suçu işlediğine dair kuvvetli şüphe bulunmasının yanı sıra, tutuklamanın zorunlu olması, sanık tutuklanmadığı takdirde, kaçacağı veya delilleri karartacağı veya kuvvetini azaltacağı hususunda da kuvvetli şüphe olması ve bu sebeplerin tutuklama kararında gerekçeleriyle birlikte gösterilmesi gerekir[440].

CMK sistematiğinde kuvvetli şüpheyi tanımlayan bir madde bulunmamaktadır. Uygulamada, Yargıtay 12. CD. kuvvetli şüpheyi, şüphe terazisinde, "eldeki deliller, bilgi ve bulgular ışığında bir olayın gerçekleştiğine dair kesine yakın bir kanaat oluşması" şeklinde tanımlamaktadır[441]. Bunun yanı sıra tutuklamaya ilişkin CMK m. 100 kapsamında, olgular yerine "somut deliller" ifadesine yer verildiği görülmektedir. Olgu ifadesi, bilimsel, nesnel, herkes tarafından kabul gören bilgileri ifade eder. Bunun

---

[438] Feridun Yenisey, "Anayasa Mahkemesi'ne Bireysel Başvuru Kararlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi: Tutuklama", **Anayasa Yargısı Dergisi**, Cilt: 33, 2016, s.213-229, s. 223.

[439] Centel, "İnsan Hakları Avrupa Mahkemesi Kararları Işığında Tutuklama Hukukuna Eleştirel Yaklaşım", s.51.

[440] Centel, s.410, 411.

[441] Yargıtay 12. CD, E. 2015/12244, K. 2016/10922, T.28.06.2016, aktaran Ayça Lütfiye Akpek, **Tutuklulukta Kuvvetli Suç Şüphesi**, İstanbul Bilgi Üniversitesi, Yüksek Lisans Tezi, İstanbul 2020, s. 101.

yanı sıra olgu kavramı, kimi olayların dayandığı neden ve sonuçları içerecek şekilde vakıa kavramının karşılığı olarak da kullanılmaktadır. Oysa bir olayın nedeni, sonucu veya cereyanı tek başına koruma tedbirlerinin uygulanması için dayanak oluşturmamalıdır. Nitekim deliller, "bir olayın kanunda olaya ilişkin gösterilen duruma uyup uymadığını" gösteren ispat araçlardır[442]. Bir olayın veya sonucun gerçekleştiğini değil, iddia edilen koşullara ve kanunda belirtilen duruma uygun şekilde gerçekleşip gerçekleşmediğini gösterir. Dolayısıyla kanunda delil kavramına yer verilerek kuvvetli suç şüphesinin oluşması için maddi vakıanın incelenmesinin yanı sıra somut delillere ulaşılması aranmaktadır. Bu şekilde, kuvvetli suç şüphesi için ikrar, tanık beyanı, yazılı belgeler ile görüntü veya ses kaydeden araçlarla yapılmış kayıtlar şeklinde cereyan eden delillerin aranmasının zorunlu tutulması yerinde olmuştur[443].

Son olarak CMK kapsamında taşınmaz, hak ve alacaklara el koyma, bilgisayar, bilgisayar kütükleri ve programlarında arama ve el koyma, iletişimin denetlenmesi, gizli soruşturmacı görevlendirilmesi, teknik araçlarla izleme gibi koruma tedbirlerinde, kuvvetli şüphe kavramından farklı olarak "kuvvetli şüphe sebepleri ifadesine yer verilmiştir. 6526 sayılı yasa ile öngörülen değişikliklerle "suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması" unsuru pek çok koruma tedbiri açısından aranmaya başlanmıştır. Doktrinde bir görüş, bu ifadeyi somut delillere dayalı kuvvetli şüphe şeklinde değerlendirmenin, başka yolla delil elde etme olanağının bulunmaması koşulu ile çelişeceğini belirtmektedir. Bu görüşe göre, kuvvetli şüphe oluşturacak yoğunlukta somut deliller mevcutsa, son çare olarak bu tedbirlere başvurulmasını gerektiren başka suretle delil elde edilmesi imkânı bulunmaması koşulu anlamını yitirmektedir. Nitekim kuvvetli şüpheye dayanak oluşturacak deliller elde edildiğine göre, başka delil elde edilmesi için son çare olarak ilgili koruma tedbirlerine başvurmak gerekli ve zorunlu olmayacaktır. Bu nedenle somut delillere dayalı kuvvetli şüphe sebepleri ifadesinin, kanun sistematiğinde kuvvetli suç şüphesi ile aynı yoğunlukta bir şüpheyi işaret etmediği, daha ziyade tedbirlere keyfi ve sıklıkla başvurulmasını engellemek, uygulamaya yol göstermek amacıyla bu terime

[442] Akpek, s. 104.
[443] Akpek, s.104, 105.

başvurulduğu belirtilmektedir. Ancak bu durum, kavramların benzerliği nedeniyle zaman içerisinde "kuvvetli şüphe" ifadesini de aşındırma riski taşımaktadır[444].

Bu çelişkiyi aşmak adına doktrinde, hem kuvvetli şüphe sebeplerinin hem de başka türlü delil elde etme imkânı olmamasının birlikte arandığı tedbirlerde, o ana kadar elde edilen delillerin suçun aydınlatılması için yeterli olmasa da sanığın mahkûmiyet oranının yüksekliğine işaret eden deliller olarak algılanması gerektiği belirtilmektedir. Bir diğer görüş ise kuvvetli şüphe sebepleri ifadesini başlangıç şüphesinden daha yoğun ancak henüz yeterli veya kuvvetli suç şüphesi derecesine ulaşmamış şüphe derecesi olarak kategorize etmektedir[445]. Bu durumda, CMK m. 100 kapsamında aranan kuvvetli şüphe ile CMK m. 135 kapsamında aranan kuvvetli şüphe sebepleri aynı yoğunlukta değildir[446]. Bunlardan ilki, daha yoğun bir şüphe derecesini ifade etmektedir. Bu ifadenin CMK sistematiğindeki basit, makul, yeterli, kuvvetli suç şüphesi derecelendirmesine uymadığı ve yorumlanmasında tereddütlere yol açtığı belirtilerek yasal bir tanımlama yapılmasının gerekliliğinin de altı çizilmektedir[447]. İlgili tedbirleri, kuvvetli şüphe oluşmakla birlikte hala şüphenin tamamen ortadan kaldırılamadığı durumlarda başkaca yol bulunmaması halinde başvurulması gereken ikincil nitelikte tedbirler olarak okumak mümkündür. Dolayısıyla söz konusu iki şart birbiriyle çelişmeksizin de uygulanabilir[448]. Böylelikle, kuvvetli şüphenin oluştuğu, ancak daha fazla gelişmenin kaydedilemediği durumlarda söz konusu tedbirler son çare olarak uygulanabilir hale gelecek[449], "kuvvetli şüphe" ile "kuvvetli şüphe sebepleri" ifadelerini farklı şüphe dereceleri olarak değerlendirmenin yaratacağı kavram karışıklığının da önüne geçilmiş olacaktır.

Şüphe dereceleri tartışılırken görüldüğü üzere koruma tedbirleri için en azından makul şüphenin varlığı aranmakta, basit şüphe hak ve özgürlükleri henüz hüküm verilmeden kısıtlayan koruma tedbirlerini uygulamak için yeterli olmamaktadır.

---

[444] Öztürk/Tezcan/Erdem/Gezer/Kırıt/Alan Akcan/Özaydın/Tütüncü/Altınok Villemin/Tok, s. 556, 557.
[445] Özbek/Doğan/Bacaksız, s.225.
[446] Yılmaz, s.158, Yasin Sezer/Ali İhsan İpek/Engin Parlak, **Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme**, Seçkin Yayınevi: Ankara, Eylül 2012, s.109.
[447] Özbek/Doğan/Bacaksız, s.363.
[448] Şahin/Göktürk de kuvvetli suç şüphesi ile kuvvetli şüphe sebepleri arasında herhangi bir fark gözetmemekte ve kuvvetli şüphe sebepleri ile başka türlü delil elde edilememesi şartlarını kümülatif şekilde aramaktadır, bkz. Şahin, Cumhur/ Göktürk, Neslihan, Ceza Muhakemesi Hukuku I, Seçkin Yayıncılık: Ankara, Eylül 2021, s.353, 354.
[449] Yılmaz, s.159

Profilleme teknolojileri, ceza muhakemesinin işleyişinde anahtar olan şüphe kavramını dönüşüme uğratmaktadır. Şüphe, kişilerin hareketlerine dayanır ve objektif bir gözlemciyi ikna edebilmeyi esas alır. Belirli bir zaman diliminde, belirli bir kişinin hareketlerini değerlendirmeyi gerektirir. Dolayısıyla suç şüphesinin belirli ve objektif olgulara dayalı olması gerekir. Bu olgular, failden değil suç teşkil ettiği iddia edilen fiilden yola çıkar. Yine söz konusu olgu ve delillerin, ilgili tedbir uygulanmadan önce elde edilmesi gerekir. Dolayısıyla, şüpheli olduğu iddia edilen kişinin fiilleri, olayın bütünlüğü içerisinde tüm şartlar gözetilerek değerlendirilir. Söz konusu kişinin hareketlerinin, gözlemlenerek diğer kişilerden ayrılması ve neden suç teşkil ettiğinin somut bir şekilde açıklanması gerekir. Her ne kadar kişisel nitelikler, olayın tüm şartlarının değerlendirilmesinde esas alınsa da bunlar fiille ilişkilendirilebildiği takdirde şüphenin oluşmasına zemin teşkil edebilir[450]. Bununla birlikte şüphe derecelerinde aranan temel unsurlar, herkese karşı eşit mesafede duran hukuk devletinde, bilinmeyen bir kişinin gerçekleştirdiği hukuka aykırı hareketleri nedeniyle ceza muhakemesinin konusu haline gelmesi üzerinden kurgulanmıştır. Kişinin daha önce gerçekleştirdiği ve suç ile ilişkisi bulunmayan tüm eylem ve tercihlerinin bilinir kılınması, geleneksel ceza muhakemesi açısından yeni bir olgudur. Artık veri tabanları üzerinden eşleştirme yapan teknolojiler, bilinmeyen bir kişi üzerinde yoğunlaşan şüpheyi aramaktan ziyade, herkesi bilinir kılmakta ve suç yoluna girmemiş kişilerin üzerine adeta sorgu ışığı tutmaktadır[451]. Özel şirketler, bankalar, internet servis sağlayıcıları ve diğer kurumlar, kolluğun yerini almaya başlamış, topladıkları bilgileri analiz ederek kolluk kuvvetlerinin erişimine açmıştır. Profilleme teknolojileri bu verileri analiz ederek kişileri sicilleri, ilişki ağları, satın aldıkları ürünler ve daha pek çok veri ile tamamen şeffaf hale getirmektedir. Kişisel özelliklerin, karakterin, sınıfsal ve azınlık gruplara aidiyetin ön plana çıktığı bu süreçte, artık objektif gözlemlere dayalı şüphe kavramı ortadan kaybolmaya yüz tutmuş durumdadır[452].

Örneğin bir kişinin gece saati, birden fazla kişiden kapalı ufak torbalar karşılığı para alması, objektif bir gözlemciyi uyuşturucu ticareti yapıldığına ikna edebilecektir. Dolayısıyla makul şüphenin oluştuğundan bahsedilebilecektir. Oysa aynı örnekte,

---

[450] Andrew Gutherie Ferguson, "Big Data and Predictive Reasonable Suspicion", **University of Pennsylvania Law Review**, Cilt:163, Sayı:2, 2015, ss.327-410, s.339, 440.
[451] Ferguson, "Big Data and Predictive Reasonable Suspicion", s.329.
[452] Ibid, s.330

profilleme teknolojileri ile metamfetamin imalatında kullanılma ihtimali olan tolüenin, iyotlu kırmızı fosfor, amonyak, hidroklorik asit gibi maddeleri[453] satın aldığı tespit edilen ve geçmişte uyuşturucu ticareti suçundan hükümlü olduğu bilinen kişinin henüz suç teşkil eden hareketi olmamasına rağmen polis tarafından aranması mümkün olabilmektedir. Bu durum ceza muhakemesinde failden yola çıkan tamamen yeni bir şüphe algısıdır.

Dolayısıyla profilleme teknolojileri, kişilerin verilerini analiz etmek üzere sevk edilmeden önce, koruma tedbirlerinde olduğu gibi herhangi bir suç şüphesinin oluşması aranmamaktadır. Kişilerin verilerine ve özel hayatın gizliliğine yoğun müdahale içeren profilleme teknolojileri, koruma tedbirlerinden farklı olarak basit şüphe dahi aranmaksızın sevk edilmektedir. Bu nedenle henüz bu teknolojiler kullanılmaya başlanılmadan, mutlaka bireyselleştirilmiş makul ve hatta kuvvetli şüphe oluşmasını arayan düzenlemelerin yapılması gerekmektedir.

Diğer bir soru ise profilleme teknolojileri eliyle varılan sonucun, fail hakkında şüphe derecesini tespit ederken kullanılıp kullanılamayacağıdır. Bu soru aynı zamanda, objektif şüphe tespitinde sübjektif faktörlerin dikkate alınıp alınamayacağına ilişkin bir soru olup, detaylı şekilde ele alınmalıdır.

Kural olarak makul şüphe veya kuvvetli şüphenin oluştuğunu kabul edebilmek için örneğin olayın gerçekleştiği mahalleye dair genel geçer veriler veya kolluğun içgüdüsü ve meslek tecrübesi yeterli olmayacaktır. Tüm şüphe dereceleri, üçüncü kişiyi ikna edecek somut olgulardan yola çıkmaktadır ve koruma tedbirlerinin uygulanması için bu olguların gerekçelendirilmesi gerekir. Oysa suç mahallerini tespit etmede kullanılan algoritmaların kırmızı alarm bölgesi olarak kabul ettiği bölgeden geçmekte olan herkesin potansiyel şüpheli olarak kabul edilmesi, makul şüphe kavramının çiğnenmesi anlamına gelecektir. Makul şüphe ve kuvvetli şüphe için

[453] Örnekteki uyuşturucu imalatına konu olan maddeleri açıklayan makale için bkz. Emre Mutlu/ Mustafa Okudan/Faruk Aşıcıoğlu, "Uyuşturucu Madde İmalatında Kullanılan Öncül Maddeler: On Yıllık Tek Merkez Verileri", **Türkiye Klinikleri Adli Tıp ve Adli Bilimler Dergisi**, Cilt:17, Sayı:1, 2020, ss.25-34, s.26.

mutlaka belirli bir kişiye hareketleri nedeniyle atfedilen, somutlaşmış ve bireyselleştirilmiş bir şüphenin varlığı gereklidir[454].

Bu konuda örnek teşkil eden United States v. Cortez kararında üst araması için makul şüphenin oluşup oluşmadığının tespitinde olayın tüm şartlarının göz önüne alınmasının gerektiği ve bu şartların durdurulan kişinin hukuka aykırı bir hareket gerçekleştirdiğine işaret etmesi gerektiği belirtilmektedir. Yine United States v. Momodu kararında günün saati, mahallede suç işlenme oranının çokluğu gibi faktörlerin koruma tedbirinin uygulanmasında dikkate alınabileceği ancak bu bilgilerin şüphelinin hareketlerinden ziyade içinde bulunduğu ortama işaret ettiği ve bu nedenle mutlaka şüphelinin suç teşkil eden hareketinin tespiti ve gerekçelendirilmesi gerektiğinin altı çizilmektedir. Son olarak United States v. Skolow kararında uyuşturucu ticaretinde fail profili çıkartılması üzerinde durulmuştur. Bu tür suçlarda faillerin sıklıkla seyahat etmesi, günün belli saatleri satış yapmaları, belli tarzda giyinmeleri gibi daha önceki davalardan yola çıkarak yapılan profillemeler üzerine, sırf bu profile uyması nedeniyle kişinin şüpheli kabul edilemeyeceği belirtilmiştir. Nitekim bu durum yalnızca önceki dava verilerinin profillenmesinden yola çıkan, ancak mevcut davadaki şüphelinin hareketlerine değil karakterine işaret eden bir müdahale içermektedir[455]. Oysa ceza muhakemesinde koruma tedbirleri gözleme dayalı, ampirik kanıtlardan yola çıkmalıdır.

Dolayısıyla bir kişinin karakterine dayalı risk puanı, yargılamaya konu fiille ilişkilendirilmediği sürece kişi hakkında tedbir alınmasına yol açmamalıdır. Profilleme teknolojilerinin dayandığı verilerin objektif ve bilimsel olduğu iddiası, ceza muhakemesinde şüphe olgusunu karşılamaya yeterli bir iddia olmadığı gibi farklı kanallardan toplanan bu verilerin doğru, güncel, güvenilir ve tarafsız olduğunu ileri sürmek mümkün değildir. Her ne kadar bu teknolojiler, ticari, idari ve diğer amaçlarla kişilerin hangi hizmeti almayı tercih ettiği, seyahat etmeyi sevdiği ülkeleri, politik ve dini görüşlerini, boş zamanlarını ne şekilde değerlendirdiklerini[456], şiddete meyilli

---

[454] Margaret Raymond, "Down on the Corner, Out in the Street: Considering the Character of the Neighborhood in Evaluating Reasonable Suspicion", **Ohio State Law Journal**, Cilt:60, Sayı:1, 1999, ss.99-141, s.105.

[455] İlgili davalar sırasıyla United States v. Cortez, 449 U.S. 411, 418 (1981), United States v. Momodu, 909 F. Supp. 1571, 1575 (N.D. Ga. 1995) United States v. Sokolow, 490 U.S. 1 (1989), rev'g 831 F.2d 1413 (9th Cir. 1987), aktaran Raymond, s. 107, 108, dipnot 38, 39.

[456] Christopher Slobogin, "Transaction Surveillance by the Government", **Mississippi Law Journal**, Cilt:75, 2005, ss.139-191, s. 145.

olup olmadıklarını, suç örgütleri ile iletişim kurup kurmadıklarını gösterme iddiasında olsa da bu iddialar, kişinin mevcut suçu gerçekleştirdiğini kanıtlamadığı sürece değerlendirme dışı bırakılmalıdır. Profilleme teknolojileri ile tespit edilen, ancak suçun konusu fiille ilişkisi bulunmayan bilgiler, şüphe tespitinde dikkate alınmamalıdır[457]. Nitekim ceza muhakemesinde önemli olan şüpheli ile suç teşkil eden hareket arasındaki bağın kurulmasıdır. Bu amaca hizmet etmeyen veriler, belli grupların hedef alınarak, olasılıklar üzerinden çeşitli suçlarla ilişkilendirildiği[458] ve ceza hukukunun ön yargılara dayalı bir silah olarak doğrultulduğu bir düzenin doğmasına yol açacaktır. Dolayısıyla profilleme teknolojilerine başvurabilmek için belirli şüphe derecelerinin öngörülmesi ve bu teknolojilerinin kullanımı sonucu varılan sonuçların fiil ile ilişki olmadığı takdirde şüphe tespitinde değerlendirilmemesi gerekir.

h) Ölçülü Olma Unsuru Açısından Değerlendirme

Kamu otoritelerince alınan bir tedbirin veya sınırlandırmanın ölçülülüğü değerlendirilirken, öncelikle alınan tedbirle ulaşılmak istenen meşru amaç tespit edilmelidir. Anayasa'da temel hak ve özgürlüklerin hangi amaçlarla sınırlandırılmasının meşru kabul edileceği belirtilmektedir. Ölçülülük ilkesi, alınan tedbirin belirtilen bu amaca ulaşmak için elverişli ve gerekli olmasını ve gerekli olsa dahi bireylerin haklarına orantısız bir şekilde müdahale içermemesini gerektirir. Dolayısıyla ölçülülük ilkesine uygunluk denetlenirken, uygulanan tedbirin elverişliliği, gerekliliği ve orantılılığı incelenir[459].

Eğer alınan tedbir, meşru amaca ulaşmayı kolaylaştırıyorsa araç elverişli, amaca erişime hiçbir etki göstermiyorsa araç elverişsizdir. Bireyleri keyfi ve gereksiz kamu gücünden korumak amacıyla, meşru bir amaca ulaşmada elverişli olmayan araçların kullanımına izin verilmemelidir. Bununla birlikte, elverişlilik ilkesi, her durumda en uygun aracın kullanmasını zorunlu kılmamaktadır. Dolayısıyla, varılmak istenen amacın kısmen gerçekleşmesini sağlayabilen araçlar dahi elverişli kabul

[457] Ferguson, "Big Data and Predictive Reasonable Suspicion", s. 388.
[458] Ibid, s.403.
[459] Yüksel Metin, "Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:1, 2017, ss.1-74, s.7.

edilebilecektir. Bu nedenle yargı kararlarında bir tedbirin elverişli olmaması nedeniyle ihlal kararı verilmesine nadiren rastlanmaktadır[460]. Gereklilik ilkesi ise meşru bir amaca ulaşmada aynı veya birbirine yakın birden fazla elverişli araç bulunduğu takdirde, bunlardan hak ve özgürlükleri daha az sınırlayıcı olan aracın seçilmesini ifade eder. Dolayısıyla gereklilik ilkesi elverişli araçları sınırlandırmakta, bunlar arasından en uygun ve hakları en az ihlal edenin seçilmesini zorunlu kılmaktadır. Son olarak orantılılık ilkesi kullanılan araç ile ulaşılmak istenen araç arasında bir orantı bulunmasını gerektirir. Başka bir deyişle, alınan tedbir ilgili kişilere ölçüsüz ve katlanılmaz yükümlülükler getiriyor, müdahale edilen hak ile korunmak istenen hukuksal değer arasında makul olmayan bir dengesizlik oluşuyorsa, bu durumda orantılılık ilkesi ihlal edilmiş olacaktır[461].

Hukuk devletinde bir tedbirin toplum geneli için sağlayacağı faydaya, bireylere ağır bedeller ödetilerek erişilemez. Özellikle kamu otoritesinin bireylere karşı çok daha güçlü konumda olduğu ceza hukuku bakımından ölçülülük ilkesinin önemi daha da büyüktür. Bu bağlamda koruma tedbirleri ile temel hak ve hürriyetlere, ancak Anayasa m.13'ün de açıkça ifade ettiği şekilde, bu hakların özlerine dokunulmaksızın, Anayasa'da gösterilen meşru amaçlar doğrultusunda, Anayasanın sözü ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine riayet eder şekilde müdahale edilebilir. Dolayısıyla ceza muhakemesinde koruma tedbirleri de önceden tanımlanmış bir amaç doğrultusunda, bu amaca hizmet edecek ve haklara en az müdahale içerecek şekilde uygulanmalıdır. Ölçülülüğün tesisi için kimi maddelerde açık düzenlemeler yer almaktadır. Örneğin CMK m.135'te iletişimin denetlenmesinin, başka türlü delil elde etme imkânı bulunmadığı takdirde uygulanacağı öngörülmüştür. Dolayısıyla bu tedbire karar verilmeden önce, amaca daha az müdahale içeren bir tedbirle ulaşma ihtimali araştırılmak zorundadır[462]. CMK md 100/4'te tutuklama kararı verilemeyecek suçlar belirtilmiş, üst sınırı iki yılı aşmayan suçlar açısından kişileri hürriyetlerinden yoksun kılan tutuklama tedbirinin orantısız olacağı açıkça gösterilmiştir. Kimi zaman mağdurun kırılganlığı da gözetilerek koruma tedbirlerinin sınırlandırıldığı görülmektedir. Bu bağlamda Çocuk Koruma Kanunu'na göre, onbeş yaşını doldurmamış çocuklar hakkında, tutuklama kararı ancak üst sınırı beş yılı aşan

[460] Yüksel, s.8, 9.
[461] Yüksel, s.11, 13.
[462] Recep Kahraman, "Koruma Tedbirlerinde Orantılılık İlkesi", **İstanbul Hukuk Mecmuası**, Cilt:79, Sayı: 1, 2021, ss. 273-299, s. 286.

hapis cezasını gerektiren suçlar söz konusu olduğunda verilebilecektir[463]. Yine bazı koruma tedbirlerinde tedbirin uygulanacağı azami süre, tedbirin ölçülülük ilkesini tesis etme bakımından önemlidir[464]. Böylelikle hak ve hürriyetin belirsiz bir süreyle sınırlandırılmasının önüne geçilmiştir. Bununla birlikte kanunda herhangi bir süre öngörülmese dahi, tedbir amacına ulaştığı anda, tedbirin geçici ve orantılı olma unsurları gereği sonlandırılması gerekir.

Profilleme teknolojileri, ceza muhakemesi sürecinde kullanılırken ilk akla gelmesi gereken soru bu teknolojilerin ceza muhakemesinin meşru amaçlarına hizmet edip etmediğidir. Yukarıdaki bölümlerde de tartışıldığı üzere, ilgili teknolojiler, failin tehlikeliliği kavramını ceza muhakemesinde yeniden gündeme getirmekte, suçu tespitten ziyade riskli bireyleri toplumdan ayrıştırma amacını muhakeme sürecine dâhil etmeye çalışmaktadır. Bu amacın özellikle insan haklarına saygılı, masumiyet karinesine dayanan ve adil yargılanmayı temel ilke edinmiş ceza muhakemesinin işleyişi ile ne denli uyumlu olduğu tartışmaya açılmalıdır. Bu amacın meşru olduğu kabul edildiği takdirde dahi, profilleme teknolojilerinin kullanımının elverişliliği, gerekliliği ve orantılılığı dikkatle ele alınmalıdır. Profilleme teknolojileri kuşkusuz ki kişilerin özel hayatı ve kişisel verilerin korunması haklarına yoğun bir müdahale içermektedir. Bu müdahalenin gelecekte işlenecek suçları önleme iddiasına dair bilimsel kanıt sunmak oldukça güçtür. Nitekim belirli kişilerin serbest kalmaları halinde gelecekte suç işleyeceklerine dair varılan sonuç, bu kişiler hakkında yakalama/gözaltı/tutuklama tedbirlerine başvurulduğu takdirde test edilemeyecektir. Elbette kişiler hapsedildiklerinde suç işleyemezler[465], ancak bu durum algoritmaların doğru tahminlerde bulunduğunu kanıtlamamaktadır. Eğer bu kişiler serbest bırakılır ve gerçekten suç işlerlerse, bu durumda "suç işlemeyi engelleme" amacına ulaşmak isteyen profilleme teknolojileri başarısız olmuş olacaktır. Kaldı ki suç işledikleri takdirde, suçun işlenme sebebinin algoritmaların öngördüğü aile yapısı, eğitim seviyesi, iş durumu, sosyal hayattaki tercihleri gibi faktörlerle bağlantılı olup olmadıkları da ayrıca kanıtlanmaya muhtaçtır. Kişilerin suç işleme motivasyonları, beklenmedik olaylar ve koşullarla şekillenebilmekte, oysa profilleme teknolojileri kişilerin hayatlarını bağlamı içerisinde değerlendirmekten yoksun, dondurulmuş

[463] Ünver/Hakeri, s.692, Kahraman, s.286, Öztürk/Eker Kazancı/Soyer Güleç, s.37.
[464] Kahraman, s.286.
[465] O'Neil, s.99, 100.

verilere dayanmaktadır. Dolayısıyla her hâlükârda profilleme teknolojilerinin elverişliliğini ve suç oranını azalttığını ileri sürmek, bilimsel bir görüşten ziyade kendi kendini doğrulayan bir totolojiden öteye geçmemektedir. Bunun yanı sıra, kişilerin ileride tekrar suç işleyeceğinin bilinebileceğini iddia etmek, aynı zamanda insan iradesini yok saymak anlamına gelmektedir. Bu iddia, kusurlu irade üzerine inşa edilmiş geleneksel ceza hukukunun temellerini tamamen sarsıcı bir etkiye sahiptir.

Ölçülülük ilkesini karşılamak için bir tedbir, elverişli olmasının yanı sıra demokratik bir toplumda gerekli olmalıdır. Burada gereklilik ilkesine yalnızca pragmatik şekilde yaklaşılmamalıdır. Ceza muhakemesi sürecinde profilleme teknolojileri ile özel hayatın gizliliğine müdahale etmeyi gerektiren acil bir ihtiyacın olup olmadığını araştırılmalı, bu ihtiyaç var ise farklı araçlarla bu ihtiyaca cevap verilip verilemeyeceği sorgulanmalıdır. Profilleme teknolojileri, ceza muhakemesinde fiil ile fail arasında bağ kurmaya elverişli verilerin çok ötesinde, sınırsız verinin toplanıp analiz edilmesinde kullanılmaktadır. Yeniden suç işlemeye dair tespit amacıyla sevk edilseler dahi, şüpheli olan olmayan ayrımı yapılmaksızın milyonlarca kişinin verilerinin toplanması kuşkusuz ki demokratik bir toplumda gerekli değildir[466]. Bu bağlamda Avrupa Birliği özelinde, 2016/687 sayılı Kolluk Direktifinin de dikkate alınması gerekmektedir. Direktifin 27. maddesi bu tür teknolojilerin uygulamaya konulmadan önce kişilerin hak ve özgürlüklerine yönelik doğuracakları etkilerin risk analizinin yapılmasını gerektirmektedir. Bu teknolojilerin sevk edilme amacına hakları en az ihlal edecek şekilde ulaşmaya yardımcı olup olmadıklarının değerlendirilmesi gerekmektedir. Dolayısıyla kişisel verilerin korunmasına ilişkin düzenlemeler de bu teknolojilerin demokratik bir toplumda kullanılmasının gerekliliğini değerlendirirken dikkate alınmalıdır. Bu değerlendirmede kişisel verileri daha az ihlal edecek bir aracın kullanılma ihtimali ve işlenen verilerin niteliği, örneğin ayrımcılığa neden olabilecek özel nitelikli verilerin işlenip işlenmediği önem taşımaktadır. Özellikle hak ve özgürlüklere yönelik risk taşıyan teknolojik uygulamalar açısından AB bünyesinde 2016/680 sayılı Direktif'in 28. maddesi ile bu teknolojiler kullanılmadan önce Kişisel Verilerin Korunması Kurullarına danışılması gerektiğ öngörülmüştür[467].

[466] Chelioudakis, s.90.
[467] Chelioudakis, s.95.

Bunun yanı sıra tedbirlerin varmak istedikleri amaç ile müdahale ettiği haklar arasında bir oran bulunmalıdır. Profilleme teknolojileri, özel hayatın gizliliğinin yanı sıra diğer hak ve özgürlüklere de ciddi müdahalelerde bulunmaktadır. Örneğin profilleme teknolojilerine konu olduğunu ve "suç işleme risk listesi", "terörist listeleri" ve daha çok pek çok listeye dâhil edilme ihtimalini düşünen kişilerin fikirlerini özgürce ifade etmesi, diledikleri yayınları okuması, araştırması veya toplanma ve örgütlenme özgürlüklerini korkmadan kullanmaları mümkün olmamaktadır. Bu durum kişilerin dini görüşlerini topluluk içerisinde ifade etmelerini ve kolektif boyutu olan diğer haklarını kullanmaktan cayarak otosansür uygulamalarına yol açmaktadır[468]. Son olarak profilleme teknolojilerinin adil yargılanma hakkına müdahale içerdiğinin altı çizilmelidir. Adil yargılanma hakkı şüpheli veya sanığın ne ile suçlandığını bilmesini, hakkında toplanan delillere erişebilmesini, bunları tartışmaya açabilmesini ve böylelikle savunmasını inşa edebilmesini sağlar. Oysa profilleme teknolojileri ile belirlenen risk puanlarının, özellikle yapay nöron ağlar veya kendine kendine öğrenebilen makine öğrenmesi söz konusu olduğunda, hangi verilere dayandığı ve veriler arası ne tür bir ilişki kurularak bu sonuca varıldığı şeffaf bir şekilde açıklanamamaktadır[469]. Bunun yanı sıra yargılama sırasında tanık-sanık arası yüzleştirme mekanizmaları ve çelişkileri giderme yöntemleri, profilleme teknolojileri açısından mümkün değildir. Bu teknolojilerin dayandığı veriler pek çok farklı veri sorumlusu tarafından işlenilmekte ve sürecin başında toplanan hatalı veya güncel olmayan bir verinin yarattığı aleyhe sonuçlar, süreç sonuna doğru katlanarak artabilmektedir. Dolayısıyla şüpheli veya sanıkların haklarındaki verilere erişimi verileri düzeltmesi veya itiraz etmesi tüm süreç sırasında mümkün olamamaktadır. Ceza muhakemesine gelindiğinde ise artık kişi hakkında puanlama çoktan verilmiş ve sonuçlara dayanılarak kişi haklarına müdahale gerçekleşmiş durumdadır[470].

Bu nedenlerle, kamu düzenini tesis etme iddiası ile pek çok farklı hakka yoğum müdahale içeren profilleme teknolojilerinin, ceza muhakemesinin insan haklarına saygılı şekilde maddi gerçeği ortaya çıkarma amacına ulaşmada elverişli, gerekli ve ölçülü olduğunu söylemek, mümkün olmamaktadır.

---

[468] Bu şekilde başka kişilerin hareketleriyle bağlantılandırılarak suçlu bulunmanın ifade özgürlüğü, din ve vicdan hürriyeti ve örgütlenme özgürlüğün etkileri için bkz. Linda E. Fisher, "Guilt By Expressive Association: Political Profiling, Surveillance and the Privacy of Groups", **Arizona Law Review**, Cilt:46, Sayı:4, 2004, ss.621-676, s.647 vd.

[469] Wisser, s.1822.

[470] Wisser, s. 1823. Amber/Bowling/Keenan, s.716.

Ceza adaleti kapsamında risk analizinde kullanılan profilleme teknolojileri, amaçları ve uygulanma usulleri bakımından ceza muhakemesi kapsamında koruma tedbirlerinden ayrılmaktadır. Profilleme teknolojileri ceza muhakemesinde delil elde etme ve maddi gerçeğe hizmet etme amacı gütmedikleri gibi, koruma tedbirlerinin araç olma, geçici olma, kanunla düzenlenme, belirli suç şüphesine dayanma, ölçülü olma özelliklerini de barındırmamaktadır. Buna rağmen bu teknolojiler, başta Amerika Birleşik Devletleri'nde olmak üzere, İngiltere, Almanya, İsviçre, İtalya gibi Avrupa ülkelerinde kişi hakkında kaçma riskini veya yeniden suç işleme riskini belirleyerek ceza muhakemesinde kullanılabilmektedir. Bu teknolojilerin, ceza hukukunda fiilden yol çıkan ve kusur ilkesine dayanan ceza sistemi ile örtüşmediği, daha ziyade suçun işlenmesini önleme ve bu bağlamda failin tehlikeliliğinin tespit için sevk edildikleri görülmektedir. Bu uygulamaların, koruma tedbirlerinden ziyade pozitivist ekolün ceza muhakemesine yansıması olan güvenlik tedbirlerine daha yakın olduklarını söylemek mümkündür. Bu nedenle, bir sonraki başlıkta profilleme teknolojilerinin güvenlik tedbirleri ile benzerlik ve farklarını tespit edilecektir.

B. Bir Yaptırım Türü Olarak Güvenlik Tedbirleri Kapsamında Profilleme Teknolojileri

1. Güvenlik Tedbirlerinin Genel Özellikleri

Ceza hukuku, suç ile bozulan düzeni yeniden tesis etme ve aynı zamanda suç işlemekten caydırma amacı taşır. Dolayısıyla suç teşkil eden fiile karşı kefaret ve ödetme kadar suç teşkil eden faaliyetler üzerinde önleyici bir etkide bulunmak da cezanın amaçları arasındadır[471]. Bununla birlikte cezalar, kimi zaman cezanın önleyici amacını yerine getirmekte yetersiz kalır. Nitekim bazı faillerin salt ceza infaz kurumlarına gönderilmesiyle kişiliklerinden kaynaklanan tehlikelilik ortadan kalkmayacaktır. Bu kişilerin yeniden topluma kazandırılmasına yönelik ayrıca tedbirlere başvurulması ve toplumun bu kişilerden korunması, faile özgü yaptırımlar olan güvenlik tedbirlerinin uygulanması fikrini doğurmuştur. Bu tedbirleri, hem fiilden hem failin kişiliğinden kaynaklanan tehlikelilik haline karşı önlem almak için

[471] Ceza hukukunun önleyici işlevi hakkında bkz. Eylem Aksoy Retornaz, "Beccaria'nın Hapis Cezasına Bakışı Üzerine Bir Değerlendirme", **Türkiye Barolar Birliği Dergisi**, Cilt:112, 2014, ss.93-106, s.97.

özgülenen ve hâkim tarafından belirlenen yaptırımlar olarak tanımlamak mümkündür[472].

Ceza hukukunda en temel ilkelerden biri olan "nulla poena sine culpa" ilkesi, ancak kusurlu kişilerin cezalandırılabilmelerini mümkün kılar. Bu ilke gereği fiili gerçekleştirdikleri sırada kusur yeteneği bulunmayan kişiler cezalandırılamayacaktır[473]. Kimi zaman akli melekelerinin yetersiz olması, yaş küçüklüğü, alkol ve uyuşturucu bağımlılığı gibi pek çok nedenle kişilerin fiili gerçekleştirdiği sırada kusur yeteneği bulunmamakta, bununla birlikte bu kişilere karşı caydırıcı yaptırımların uygulanmasında toplumun korunması için zorunluluk bulunmaktadır. Oysa kusur yeteneği bulunmayan bir kişi, ceza kanundaki tarife uygun bir fiili gerçekleştirse dahi, bu kişiye ceza yaptırımı uygulamak mümkün değildir. Nitekim cezanın verilme amacı değerlendirildiğinde, kusur yeteneği bulunmayan kişilerin, korkutma ve caydırma amaçlarını algılayabilmeleri imkân dâhilinde değildir. Bu durumda bu kişilere ceza uygulansa dahi erişilmek istenen amaca ulaşılamayacaktır. Öte yandan kusur yeteneği olmayan kişilere hiçbir ceza yaptırımı uygulanmaması, toplumu savunmasız bırakır. Bu nedenle, isnat yeteneği bulunmayan ve tekrar suç işleme tehlikesi bulunan kişileri yeniden topluma kazandırmaya yönelik ceza ile birlikte veya ceza yerine geçen güvenlik tedbirlerinin uygulanması öngörülmüştür[474]. Dolayısıyla, güvenlik tedbirleri, cezalardan farklı olarak faili eğitmek, koruma altına almak ve yeniden sosyalleştirmek amacıyla amacıyla suç teşkil eden fiili gerçekleştirenlere yönelik yaptırımlar uygulanmasını öngörülmektedir[475].

Güvenlik tedbirlerinin hukuki niteliği ele alındığında, bu tedbirlerin ceza hukuku kapsamında yaptırımlar olduğu, ancak cezalardan farklılaştığı göze çarpmaktadır. Cezalar her ne kadar önleyici fonksiyonu bakımından güvenlik tedbirleriyle benzeşse de temel olarak işlenen suça yönelik bir reaksiyon teşkil ederler. Güvenlik tedbirleri ise yeniden suç işlenmesi tehlikesine, dolayısıyla gelecekte gerçekleşmesi muhtemel

---

[472] Mehmet Emin Artuk/Erkam Yılmaz, "Teorik Açıdan Güvenlik Tedbirleri", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:2, Güz 2020, ss.7-43, s.9.

[473] Artuk/Yılmaz, s.8.

[474] Hamide Zafer, "Emniyet Tedbiri Muhakemesinin Özellikleri", **İstanbul Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:62, Sayı:1-2, ss.263-314, s.265.

[475] Veli Özer Özbek/Koray Doğan/Pınar Bacaksız, **Ceza Hukuku Genel Hükümler**, Seçkin Yayınevi: Ankara, Eylül 2021, s.626, 627. Suçun konusu ya da işlenmesinde kullanılan araca yönelik güvenlik tedbirleri de bulunmaktadır. Örneğin uyuşturucu maddenin müsadere edilmesi veya kazanç müsaderesi bu kapsamda ele alınabilecek tedbirlerdir, bkz. Özgenç, İzzet, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayınevi: Ankara, Eylül 2021, s. 929, 930.

suça yöneliktir. Uygulanabilmeleri, evleviyetle fail tarafından suçun işlenmesine bağlıdır, ancak güvenlik tedbirleri işlenmiş suça cevap değil, gelecekteki suçluluktan toplumu koruma vasıtasıdır[476]. Dolayısıyla, cezanın birincil amacı "fiilin öcünü alma" şeklinde geriye yönelik iken güvenlik tedbirleri ileriye yönelik olarak kişileri topluma yeniden kazandırma amacını gütmektedir[477]. Bununla birlikte hümanist ceza hukuku anlayışında, "hiçbir ceza yalnız ceza olma vasfını muhafaza etmemelidir"[478]. Bu bağlamda salt kefaret anlayışından beslenmemesi gerekir. Bu anlayış, insancıl ceza hukukunda cezaların amacını güvenlik tedbirlerine yaklaştırmaktadır. Güvenlik tedbirlerini asıl ayırt eden, fiili değil faili ön plana alarak daha çeşitli önlemler içermeleri, bunun yanı sıra kusur yeteneği olmayan kişilere dahi uygulanabilmeleridir. Aşağıda daha detaylarıyla ele alınacak failin tehlikeliliği kavramının ceza hukukuna sirayeti, güvenlik tedbirleri ile somutlaşmıştır.

Güvenlik tedbirlerinin, ceza hukuku çerçevesinde düzenlenmiş olmakla birlikte idari tedbir niteliği taşıdığı görüşü de doktrinde ileri sürülmektedir. Buna gerekçe olarak güvenlik tedbirlerinin gelecekteki tehlikeye yönelik olmaları gösterilmiştir[479]. Tehlikeliliğe odaklanmaları ve önleyici fonksiyonları nedeniyle güvenlik tedbirlerinin "polis tedbirleri" olarak kategorize edildiği de görülmektedir. Ancak idare hukukunda kolluk tedbirleri, bireylerin kişiliği ile değil, kamu düzenine yönelik tehlike oluşturan faaliyetler ile ilgilenir[480]. Bir suç işlenmeden önce devreye giren önleyici idari tedbirler, suçun işlenmesi üzerine uygulanan güvenlik tedbirleri ile karıştırılmamalıdır. İdari tedbirler ile emniyet tedbirleri arasındaki sınırları belirgin şekilde çizen Kunter, öncelikle yaptırım içeren tedbirleri, kendi içerisinde bastırıcı tedbirler ve önleyici tedbirler olarak ayırmaktadır. Bastırıcı tedbirler, suçlunun "tehlike hali suç şeklinde meydana çıktıktan sonra" tatbik edilir. Önleyici tedbirler ise suç işlenmeden önce ("ante delictum") devreye girerler. Önleyici tedbirleri kendi içerisinde suç sebeplerini ortadan kaldırmak veya azaltmak üzere sevk edilen "uzak önleyici" tedbirler veya suç işlemeye hazırlanan kişileri zararsız hale getirmeye çalışan polis tedbirleri ("yakın önleyici tedbirler") olarak ikiye ayırmak mümkündür. Bunlar

---

[476] Artuk/Yılmaz, 14, 15.
[477] Zafer, "Emniyet Tedbiri Muhakemesinin Özellikleri", s. 267, Faruk Erem,"Türk Ceza Kanununda Emniyet Tedbirleri", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:1, Sayı:3, 1944, s. 351-378, s.352.
[478] Erem, "Türk Ceza Kanununda Emniyet Tedbirleri", s.355.
[479] Vedat A. Dilberoğlu, "Cezalar ve Güvenlik Tedbirlerinin Amacı ve Niteliği", **Ankara Üniversitesi Hukuk Fakültesi Dergis**i, Cilt: 65, Sayı: 4, 2016, ss. 1517-1544, s.1523.
[480] Dilberoğlu, s.1522.

"suçluluğu tedavi etmek" amacı gütmezler, yalnızca tehlike doğmadan önce müdahale etmekle ilgilenirler[481]. Bu bağlamda örneğin PVSK m.13'te öngörülen kolluğun "toplum için tehlike teşkil eden akıl hastası, uyuşturucu madde veya alkol bağımlısı serseri veya hastalık bulaştırabilecek kişileri" yakalama yetkisi önleyici bir yetkidir. Güvenlik tedbirleri ise bu kişileri, suç teşkil eden bir eylem gerçekleştirmelerinin ardından yeniden sosyalleşmelerini sağlamak amacıyla uygulanır. Dolayısıyla güvenlik tedbirleri, kişinin suç işlemesiyle ortaya çıkan "cürmî tehlikelilik"le ilgilenirken, polis tedbirleri "içtimai tehlikelilik" denilen, topluma yönelik tehlikelilik ile ilgilenir. İki farklı hukuk dalına ve farklı usullere tabi olan bu tedbir türlerinin karıştırılmaması gerekir. Nitekim bu kavram karışıklığı, kimi ülkelerde emniyet tedbirlerinin henüz suç işlememiş kişilere uygulanmasına yol açmış[482] ve ceza hukukunun alanı "içtimai tehlikeliliği" de içerecek şekilde genişletilmiştir.

2. Failin Tehlikeliliği

Güvenlik tedbirlerinin, ceza hukuku çerçevesinde, cezadan farklı bir yaptırım olarak hukuki niteliğinin tespit edilmesinin ardından, bu tedbirlerin temelini oluşturan tehlikelilik kavramının üzerinde durulmalıdır. Nitekim bu kavramın ceza hukukuna girmesi, mevzuatta esaslı değişikliklere açmış, ceza kanunlarında hazırlık hareketlerine yayılan suçların düzenlenmesine yol açtığı gibi, muhakeme ve infaz sürecini de değişime uğratmıştır.

Fiilden ziyade failin tehlikeliliği üzerine yoğunlaşmak, Ceza Hukukunda 19. yüzyılda ortaya çıkan Pozitivist Okulun mirasıdır. Pozitivistler, insanların hareketlerinin belirli sebeplerin determinist şekilde meydana getirdiği sonuçlar olduğunu ileri sürer. Bu okula göre, karar verme yetisi olduğunu sanan insanlar, aslında yalnızca antropolojik, fiziki ve sosyal şartların onları yönelttiği şekilde hareket etmektedir[483]. Bu iddianın iki sonucu vardır. İlk sonuç, kişilerin hür iradesi olmadığı, fillerini tayin etmekten yoksun oldukları, dolayısıyla kusurlu fiil ve iradeyi esas alan ceza anlayışının yerinde olmadığıdır. İkincisi, benzer sosyal, fiziksel ve kalıtsal özellikleri gösteren kişilerin, suç yoluna kaçınılmaz şekilde gireceği ve geleceklerinin

[481] Nurullah Kunter,"Bugünkü Ceza Hukukunda Emniyet Tedbirlerinin Yeri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt:13, Sayı:4, 1947, ss.1327-1349, s.1343, 1344.
[482] Kunter, s.1344, 1345.
[483] Artuk/Yılmaz, s. 19.

öngörülebilir olduğu iddiasıdır. Bu nedenle, faillerin işlediği suçun ağırlığı ve ne şekilde bu suçu işledikleri kadar, fiili işlemeden önceki hayat tarzları, yaşam koşulları, aile yapıları ve diğer sübjektif nitelikler, yeniden suç işleme eğilimlerinin tayininde göz önüne alınmalıdır. Böylelikle failin tehlikelilik hali tayin edilerek yaptırım öngörülmeli ve gerektiğinde bu yaptırım başka yaptırımlara çevrilebilmelidir. Bu yönüyle faildeki tehlike hali, suçu değil cezayı etkileyen bir sebeptir. Bugünkü ceza hukukunun temeli olan kusurluluk ise sadece suç teşkil eden fiilden yola çıkarak belirlenir. Failin geçmişi veya gelecekte yeniden suç işleme eğiliminde olması, işlediği fiil açısından kusurunun ve suçun oluşup oluşmadığının tespitinde dikkate alınmaz[484].

Pozitivist ekolün önde gelen kurucularından Ferri, failin tehlikeliliğini belirlerken kişilerin fiziki ve psikolojik yapılarını ifade eden antropolojik faktörlerin, bulundukları çevreye ilişkin iklim, mevsim, günün bölümü gibi fiziki faktörlerin ve son olarak örf, âdeti din, aile yapısı, eğitim durumu ve alkol veya uyuşturucu bağımlılığı gibi sosyal faktörlerin dikkate alınması gerektiğini belirtmiştir[485]. Pozitivistlerin ileri sürdüğü bu faktörlerin büyük kısmının bugün profilleme teknolojileri tarafından değerlendirilen etkenler arasında yer alması dikkat çekicidir. Bununla birlikte pozitivistler, "tehlikeli kişiler" şeklinde genel bir grup yaratmakla yetinmemiş, suçlulara ilişkin farklı alt kategoriler yaratarak, her suçlu kategorisine yönelik farklı tedbirlerin uygulanması gerektiğini vurgulamıştır. Bu bağlamda örneğin 1919 tarihli İtalyan Ceza Kanunu taslağını hazırlayan Ferri'ye göre, suçlular doğuştan suçlu, akıl hastalığı olan suçlular, itiyadi suçlular, tesadüfi suçlular ve ihtiras suçluları şeklinde gruplandırılabilir[486]. Farklı nedenlerle kusurlu kabul edilemeyecek suçlu türlerinin hepsinde ortak husus, toplumun bu kişilere karşı korunması gerektiğidir. Bununla birlikte, münhasıran failden kaynaklanan tehlikelerin savuşturulması için failin yapısına bağlı, bireyselleştirilmiş güvenlik tedbirleri öngörülmelidir[487].

Bugün profilleme teknolojilerinin, bir kişinin suç işleyip işlemeyeceğini, suçu nerede işleyeceğini veya suç işlemiş faillerin yeniden suç işleme olasılığını tespit ettiği görülmektedir. Bunlardan özellikle yeniden suç işleme ihtimali çerçevesinde itiyadi suçlular üzerinde ayrıca durulmalıdır. Bir suçlunun itiyadi suçlu olup olmadığını tespit

[484] Ümit Kocasakal, **Ceza Hukukunda İtiyad**, İstanbul Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 1994, s.19, 20.
[485] Kocasakal, s.16.
[486] Kocasakal, s.12.
[487] Artuk/Yılmaz, s.16.

etmek için yalnızca birden fazla kez suç işlemesine dayanmak yanıltıcı olabilecektir. Nitekim kimi zaman iki veya daha fazla suçun işlenmesi, tesadüflerin veya alkol, uyuşturucu bağımlılığı gibi farklı nedenlerin neticesi olabilir. Pozitivistlere göre en tehlikeli suçlu grupları arasında bulunan itiyadi suçluları tespit için, birden fazla kere suçun işlenmesi şeklinde objektif bir kriterin yanı sıra, bir adım daha ileri gidilerek, failin sübjektif nitelikleri, örneğin geçmişi ve kişiliği incelenmeli, gelecekte yeniden suç işleme eğilimi bu iki unsur birlikte dikkate alınarak tespit edilmelidir. Suç işleme hususunda ısrar ve alışkanlık gösteren, tekrar suç işleyeceği objektif ve sübjektif unsurlara göre belirlenen kişilere yalnızca ceza verilmesi yeterli olmayacaktır, bu kişilere yönelik tedbirlerin alınması gerekir[488]. Bunun yanı sıra suç işlemeyi alışkanlık haline getiren itiyadi suçlular ile birden çok kez suç işlemekle birlikte alkol, uyuşturucu bağımlılığı veya akli melekelerinin yetersizliği nedeniyle hukuka aykırı fiilleri gerçekleştiren kişiler ayırt edilmelidir. Nitekim farklı nedenlerle suç işleyen bu gruplar, topluma dönük farklı sorunlar doğururlar. Dolayısıyla bu kişilere uygulanacak bir toplumsal savunma aracı olan güvenlik tedbirleri de farklı önlemler içermelidir[489]. Bu yönde, Avrupa Konseyinin girişimi ve Birleşmiş Milletlerin desteği ile kurulan Avrupa Birliği İstişari Grubu da 1956 tarihinde Cenevre'de gerçekleştirdiği konferansta[490], serseriler ve dilencilerin, kabahat veya taksirli suç işleyenlerin ve birden fazla kez tesadüfi suç işleyenlerin, itiyadi suçlu grubunun dışında değerlendirilmesi gerektiğini vurgulamıştır[491]. Dolayısıyla bu kişilere uygulanacak tedbirlerin, itiyadi suçlulardan farklı olması gerektiğinin altı çizilmiştir.

Modern ceza hukukunda elbette "doğuştan suçlu" kavramı kabul görmemektedir. Pozitivistlerin belirli kişilerin doğuştan suç işleme potansiyeli barındırdığını ileri süren determinist yaklaşımı kabul edilmemiş, ceza hukuku sistemi, herkesin özgür iradesinin olduğu fikri üzerine inşa edilmiştir. Bununla birlikte fiili işlediği sırada kendisine kusurluluk atfedilmesi mümkün olmayan, ancak topluma yönelik somut tehlike arz eden kişilere yönelik önlemler, pozitivistlerin etkisiyle ceza hukuku düzenlemelerinde yerini almıştır. Ancak modern ceza hukukunda, tehlikeli bireyleri toplumdan ve sosyal hayattan uzaklaştırma, güvenlik tedbirlerinin yegâne

[488] Kocasakal, 13-15.
[489] Kocasakal, 23, 24.
[490] Detaylar için bkz. Sahir Erman, "Suçun Önlenmesi ve Suçlular Hakkında Yapılacak Muamele Mevzuunda Birleşmiş Milletler Avrupa Bölgesi İtişari Grubunun Üçüncü Konferansı", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Sayı:1-2, 1958, ss.14-26, s.14.
[491] **Ibid.**, s.20.

amacı değildir. Aksine, güvenlik tedbirlerinin yöneldiği amaç, bu kişileri insan onuruna yaraşır bir sosyal hayata yeniden hazırlamak olmalıdır[492].

3. Güvenlik Tedbirlerinin Uygulanabilme Şartları

Bir ceza hukuku yaptırımı olan, dolayısıyla kişi hak ve özgürlüklerini sınırlayan güvenlik tedbirleri, belirli sınırlara tabi olmak zorundadır. Bunlardan ilki kanunilik ilkesidir. Suç ve cezada kanunilik ilkesi, güvenlik tedbirleri için de geçerlidir. Güvenlik tedbirini gerektirecek fiiller ve bu fiiller işlendiği takdirde hangi tedbirlerin uygulanacağı kanunda açıkça gösterilmelidir[493]. Nitekim Anayasa'nın 38. maddesinde ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur denilmiş, yine TCK m.2 kapsamında da kanunun açıkça suç saymadığı bir fiil için kimseye güvenlik tedbiri uygulanamayacağı güvence altına alınmıştır.

Güvenlik tedbirlerine, hapis cezalarında olduğu gibi hâkim kararıyla hükmedilmelidir. Hürriyeti kısıtlayıcı etkisi olan güvenlik tedbirleri açısından, kararın adil ve hukuka uygun olması için hâkim güvencesi şarttır[494]. Güvenlik tedbirine hükmedebilmek için ilk olarak ilgili kişinin suç teşkil eden fiili işleyip işlemediğinin tespit edilmesi gerekir ki bu duruma ancak yargı karar verecektir. Yargı kararı ile fiilin işlendiğinin tespit edilmesinin ardından, ikincil olarak hâkim, kanunda belirtilen sınırlar içinde uygulanacak tedbire karar verecektir. Karar vermeden önce uzman yardımı almak mümkün ve çoğu durumda gereklidir, ancak nihai karar yine hâkim tarafından verilecektir[495].

Güvenlik tedbirleri kusur ilkesine dayanmadığından, orantılılık ilkesi çerçevesinde sınırlanmaktadır. İlgili tedbire, failin durumu, bağımlılığı, yaşı, akli melekeleri ve diğer nitelikleri gözetilerek karar verilmelidir. Alınacak tedbir, topluma yeniden kazanma amacı için gerekli ve bu amaç için elverişli olmalıdır. TCK m. 3 de suç işleyen kişi hakkında işlenen fiilin ağırlığı dikkate alınarak, fiilin ağırlığı ile de orantılı şekilde güvenlik tedbirine hükmolunacağının altını çizmektedir[496]. Cezada

---

[492] Kocasakal, s. 46.
[493] Erem, s.352, Dilberoğlu, s. 1536, Artuk/Yılmaz, s. 28.
[494] Artuk/Yılmaz, s.30.
[495] Dilberoğlu, s.1540.
[496] Artuk/Yılmaz, s.29.

orantılılık açısından, fiilin ağırlığı ve failin kusurluluğu dikkate alınırken, güvenlik tedbirlerinde kişinin kusur yeteneği bulunmadığından kusur yerine failin tehlikelilik hali dikkate alınacaktır[497]. Tehlikelilik hali kişilerin sosyal özellikleri, geçmişleri, aile yapıları ve eğitim düzeylerine dayanarak belirlenebilir, ancak öncelikle söz konusu tehlikeliliğin suç teşkil eden bir fiille dışa vurulmuş olması gereklidir. Aksi halde kişinin tehlikeliliği ceza hukukunun konusunu oluşturmayacaktır. Bu nedenle failin gelecekte ceza hukuku normlarını ihlal edeceğine yönelik tehlike halinin tespit edilmesi için öncelikle suç işlenmiş ve ardından tekrar suç işlenme tehlikesi bulunup bulunmadığı yargı makamı tarafından değerlendirilmiş olmalıdır. Salt hazırlık hareketlerinde bulunan kişiye ceza hukuku yaptırımı olan güvenlik tedbiri uygulanamayacaktır[498]. Suç teşkil etmemekle birlikte, belirli dış gösterilere dayanarak, bir kişi hakkında güvenlik tedbirlerine müracaat edilebileceğini öneren Lombroso'nun düşünceleri müspet hukukta kabul görmemiştir[499]. Bu nedenle, suç işlenmemiş kişiye güvenlik tedbiri uygulanması, hak ve özgürlüklerin hukuka aykırı şekilde kısıtlanması anlamına gelecektir.

Güvenlik tedbirleri süreleri bakımından da cezalardan farklı nitelik gösterirler. Kanunda suç teşkil eden fiillerin karşılığı olan cezaların süresi öngörülmüşken, güvenlik tedbirleri açısından, bu tedbirlerin failin tehlikeliliğine yönelik olmaları nedeniyle belirli bir süre öngörülmemiştir. Suçludaki topluma yönelik tehlike halinin ne zaman tamamen ortadan kalkacağını önceden tespit etmek mümkün değildir, bu nedenle güvenlik tedbirlerine süre bakımından sınır öngörülmeksizin karar verilebilmektedir[500]. Fail sosyal hayata yeniden uyum sağlayabilecek ve toplum bakımından tehlike göstermeyecek hale ulaşana kadar güvenlik tedbiri uygulanacaktır. Ancak kişinin tehlikelilik halinin devam ettiğinin veya topluma uyum sağlamaya hazır olduğunun mutlak bir şekilde belirlenmesi imkânsızdır. Bununla birlikte pozitivistlerin "suçluların düzelmezliği karinesi" modern ceza hukukunda kabul görmemektedir. Dolayısıyla, tehlikelilik halinin giderilmesi için süreler bakımından esneklik tanınmış olsa da süre açısından belirsizliğin suiistimal edilmesi önlenmelidir. Aksi halde mahkûmun umudunu yitirmesi ve yeniden uyum için motivasyonunu kaybetmesi söz konusu olacaktır. Özellikle güvenlik tedbirleri açısından kanunda üst sınırın

[497] Dilberoğlu, s.1523, Erem, s.353.
[498] Artuk/Yılmaz, 25-28.
[499] Erem, s.352.
[500] Erem, s.353. Erem bu durumu "hudutsuz hüküm" olarak niteliendirmektedir.

öngörülmemesi, keyfiliğe yol açma riski barındırmaktadır[501]. Bu nedenle karşılaştırmalı hukukta örneğin İtalya, Brezilya, Polonya kanunlarında, güvenlik tedbirleri için sürenin alt sınırını öngörülmüş; Belçika, Hollanda ve İspanya'da ise tedbirin üst sınırı belirlenmiştir. Yalnızca alt veya üst sınırın öngörüldüğü bu düzenlemeler, "nispi müddetsiz hükümler"dir. Bunlar arasında Belçika ve Hollanda üst sınır öngörmekle birlikte, ara bir formül olarak failde tehlikeliliğin devam etmesi halinde hâkime kanunda öngörülen süreyi uzatma yetkisi verilmiştir. İngiltere ve Romanya gibi kimi ülkelerde ise güvenlik tedbirleri açısından hem alt hem üst sınırların belirlendiği kanunlara rastlanılmaktadır[502]. Türkiye'de TCK m.32/1 kapsamındaki akıl hastaları, TCK m.54'te öngörülen müsadere, yine TCK m.59'daki sınır dışı edilme ve TCK m. 60'ta tüzel kişilere yönelik düzenlemelerde güvenlik tedbirleri bakımından azami veya asgari bir sınır görülmemiştir. Diğer gruplara yönelik tedbirler ise belirli bir süreyle sınırlanmaktadır. Örneğin Çocuk Koruma Kanunu m.7/6 kapsamında çocuklar hakkında koruyucu ve destekleyici tedbirler 18 yaşının tamamlanmasıyla sonlandırılacak, yine belirli hakların sınırlanmasına ilişkin TCK m.53 kapsamındaki tedbir, kişinin işlediği suç için öngörülen mahkûmiyetin infazı tamamlanmasıyla sona erecektir. TCK m.32/2 gereği, akıl hastalığı kişinin isnat yeteneğini tamamen ortadan kaldırmayacak, yalnızca azaltacak derecede ise kişi hakkında öngörülen hapis cezasından daha uzun süre güvenlik tedbiri uygulanması mümkün değildir[503]. Ancak güvenlik tedbirlerinin hak ve özgürlükleri ihlal etmemesi açısından bu tedbirlerin belirli bir süre ile kısıtlanması ve ara çözüm olarak örneğin failin hâlâ uyuşturucu bağımlılığını yenemediği veya isnat yeteneğini ortadan kaldıran diğer sebeplerin devam ettiği tespit edildiği halde sürenin uzatılması daha yerinde olacaktır.

Sonuç olarak kanuni tarife uygun fiilde bulunmamış kişinin ileride suç işleyeceğine dair tehlikenin mutlak kesinlikte tespit edilmesi mümkün değildir[504]. Bu bağlamda, kişinin hürriyetini kısıtlayan güvenlik tedbirlerinin uygulanması için öncelikle kişinin suç işlemiş olması gerekir. Söz konusu objektif unsur oluşmadan, salt kişinin karakteri, geçmiş sabıkaları, suçu işlemeden önceki veya işledikten sonraki tutumu, kişisel, ailevi ve sosyal ilişkileri tek başına güvenlik tedbirlerinin uygulanması

[501] Kocasakal, s.43.
[502] Artuk, "Güvenlik Tedbirleri", s. 473, 474.
[503] Artuk/Yılmaz, s.37.
[504] Zafer, s.272.

için yeterli değildir. Bunun yanı sıra şahsın toplum bakımından tehlike arz edip etmediği hâkim tarafından incelenmeli ve kişinin özgürlüğü hâkim denetimiyle garanti altına alınmalıdır. Kimi ülkelerde, hâkimin takdir yetkisi kanunla daha da daraltılmış, hangi hallerin tehlikeli hal sayılacağı açıkça tanımlanmıştır[505].

Modern ceza hukuku, kişilerin tehlikeli halinin, başka bir deyişle suç işleyeceği ihtimalini değerlendirmekle birlikte, bu tahminin "matematik bir denklem sonucu"[506] gibi keskin olmadığını dikkate alır. Dolayısıyla günümüzde insan onuruna ve iradesine saygı üzerine inşa edilen ceza hukuku, kişileri kararlarını değiştirmekten yoksun "doğuştan ve ebedi suçlu" olarak kabul etmemektedir. Bu nedenle güvenlik tedbirleri, kişiyi tamamen toplumdan soyutlamayı değil, onun yeniden suç işleme eylemliliğinden uzak duracak bir birey olarak topluma kazandırmayı amaçlamaktadır.

4. Profilleme Teknolojilerinin Güvenlik Tedbirleri ile Karşılaştırılması

Profilleme teknolojileri, güvenlik tedbirlerine benzer bir şekilde tehlikelilik kavramı üzerine yoğunlaşmaktadır. Precobs, Predpol gibi profilleme yazılımları, sosyal, ekonomik faktörler ve suç oranlarını analiz ederek kimi zaman tehlikeli bölgeleri kimi zaman ise tehlikeli kişileri tespit etmek üzere kullanılmaktadır. Ancak bu teknolojilerin güvenlik tedbirlerinden en büyük farkı, kişilerin hiç suç işlemediği hallerde de uygulama alanı bulmalarıdır.

Kişiyi suç işlemeden önce hedef alan profilleme teknolojilerine örnek olarak CAPPS II verilebilir. CAPPS II ile farklı veri tabanlarından elde edilen veriler birleştirilerek topluma tehlikeli olabilecek kişiler uçuş yasağı listesinde toplanmaktadır[507]. Hakkında herhangi bir soruşturma veya kovuşturma bulunmayan kişilerin, seyahat özgürlüğü sadece bu teknolojiler tarafından tehlikeli bulunmaları sonucu engellenebilmektedir. Uçuş yasağı bu tür listelerden yalnızca biridir. Yine Şikago'da başvurulan profilleme yazılımları oldukça genel bir liste olan "tehlikeli

[505] Bu duruma örnek olarak İtalyan Ceza Kanunu'nda itiyadi (m.102), profesyonel (m.105) ve suça eğilimli (m.108) kişilerin gösterildiği ve yalnızca bu niteliklere uygun kimse hakkında güvenlik tedbirleri uygulanabileceği (m.109) hususunda bkz. Artuk, "Emniyet Tedbirleri", s.468. Türk Ceza Kanunu'nda ise md. 6/1/h'de itiyadi suçlu tanımına yer verildiği ve bu tanımın kişinin kasıtlı bir suçun temel ya da nitelikli hallerini bir yıl içerisinde ikiden fazla kez işlemesi şeklinde sadece objektif unsurlara dayandığı görülmektedir.

[506] Kocasakal, s. 21.

[507] Ayrıntı için bkz. Florence, s.2156 vd.

kişiler" listesi oluşturmakta, bu kişiler henüz suç işlemeden kolluk denetimi altında tutulmakta ve suç işlerlerse alacakları cezalara ilişkin uyarı almaktadır[508].

Bunun yanı sıra PredPoL, Hunchlab gibi yazılımlar, bir bölgede daha önce hangi tip suçların işlendiği, suç işlenme sıklığı, bölgenin ekonomik, sosyal yapısı gibi unsurlara dayanarak tehlikeli bölgeleri tespit etmek üzere kullanılmaktadır. Bu yazılımlar aracılığıyla tespit edilen bölgelerde yaşayan kişiler, henüz suç işlemeseler dahi durdurma, arama ve sürekli gözetim altında tutulma gibi tedbirlere maruz bırakılmaktadır[509]. Bu yazılımların, güvenlik tedbirlerinden ilk göze çarpan farkı, soyut bir tehlikeye dayanmaları ve kişilerin herhangi bir hukuk normunu ihlal eden davranışları bulunmaksızın müdahaleye uğramalarına kapı aralamalarıdır. Bu tedbirlerin, suç işlenmeden önce devreye giren ve suç ile ortaya çıkan cürmi tehlikelilikten çok, topluma yönelik tehlikeyi bertaraf etmek isteyen polis tedbirleri kapsamında ele alınması daha yerindedir. Ancak bu tür profilleme teknolojilerinin vardığı sonuçlarla, hakkında hiçbir somut suç şüphesi bulunmayan kişilere karşı ceza muhakemesi araçları seferber edilmektedir. Bu tür teknolojilere dayanarak kişilerin seyahat özgürlüklerinin ve özel hayatın gizliliği haklarının kısıtlanması kuşkusuz ki hukuka aykırıdır. Bu bağlamda, belirlenen mahallelere sürekli kolluk sevk edilmesi, bu kişilerin düzenli olarak durdurulmaları, aranmaları ve verilerinin yeni tehlike listeleri oluşturmak üzere toplanması, profilleme teknolojilerinin tespit ettikleri mahalleleri bir nevi açık ceza infaz kurumuna dönüştürmektedir. Yine kişilerin kendilerine açıklanmayan sebeplerle ve hâkim kararı olmaksızın uçuş yasağına tabi tutulması, yargılanmaksızın adli kontrol tedbirine tabi tutulmaları anlamına gelmektedir. Dolayısıyla suç işlenmeden önce gerçekleştirilen bu müdahalelerin, idare ve kolluk hukuku kapsamında kalması gerektiğinin altı çizilmeli, suç öncesi bu alanda, ceza muhakemesi kapsamındaki tedbirler seferber edilmemelidir.

Kişilerin suç işlemelerinin ardından başvurulan profilleme teknolojilerine örnek olarak ise Static 99 ve PTRA (Pre Trial Risk Assessment) verilebilir. Daha önce açıklandığı üzere cinsel suçlarda itiyadi suçluların tespiti için kullanılan Static 99, ilgili kişinin yaşı, daha önce uzun süreli ilişki yaşayıp yaşamadığı, mağdurun özellikleri, kişinin daha önce cinsel suç işleyip işlemediği ve en son işlediği suçun tarihi gibi

[508] Lynskey, s. 167, 168.
[509] O'Neil, s.85 vd.

unsurlara dayanmaktadır[510]. Bunun yanı sıra PTRA ve benzeri yazılımlar, kişinin aile yapısı, eğitim düzeyi, işsiz olup olmadığı, Amerikan vatandaşlığı bulunup bulunmadığı, işlediği suçun ağırlığı, alkol veya uyuşturucu bağımlılığı gibi unsurları dikkate almaktadır[511]. Yine LSI-R yazılımı kişinin sabıka kaydı, maddi durumu, boş zamanlarını ne şekilde değerlendirdiği, akıl sağlığı, alkol-uyuşturucu kullanma oranı gibi farklı faktörleri irdeleyerek kişinin tehlikeliliğini tespit etmektedir[512].

Bu tür yazılımlar, en azından suç işlemiş kimselerin yeniden suç işleme veya genel olarak tehlikeliliklerini tespit ettiklerinden güvenlik tedbirlerine yaklaşmakla birlikte daha detaylı ele alındıklarında çok temel farklılıklar barındırmaktadır.

Bu farklardan ilki gerek suç işlenmeden önce gerek sonrasında başvurulan profilleme teknolojilerinin amaçları bakımındandır. Bu tür teknolojiler, güvenlik tedbirlerinin öncelikli amacı olan faili yeniden topluma kazandırmayı hedeflememektedirler. Aksine, kişileri "toplumun kalanından farklı", "antisosyal" olduğu iddia edilen gruplar altında toplayarak toplumdan ayırmak üzere kullanılmaktadırlar. Toplumu "sapkın kişiliğe sahip" olanlar ve "güvenilir vatandaşlar" olarak ikiye ayıran bu uygulamalar, fiilden yola çıkan tehlikelilik anlayışı yerine kişinin değiştirmesi mümkün olmayan aile yapısı, sınıfı, yaşını, kısacası bizatihi varlığını soyut bir tehlike olarak kabul etmektedir[513]. Bu durum, kişilere yeniden şans tanıyan ve sosyal hayata kazandırılmalarını hedefleyen modern ceza hukuku anlayışından, "doğuştan, değiştirilemez" suçlu algısına dayanan bir önceki yüzyıla dönüşe işaret etmektedir.

İkinci fark kanunilik ilkesi açısından görülmektedir. Güvenlik tedbirlerinin hangi hallerde uygulanacağının ve bu hallerde ne gibi tedbirler alınacağının kanunda açıkça belirtilmesi gerekir. Oysa bu tür teknolojilerin ceza hukukunda kullanılma usulü ve hangi hallerde bunlara başvurulabileceği açıkça düzenlenmemiştir. Kaldı ki bu teknolojilere ilişkin açık bir düzenleme bulunsa dahi, belirlilik ilkesinin sağlanması mümkün değildir. Nitekim bu teknolojilerin kişisel verileri bölümünde üzerinde

[510]Rettenberger/Eher, s.356, 357.
[511] Gouldirn, s. 710, 711.
[512] Hamilton, s.258.
[513] Tyler, Tom R./ Jackson, Jonathan/ Mentovich, Avital, "The Consequences of Being an Objectof Suspicion: Potential Pitfalls of Proactive Police Contact", **Journal of Empirical Legal Studies**, Cilt:12, Sayı: 4, Aralık 2015, ss. 602–636, s.608-610.

detaylı şekilde durulduğu üzere, makine öğrenmesine dayanması, hangi veriler arasında ne tür bir bağın kurulduğunu, dolayısıyla hangi verilere dayanılarak tehlike skoruna ulaşıldığını açıklamayı imkânsız kılmaktadır. Dolayısıyla, açık bir düzenleme ile suç işlenmiş olması, süre sınırı, hâkim denetimi gibi güvenceler öngörülse dahi, bu teknolojilerin failin tehlikeliliği sonucuna nasıl vardıklarını öngörülür şekilde açıklamak mümkün olmayacaktır.

Güvenlik tedbirleri, öncelikle kişinin suç işlediğinin tespitini içermektedir. Bu tespit ancak yargı makamı tarafından yapılabilir. Kişinin akıl sağlığı, bağımlılığının kusur yeteneğine etkisi gibi hususlar bilirkişi görüşü alındıktan sonra tespit edilmekle birlikte, güvenlik tedbirine ilişkin son karar yine hâkim tarafından verilecektir. Oysa profilleme teknolojileri kişinin tehlikeliliğini kimi zaman salt sübjektif, kimi zaman ise objektif unsurları dikkate alarak, ancak hangi unsurların tehlikelilik tespitinde esas olduğunu gerekçelendirmeksizin otomatik olarak belirlemektedir. Bu sürecin insan eliyle, mantık süzgecinden geçirilerek değerlendirilmesi mümkün olmamakta, hatta bizzat yazılımcılar tarafından bile tamamen açıklanması imkân dâhilinde bulunmamaktadır. Bu durumda salt profilleme teknolojilerinin aldığı kararlara, içeriği anlaşılmaksızın onay vermek, şekli bir kontrolden öteye geçmeyecektir. Bu nedenle süreçte, güvenlik tedbirlerinde söz konusu olduğu gibi gerçek bir hâkim denetiminden bahsetmek mümkün değildir.

Son olarak güvenlik tedbirlerinin failin durumu gözetilerek verilmesi ve bireyselleştirilmesi gerekir. Nitekim yeniden sosyalleştirme amacını gerçekleştirmek için her failin ihtiyacına göre uygun yöntem belirlenmelidir. Oysa yukarıda açıklandığı üzere profilleme teknolojileri kişinin uyuşturucu bağımlılığı, akıl sağlığı, suça eğilimi gibi pek çok farklı faktörü bir arada değerlendirmekte, hepsi üzerinden soyut bir tehlikelilik puanı öngörmektedir. Bu durum genelgeçer nitelikte tehlikeli kişi listesinin oluşturulması ve bu kişilere tek tip muamele gösterilmesine yol açmaktadır. Bu teknolojiler, belirli gruplar halinde kategorize edilmiş verilere dayanır ve "tehlikeli kişiler" grubuna dair genel çıkarımlarda bulunur. Olayın şartları ve failin özellikleri irdelenmeden, istatistiksel bir şekilde fail bu gruplardan biri ile ilişkilendirilir. Dolayısıyla profilleme puanı verilirken kararın bireyselleştirilmesi söz konusu değildir. Oysa fail, ait olduğu iddia edilen gruptaki herkesle birebir aynı özellikleri

sergilemeyecektir[514]. Bu nedenle pek çok kişinin verisi üzerinden genellemeler yapılarak oluşturulmuş ve geleceğe yönelik riskleri belirten sonuçların, bireylere doğrudan uygulanması, güvenlik tedbirlerinin amaç ve araçları ile uyumlu değildir.

Profilleme teknolojilerinin kullanımı sonucunda kişiler gelecekte suç işleme ihtimalleri üzerinden kimi zaman daha uzun süreli cezalar almakta veya belirli kurumlarda gözetim altında bırakılmaktadır. Kimi zaman bu puanlar infaz rejimine etki etmekte, koşullu salıverilmenin reddedilmesi veya örneğin kişinin kapalı cezaevine sevk edilmesi gibi sonuçlar doğurmaktadır. Ancak bu durum topluma yeniden kazandırma amacı gütmemekte, bu tedbirleri "toplumun düşmanlarına karşı" kefaret ödetici cezalara dönüştürmektedir[515]. Bununla birlikte güvenlik tedbirlerinden farklı fonksiyona sahip cezalar, gelecekte işlenecek fiillere yönelik verilemez. Gelecekte gerçekleşmesi yalnızca ihtimal dâhilinde olan hareketler için kişiye hapis cezası verilmesi veya koruma tedbirlerinin kalıcı hale gelecek şekilde uygulanması ceza hukuku sistematiği açısından mümkün değildir. Aksi bir yorum, kişilerin suç yoluna girmeden cezai sorumluluğunun kabul edilmesi anlamına gelir.

Güvenlik tedbirlerinin işlenen suçtan ziyade gelecekte işlenecek suçları engellemeye odaklandığı görülmektedir. Oysa kişilerin gelecekte bir tehlike doğuracağını kesin olarak tespit etmek mümkün değildir. Dolayısıyla kesin olmayan bu tehlikeyi bertaraf etmek için kullanılacak araçlar, ölçülülük ilkesi gereği gerekli ve elverişli olmalı, hak ve özgürlüklere orantısız şekilde müdahale etmemelidir. Gelecekte gerçekleşmesi yalnızca bir ihtimal olan suç tehlikesine karşı güvenlik tedbirlerini orantılı kılan, sevk edilen araçların iyileştirici, yeniden sosyalleştirici nitelikte olmasıdır. Ancak profilleme teknolojilerinin vardıkları sonuç üzerine verilen ceza niteliğindeki tedbirler ölçülülük ilkesinden uzaklaşmaktadır. Öncelikle profilleme teknolojilerinin suç oranını azaltma hususunda başarılı ve gerekli bir yöntem olduğu henüz kanıtlanmamıştır[516]. Bu amaca ulaşmada profilleme teknolojilerini sevk ederek kişileri özgürlüklerinden men etmenin diğer yöntemlere göre daha elverişli olduğunu söylemek mümkün değildir. Suç işlenmesini önlemek ve kamu düzenini korumak adına belirli kişilerin soyut tehlikelilik halinin gerekçe

[514] Melissa Hamilton, "Back to the Future: The influence of Criminal History on Risk Assessments", **Berkeley Journal of Criminal Law**, Cilt:20, Sayı:1, 2015, ss. 75-134, s.118, 119.
[515] Hamilton, "Back to the Future", s.116.
[516] Hamilton, "Back to the Future", s.118.

gösterilerek ikincil hapis cezası niteliğindeki tedbirlere maruz bırakılmaları amaç ile araç arasında bir orantısızlık olduğunu göstermektedir. Nitekim, profillemeye konu kişilerin hepsi itiyadi suçlu, akıl hastası veya alkol bağımlısı değildir. Çoğu durumda bu teknolojiler, kusur yeteneği olan ve işledikleri suçun karşılığında zaten ceza sorumluluğu doğabilecek kişilere de uygulanmaktadır. Bu kişilerin salt profilleme teknolojilerinin yaptığı değerlendirmeler nedeniyle daha uzun süre hapis cezası çekmeleri veya sürekli gözetim ve ek yaptırımlara maruz bırakılmaları, geleneksel güvenlik tedbirleri ile öngörülen suçu önleme ve failleri yeniden topluma kazandırma amacının dışına taşmaktadır. Kimi zaman işledikleri hafif suçlar hatta kabahatlerle kimi zaman ise henüz suç dahi işlemeden profilleme teknolojilerine konu olan kişilere yönelik verilen tehlikelilik puanları, aldıkları cezalara ek olarak ev, iş başvuruları, kredi veya devlet yardımı almaları gibi pek çok alanda hayatları boyunca yeniden karşılarına çıkmaktadır. Dolayısıyla bu kişilerin sisteme kazandırılması değil, aldıkları kötü puan nedeniyle "değişmez suçlu" kategorisinde tutularak "sıfır tolerans" politikasına maruz bırakılmaları söz konusudur[517]. Bu tür bir daimi cezalandırma ve toplumdan dışlama politikasının, demokratik toplumda gerekli, elverişli ve orantılı olduğunu iddia etmek mümkün değildir.

Profilleme teknolojileri failin tehlikeliliğini dikkate alarak sevk edilmeleri ve özgürlüklere müdahale içeren yaptırımlara yol açmaları bakımından güvenlik tedbirlerine yaklaşmaktadır. Ancak profilleme teknolojilerinin güvenlik tedbirlerinin uygulanmasını meşru kılan iyileştirici, eğitici, topluma kazandırıcı araçlardan yoksun olduğu, daha ziyade kalıcı şekilde damgalama ve toplumdan uzaklaştırma amacıyla kullanıldıkları görülmektedir. Bunun yanı sıra kanunda açıkça öngörülmeden uygulandıkları, kimi durumlarda kişilerin henüz işlediği bir suç dahi söz konusu olmadan tehlikelilik tespiti yaptıkları, bireyselleştirme yapmaksızın istatistiksel genellemelere dayandıkları, tüm bu nedenlerle güvenlik tedbirlerinden farklılaştıkları görülmektedir.

Profilleme teknolojileri bu bağlamda ne koruma tedbiri olarak değerlendirilebilmekte ne de bir güvenlik tedbiri olarak ele alınabilmektedir[518]. Ancak

[517] Sıfır tolerans politikası ve belirli grupların toplumdan daimi şekilde soyutlanmasına yol açması üzerine bkz. Tyler/Jackson/Mentovich, s.608-610.

[518] Bunları ceza muhakemesi tedbirleri ile güvenlik tedbirleri arasında yer alan, "önceye alınmış ceza yaptırımları" şeklinde nitelendiren görüş için bkz. Erman,"Ceza Hukukunun Dönüşümü", s. 471.

pek çok ülkede ceza muhakemesinde kullanılmaya devam etmekte ve vardıkları sonuçlar, karar ve hükümlerde değerlendirilmektedir. Mahkemelerin profilleme teknolojilerinin vardıkları sonuçları farklı şekilde değerlendirdiği, bu hususta açık düzenleme eksikliğinin farklı sonuçlara varılmasına yol açtığı görülmektedir. Bunları ara kararlara veya hükme esas almayan mahkemeler bulunduğu gibi ilgili teknolojilerin vardıkları sonuca dayanarak hüküm kuran mahkemeler de bulunmaktadır. Mahkemelerin risk değerlendirme teknolojilerinin delil değerine ilişkin yaklaşımlarını irdelemek ve bu hususta uygulamanın yeknesak hale getirilmesine katkıda bulunmak adına bir sonraki bölümde profilleme teknolojilerinin vardıkları sonuçların ceza muhakemesindeki delil değeri üzerinde durulacaktır.

III. PROFİLLEME TEKNOLOJİLERİNİN DELİL NİTELİĞİ

A. Delil Kavramı

Ceza muhakemesi, iddianın sunduğu tez ile savunmanın ileri sürdüğü antitezi dikkate alarak sentez yapan mahkemeler aracılığıyla maddi gerçeğe diyalektik şekilde ulaşılmasını sağlayan bir süreçtir[519]. Çözülmesi gereken uyuşmazlığın maddi ve hukuki olmak üzere iki kısmı bulunur. Diyalektik yöntemle, kolektif şekilde çözülecek kısım, uyuşmazlığın maddi meseleyi ilişkilendiren kısmıdır[520]. Maddi mesele çözülürken, mahkeme, iddia ve savunmanın sürece katılmasını sağlamak zorundadır. Bu süreç ile ilk olarak itham edilen eylemin işlenip işlenmediği, ikincil olarak işlenmiş ise sanık tarafından işlenip işlenmediği tespit edilecektir[521]. Hâkim maddi hususu sabit görmesi üzerine, bir hükme varacaktır. Hâkimin hükme varması, maddi meseleyle ilgili iddia veya müdafaanın hakikate uygun veya aykırı olduğu yönünde kanaatini ifade eder. Bu hükümle birlikte taraflar iddia ve müdafaalarını ispat etmiş veya edememiş olmaktadır[522]. Ancak maddi uyuşmazlığın gerçeğe uygun şekilde çözülmesiyle hukuki uyuşmazlığın doğru çözülmesi mümkün olabilir. Maddi uyuşmazlık çözüldükten sonra varılan sonuca, hukuk normlarının uygulanması, uyuşmazlığın hukuki boyutunu oluşturur[523].

Maddi uyuşmazlık ya da maddi sorun, geçmişte gerçekleştiği ileri sürülen bir olaydır. Bu bağlamda hâkim, muhakeme sonunda maddi meseleyi çözmek için adeta bir tarihçi gibi, önceden gerçekleşmiş olayı yeniden yaşatacak, "geçmişin bulutları arasından hakikatı görmeğe çalışacaktır"[524]. Bunu yapabilmenin tek yolu bugün var olandan yola çıkmak ve varlığını duyularımızla algılayabildiğimiz delillere başvurmaktadır. Deliller, taraflar bakımından ispat, hâkim bakımından ise sabit görme denilen faaliyetler için kullanılan araçlardır[525]. Dolayısıyla deliller, ceza

---

[519] Faruk Erem, "Ceza Usulünün Temeli", **Yargıtay Dergisi**, Cilt:10, Sayı:4, Ekim 1984, s.395-399, s. 399.
[520] Nurullah Kunter**, Ceza Muhakemesi Hukuku**, Beta Yayınevi: İstanbul, 1998, s.584.
[521] Fatih Birtek, **Avrupa İnsan Hakları Mahkemesi, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat**, Adalet Yayınevi: Ankara, Kasım 2017, s.9, 10.
[522] Kunter, **Ceza Muhakemesi Hukuku**, s.584.
[523] Yaprak Öntan, **Ceza Muhakemesi Hukukunda Bilirkişilik**, Ankara Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Ankara 2011, s.4
[524] Kunter, **Ceza Muhakemesi Hukuku**, s.585.
[525] Kunter, **Ceza Muhakemesi Hukuku**, s.584.

uyuşmazlığına konu olayı temsil ederek mahkeme önünde canlandırılmasını sağlar, birer yapboz parçası gibi ceza muhakemesinde resmin bir araya getirilmesine katkı sunar[526]. Soruşturma evresinin başlangıcında bulunan şüphe bu yolla kovuşturma evresine geçildiğinde yenilir. Ceza muhakemesinin delil olmadan başlaması mümkün olmadığı gibi, ilerlemesi de delil olmadan mümkün değildir. Kovuşturma nihayetinde hükme "delil" olarak adlandırılan ispat araçları vasıtasıyla varılacaktır[527].

Doktrinde soruşturma aşamasında toplanan verilerin delilden ziyade şüphe sebebi olduğunu, delil kavramının ise ancak kovuşturma aşamasında mahkeme tarafından doğruluğu, güvenilirliği ve olayla ilgisinin tespit edilmesi üzerine kullanılabileceğini söyleyen görüşler bulunmaktadır. Örneğin Kunter, delilerin muhakeme sonunda meseleyi çözen hâkimin başvurduğu bir vasıta olduğunu, yalnızca kovuşturma aşamasında başvurulan araçlara delil denilebileceğini belirtmektedir. Kunter'e göre soruşturma sürecinde, delilden ziyade "şüphe sebebi" söz konusudur[528]. Bununla birlikte günümüzde, soruşturma aşamasında şüphe sebebini gösteren olguların da delil olarak addedilebileceği yönünde karşı görüşler bulunmaktadır. Buna gerekçe olarak, bütün ispat araçlarının delil olduğu, ceza muhakemesinin delil olmadan başlayamayacağı, yine delil olmadan ilerleyemeyeceği gösterilmekte, bir şeyin delil vasfını haiz olması ile delil olarak hükme esas alınması değerlendirmelerinin farklı değerlendirmeler olduğu belirtilmektedir[529]. Dolayısıyla, soruşturma evresinde de olayı temsil eden deliller araştırılır, ancak bunların müşterek şekilde değerlendirilmesi kovuşturma aşamasında gerçekleştirilecektir[530]. Bununla birlikte, soruşturma aşamasında maddi gerçeğe ulaşma amacı güdüldüğü, bu aşamada da elde edilen bulguların gerek savcı gerek hâkim tarafından değerlendirmeden geçirildiğini söylemek mümkündür. Nitekim koruma tedbirlerini düzenleyen m. 100/1, 138, 134 gibi pek çok hükümde "kuvvetli suç şüphesinin varlığını gösteren somut delillerin varlığı" aranmıştır. Dolayısıyla ulaşılan bilgi ve belgelerin, kuvvetli şüpheyi

[526] Centel, **Ceza Muhakemesi Hukuku**, s.255.
[527] Ali Can Buğdaycı, **Önleyici Kolluk Faaliyeti Esnasında Elde Edilen Bilgiler ve Bunların Ceza Muhakemesindeki Delil Değeri**, Ankara Yıldırım Beyazıt Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Ankara, Nisan 2019, s. 95.
[528] Kunter, **Ceza Muhakemesi Hukuku**, s.585.
[529] Cumhur Şahin/Neslihan Göktürk, **Ceza Muhakemesi Hukuku II**, Seçkin Yayınevi: Ankara, 11. Baskı, Şubat 2021, s.29.
[530] Centel/Zafer, s.256.

destekleyecek düzeye erişip erişmediği, gerçeği yansıtan bir delil olarak kabul edilip edilemeyeceği ele alınmış olmaktadır[531].

Delil kavramı delil kaynağı ile karıştırılmamalıdır. Delil kaynağı bünyevi iken delilin fonksiyonel niteliği vardır[532]. Delil kaynağı, olayı temsil gücü olabilecek ve muhakeme makamları tarafından incelenecek bir beyan ya da bilgi sunan varlıktır, bunlar delilin ulaşıldığı yeri gösterir. Delil kaynağı bir kişi veya eşya olabilir. Bu bağlamda yine tanık beyanı delil iken, tanık delil kaynağıdır. Kaynak üzerinden delil bir kere elde edilmekle birlikte, kaynağın yok olması, bu bağlamda tanığın vefat etmesi, delili geçersiz kılmayacaktır[533].

Delilin muhtevası da delilin kendisinden farklı bir kavramdır. Bir tehdit mektubu belge delili iken, mektubun içeriği delilin muhtevasıdır[534]. Yine parmak izi açısından, parmak izindeki çizgi ve boğumlar delilin muhtevası, parmak izini veren kişi delilin kaynağı ve son olarak parmak izi delili teşkil eder[535].

Son olarak delilin içeriğini öğrenmek veya değerlendirmek için başvurulan araçlar delil ile karıştırılmamalıdır. Bunlar maddi olayın öğrenilmesine hizmet etmelerine rağmen delilin içeriği veya değerini öğrenme araçlarıdır[536]. Delilin içeriğinin öğrenilmesi, bilimsel veya teknik bilgi gerektirdiğinde ya da delilin değerlendirilmesi sırasında bir uzmana başvurma ihtiyacı doğurduğunda, delil değerlendirme araçları kullanılır[537]. Örneğin ceset üzerinde bulunan yara izi, kan izi, kurşun izi delildir. Ancak kimi durumlarda bunların anlamlandırılması ve olayın aydınlatılması için teknik bilgiye ihtiyaç duyulur. Bu bağlamda uzman bilirkişi tarafından yapılan inceleme delili anlamaya yardımcı olan, delili değerlendirme aracıdır[538]. Hâkimin özel ve teknik bilgisi olsa dahi, hukuk dışı bir alanda delilin aydınlatılması ve herkes tarafından anlaşılması için bu araçlara başvurulması gerekir. Delil değerlendirme araçları maddi olayın bir parçası değildir. Yalnızca gerçeğe

---

[531] Birtek, s.20, 21.
[532] Kunter, **Ceza Muhakemesi Hukuku**, s. 585.
[533] Birtek, s.22, 23.
[534] Kunter, **Ceza Muhakemesi Hukuku**, s. 585.
[535] Birtek, s. 23.
[536] Kunter, **Ceza Muhakemesi Hukuku**, s.585.
[537] Öntan, s. 5.
[538] Birtek, s. 25.

ulaşabilmek için maddi bulguların anlaşılmasında "köprü" görevi gösterir[539]. Bununla birlikte bilirkişi başlığı altında daha detaylı tartışılacağı üzere doktrinde "delil değerlendirme aracı" olarak sınıflandırılan "bilirkişi" ve "keşif" kavramlarının "belirti delili" altında ele alan görüşler de bulunmaktadır[540].

Ceza Muhakemesi hukukunda delil serbestisi ilkesi geçerlidir. Bu ilkeye göre bir hususun mutlaka belirli tip delillerle ispatlanmasını gerektiren kurallar bulunmamaktadır. Hukuksal özellikleri haiz her şey delil olabilir[541]. Dolayısıyla bu ilke, her şeyin delil olması, her şeyin her şeyle ispat edilebilmesi ve her zaman delil olarak sunulabilmesini ve serbestçe değerlendirilebilmesini içerir[542]. Nitekim ceza muhakemesi sırasında ispat edilecek olay, muhakemeden önce gerçekleşmiştir ve olayların ortaya çıkış zamanı ile şartlarının önceden bilinmesi mümkün değildir. Bu nedenle olayları gösterecek deliller, şekli sınırlamalarla kısıtlanmamalıdır. Her şey her zaman kanıt olarak sunulabileceği gibi, hâkimin delilleri kendiliğinden araştırması da mümkündür. Hâkimin tespitini belirleyecek üstün bir delilden de söz edilemez. Amaç maddî gerçeğe ulaşarak adaleti tesis etmek olduğundan, somut olayın ispatına yarayan her türlü vasıtayı değerlendiren hâkim bu vasıtalardan hangisini kabul edeceğini serbestçe takdir edecektir[543]. Ancak delil ve delilleri değerlendirme serbestliği elbette sınırsız değildir. Akılcı bir anlayışla, ispat edilmesi istenen olaylar tetkik edilmeli, lehte ve aleyhte tüm hususlar değerlendirilmelidir. Bunun yanı sıra her şey delil olarak değerlendirilebilmekle birlikte delil olarak hükme esas alınabilecek şeylerin belli nitelikleri barındırması gerekir[544].

Bu niteliklerden ilki delillerin gerçekçi olma özelliğidir. Delil kişilerin iç dünyasına değil, beş duyu ile algılanabilir gerçeğe işaret etmelidir. Dolayısıyla,

---

[539] Birtek, s.218.
[540] Centel/Zafer, s. 321.
[541] Ünver/Hakeri, s.1453.
[542] Şahin/Göktürk, **Ceza Muhakemesi Hukuku II**, s.32. Bununla birlikte Centel/Zafer duruşmanın akışının ispatında yasal delil sisteminin benimsendiğini, duruşmanın usulüne uygun şekilde yapılıp yapılmadığının ancak tutanakla ispat olunabileceğini vurgulamaktadır, bkz. Centel/Zafer, s. 255, 256.
[543] Ferhat Karabulut/Ersin Karapazarlıoğlu/Hamza Tosun,"Ceza Muhakemesinde Delil Kavramı ve Kovuşturma Sürecinde Hâkimlerin Delil Algısı", **Türkiye Barolar Birliği Dergisi**, Sayı:120, 2015, ss. 385-422, s.390.
[544] Kunter, **Ceza Muhakemesi Hukuku**, s.586, 587.

düşünülen, imgelenen değil dış dünyada var olan, algılanabilen ve duyumsanabilen şeyler delil olabilir[545].

Bunun yanı sıra delillerin akılcı olması gerekir. Ancak akla ve hakikate uygun olarak ifade edilen şeyler delil olarak kabul edilebilir. Bilim tarafından kabul görmeyen, hurafe niteliğinde, rasyonel nitelik taşımayan hiçbir şey delil olarak kabul edilemeyecektir[546]. Nitekim delillerin saplantı ve ön yargılardan uzak ve hayatın olağan akışına uygun olması[547], maddi gerçeğin aydınlatılması için büyük önem taşımaktadır. Maddi olay akla, bilime ve tecrübe kurallarına aykırı olacak şekilde değerlendirildiği takdirde hatalı değerlendirilmiş olacak ve adaletin tesisi mümkün olamayacaktır.

Bunun yanı sıra deliller, soruşturmaya konu olayın bütününü ya da bir parçasını temsil ediyor olmalıdır[548]. Olay ile ilgisi kurulamayan verilerin delil değeri yoktur. Bu nedenle öncelikle maddi olayı yeniden canlandırabilmek ve değerlendirebilmek için hangi hususların tespit edilmesi gerektiği belirlenmeli, ardından bunlarla ilişkili olan şeyler delil olarak değerlendirilmelidir. Aksi halde "maksada elverişlilik" söz konusu olmayacaktır. CMK m. 206/2 (b) bendinde bu husus "delil ile ispat edilmek istenilen olayın, karara etkisi yoksa" reddolunacağı şeklinde düzenlenmiştir. Nitekim olayla ilgisi olmayan hususlara yer verilmesi olayı temsil etmez, ancak faile yönelik şüphe yaratabilir. Bu tür bir şüphe, objektif kanaate gölge düşürebilir. Yine olayı temsil edicilik unsuru ile ilişkili olarak Ceza Muhakemesi Kanunu tasarısında m. 218'de "sanığın tavır ve hareketine ilişkin açıklamayı içeren belgeler dosyada yer alsa da duruşmada okunamaz" hükmüne yer verilmiş, ancak bu hüküm kanunlaşmamıştır[549]. İlgili madde sanık hakkındaki güvenlik soruşturması ve benzeri nitelikte belgelerin okunması ve bu yolla mahkemelerin etkilenmesini önlenmek amacıyla

[545] Birtek, s.56, Şahin/Göktürk, Ceza Muhakemesi Hukuku II, s. 34. Bir ispat aracına delil diyebilmek için "akla, yani bilime, maddi gerçeğe ve hukuka uygun" olması gerektiği, gerçeğin "akla uygun ve realist, olayın bütünü veya bir parçasını temsil eden kanıtlar" veya bunların bir bütün olarak ele alınması ile tespit edilebileceğine dair, bkz. Yargıtay 6. CD, E. 2020/207, K. 2020/4968, T. 15.12.2020, https://lib.kazanci.com.tr/.
[546] Kunter, Ceza Muhakemesi Hukuku, s. 588, Yenisey/Nuhoğlu, s 514.
[547] Birtek, s. 57.
[548] Ünver/Haker, s. 1454, Yenisey/Nuhoğlu, s.514.
[549] Birtek, s. 52, dipnot 212.

düşünülmüştür[550]. Temsil edicilik unsuru ayrıca delilin sağlam, yani güvenilir olmasını gerektirir. Doğru ve inandırıcı olmayan bir delilin olayı temsil ettiği kabul edilemeyecektir. Kural olarak delilin sağlamlığını hâkim takdir etmekle birlikte, kimi durumlarda kanun koyucu da bir belgenin güvenilir bir delil olmayacağını önceden belirleyebilir. Örneğin mülga 1412 sayılı Ceza Muhakemeleri Usul Kanunu'nda 249. maddede "maznunun tavru hareketine dair şahadetnameler müstesna olmak üzere" denilerek, kişiye ait iyi hal belgelerinin güvenilmezliği öngörülmüş, bunlar duruşmada okunacak belgelerin ve raporların dışında tutulmuştur[551]. Delillerin sağlamlığı kendi içinde ve ayrıca diğer delillerle birlikte ele alınarak değerlendirilmektedir. Delil sağlamlığı mahkemenin takdirinde olmakla birlikte, iddia ve savunmanın da delil tartışma sürecine katılması, bu sağlamlığın teyit edilmesi açısından önem arz etmektedir. Nitekim bir sanığı suçlayan tanık beyanı veya diğer deliller gerçek dışı düzenlenmiş veya hatalı olabilecektir. Savunma eğer ifade verenin veya ifadenin içeriğinin güvenilirliğini sınayamaz veya sınamasına izin veren bilgilerden yoksun kalırsa, delilin sağlamlığını aydınlatmak mümkün olmayacaktır. Bu bağlamda ifade sahiplerinin düşmanca tutumları ve önyargılı olduklarını ortaya koyabilmek veya ifade içeriğini diğer delillerle çürütebilmek için savunmaya eşit silahlar tanınmalıdır[552]. Örneğin duruşmada bulunmayan delil kaynaklarının, hâkim önünde sorgulanmasını gösteren video kaydının iddia ve savunmayla paylaşılması, böylelikle beyanı alınan kişinin gözlemlenmesinin mümkün kılınması silahların eşitliği için önemlidir. Yine tanığın anlatımlarının, diğer tanıklar, adli tıp delilleri veya uzman raporu ile teyit edilmesi delillerin sağlamlığını tespit açısından gereklidir[553].

Delillerin diğer bir vasfı da erişilebilir olmalarıdır[554]. Bir bulgu ancak ulaşılabildiği takdirde olayla ilgisi, doğruluğu, güvenilirliği, kısaca ispata elverişliliği değerlendirilebilecektir. Mahkemece bilinmeyen hususların delil olarak kabul

---

[550] Ayrıntı için bkz. Türkiye Barolar Birliği tarafından oluşturulan CMUK Tasarısı Hakkında Komisyon Tarafından Hazırlanan Genel Gerekçe, http://tbbyayinlari.barobirlik.org.tr/TBBBooks/2004_cmuk_taslak.pdf, Erişim Tarihi:15.07.2021

[551] Kunter, **Ceza Muhakemesi Hukuku**, s. 590.

[552] Anayasa Mahkemesi, Atila Oğuz Boyalı Başvurusu, Başvuru No: 2013/99, Karar T.: 20.3.2014, para. 55, Anayasa Mahkemesi Sebahat Tuncel Başvurusu, Başvuru No: 2014/1440, Karar T. 26.02.2015, R.G. Sayı: 14.03. 2015- 292294, para. 95, https://kararlarbilgibankasi.anayasa.gov.tr, Balta ve Demir/Türkiye, Başvuru No. 48628/12, 23.06. 2015, para. 58, https://hudoc.echr.coe.int/, Erişim Tarihi: 15.07.2021.

[553] Sibel İnceoğlu, **Adil Yargılanma Hakkı: Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-4**, MRK Baskı: Ankara, Nisan 2018, s.354.

[554] Centel/Zafer, s.259, Birtek, s.61, Şahin/Göktürk, **Ceza Muhakemesi Hukuku II**, s. 34.

edilmesi mümkün değildir. Ancak zorunlu hallerde, bir kez değerlendirilmesinin ardından erişilemeyen beyan ve bulguların, kendileri yerine bunlara ilişkin tutanakların okunması kabul edilmektedir. Bu durumda yine okunan tutanakların, doğruluğu ve sağlamlığını tartışma imkânı tanınmış olacak, bu tutanaklar vicdani kanaate esas alınabilecektir[555].

Delilin en önemli unsurlarından biri de müşterek (kolektif) olma unsurudur. Delile sadece hâkim tarafından erişilmesi yeterli değildir. İddia ve savunmanın da delilleri öğrenmesi ve kolektif olarak hüküm verme sürecine katılmaları gerekir. Delilin müşterek olmasından, taraflarla paylaşılması ve tüm süjeler ile birlikte tartışılması anlaşılmalıdır. Aksi halde hâkim, olay hakkında salt kendi çıkarımına göre karar verecek, kanaatini duruşma dışında edinmiş olacaktır. Bu anlamda, delilin müşterekliği, hâkimin kanaatini yalnızca duruşmadan edinmesini gerektiren "hâkimin şahsi bilgisine dayanmaması ilkesi"[556] ile yakından ilintilidir. Bununla birlikte bu unsurun sağlanması için delillerin duruşmada sunulmasının tek başına yeterli olmadığı göz önüne alınmalıdır. Delilin duruşmada ikamesi, doğrudan doğruyalık ilkesini karşılamaya yeterli olmakla birlikte, bu durum delillerin tartışıldığı anlamına gelmemektedir. Ceza muhakemesinin özünü oluşturan diyalektik yöntem için, tarafların görüşleri alınmalı, bu görüşlerin birbirleri ile çarpışması ile bir sentez oluşturulmalıdır[557]. Bu nedenle müştereklik unsuru, savunma hakkının ve adil yargılanmanın temelini oluşturur. Yargı kararlarında da bu unsura dayanılarak, "dosya içinde bulunmayan ve duruşmalar sırasında tartışılmayan iletişimin tespiti tutanaklarının hükme esas alınması"[558], "ifade tutanağına 'özet' halinde geçirilen whatsapp mesajlaşma kayıtlarının, görüşme tarihleri, saatleri belirtilerek, ayrıntılı diyaloglar şeklinde, ekran görüntülerine de yer verilerek denetime olanak verecek şekilde" dosyaya konulmadan ve duruşmada okunmadan, dolayısıyla sanığın görüşü

[555] Birtek, s.62, 63. CMK m.211'de sayılan hallerden, tanık veya sanığın suç ortağının ölmüş olması veya akıl hastalığına tutulması veya bulunduğu yerin öğrenilememesi zorunlu hallere örnek olarak verilebilir. Bununla birlikte doktrinde, erişilebilirliğin kimi zaman uluslararası adli yardımın başarılı olmaması gibi sebeplerle mümkün olmayabileceği, bununla birlikte ulaşılamıyor olmasının ilgili ispat aracının delil olmadığı şeklinde değerlendirilemeyeceğini ileri süren görüşler de bulunmaktadır, bkz. Ünver/Hakeri, s. 1454.

[556] Kunter, **Ceza Muhakemesi Hukuku**, s. 591.

[557] Birtek, s. 64.

[558] Yargıtay 10. CD, E. 2020/1651, K. 2021/3431, T. 11.03.2021, https://lib.kazanci.com.tr/, Erişim Tarihi: 16.07.2021.

alınmaksızın hüküm kurulması[559], "mağdure ifadesi ile CD görüntüleri arasında farklılıklar mevcut olmasına rağmen, olayın tek tanığı konumunda bulunan mağdurenin" duruşmaya getirilmeden ve çelişki giderilmeden eksik araştırma ile hüküm kurulması[560] karşısında, kurulan hükümlerin bozulduğu görülmektedir. Hâkimin delilleri serbestçe tayin yetkisi sınırsız değildir ve hâkim vicdani kanaatini, CMK m. 217 ile açıkça düzenlendiği üzere, ancak duruşmaya getirilmiş ve tartışılmış delillere dayanarak oluşturabilir. Kimi durumlarda delil değerlendirme araçlarına başvurulması de delilin müşterekliği unsuru ile ilintilidir. Nitekim delilin muhtevasının anlaşılmasının teknik bilgi gerektirdiği durumlarda, delilin gerçek anlamda tartışılabilmesi için bilirkişiye müracaat edilmesi zorunludur. Delilin içeriğinin mutlaka iddia, savunma ve yargı makamları tarafından anlaşılabilmesi gerekir. Aksi halde, gerçek anlamda bir savunma veya karşı iddiada bulunmak mümkün olmayacaktır[561]. Bu nedenle sağlamlığının incelenmesi uzmanlık gerektiren dijital kayıtlar hakkında sadece kolluk tarafından yapılan teknik tespitlerle yetinilerek ve inceleme tutanaklarının savunma ile paylaşılmaksızın hükme esas alınması, Anayasa Mahkemesi tarafından silahların eşitliği ilkesi ve adil yargılanma hakkının ihlali olarak kabul edilmiştir[562].

Müştereklik unsuru soruşturma aşamasında gizlilik ilkesi uyarınca kimi zaman gerçekleştirilememektedir. Her ne kadar CMK m.157, savunma hakkına zarar vermemek koşuluyla usul işlemlerinin gizli yapılacağını belirtse de CMK m.153 kapsamında müdafiin soruşturma amacını tehlikeye düşürmemek için dosya içeriğini inceleme ve belgelerden örnek alma yetkilerinin kısıtlanabildiği ve kimi işlemlerin gizli yürütülebildiği görülmektedir. Bu durum müştereklik unsurunun, soruşturma evresinde her zaman karşılanamadığını göstermektedir. Ancak aleniliğin zorunlu olduğu kovuşturma evresinde bu unsur mutlaka tesis edilecektir. Aksi halde CMK m. 216 ve 217 gereği, hâkim iddia ve savunma ile duruşmada paylaşmadığı ve huzurunda tartışılmayan delillere dayanarak hüküm kuramaz[563]. Dolayısıyla, ferdi hükmün

[559] Yargıtay 10. CD, E.2021/2849, K.2021/5922, T. 24.05.2021, https://lib.kazanci.com.tr/, Erişim Tarihi: 16.07.2021.
[560] Yargıtay 14. CD, E. 2020/4256, K. 2021/2398, T. 25.3.2021, https://lib.kazanci.com.tr/, Erişim Tarihi: 16.07.2021.
[561] Birtek, s.65.
[562] Anayasa Mahkemesi, Başvuru no: 2014/253, Karar T.: 9.1.2015, para 55, 76, 77, https://www.resmigazete.gov.tr/eskiler/2015/05/20150512-12.pdf, Erişim Tarihi: 17.07.2021.
[563] Birtek, s. 66.

verilmesi tek bir süjenin elinde olmakla birlikte, kolektif hükmün geçerliliği, ancak farklı süjelerin sürece katılabilmesi ile mümkündür[564].

Son olarak delil hukuka uygun elde edilmiş olmalıdır. Deliller maddi gerçeğin bulunmasına hizmet ederler. Bununla birlikte hümanist ceza hukuku, bu gerçeğin ne pahasına olursa olsun elde edilmesine izin vermemekte, kişi onuru, hak ve özgürlüklerini korumak adına belirli sınırlar öngörmektedir. Delillerin hukuka uygun şekilde toplanmış olması, delil serbestisi açısından en önemli sınırlardan biridir. Delil toplama sürecinin, kanunda öngörülmüş usul ve güvencelere uygun şekilde yapılmış olması, şüpheli ve sanık için olduğu kadar, hukuk devletinin tesisi için de büyük önem arz etmektedir. Hukuka aykırı deliller, temsil edici olsa dahi mahkeme tarafından değerlendirilemez ve hükme esas alınamazlar. Kimi deliller konu bakımından yasaklanmıştır. Örneğin CMK m. 47 kapsamında konunun devlet sırrı olması halinde tanık beyanı açısından özel düzenleme öngörülmüştür. Kimi durumda anayasal temel hakları korumak amacıyla bazı yasaklar öngörülmektedir. Anayasa m. 38 gereği kimsenin kendisini ve kanunda gösterilen yakınlarını suçlayacak beyanda bulunmaya ve bu yönde delil göstermeye zorlanamaz. Bunun yansıması, örneğin belli tanıklara çekinme hakkı tanınması ve m.210/2 gereği tanıklıktan çekinebilecek olan kişinin, duruşmada tanıklıktan çekindiğinde, önceki ifadesine ilişkin tutanağın okunamaması gibi hükümlerde görülmektedir[565]. Son olarak bazı deliller, elde edilmeleri için başvurulan metot dolayısıyla yasaklanmıştır. Hukuka aykırı elde edilmiş delillerin değeri Anglosakson hukukunda ve Kıta Avrupası'nda farklı şekillerde değerlendirilse de CMK kapsamında m. 206/1 (a) ile kanuna aykırı olarak elde edilmiş delillerin duruşmada ortaya konulamayacağı, yine CMK m.217/2 kapsamında hukuka aykırı delillerin hükme esas alınamayacağı açıkça öngörülmektedir[566].

B. Delil Türleri

Deliller doktrinde farklı şekillerde sınıflandırılmışlardır. Kunter delilleri temel olarak asli (somut) olaya ilişkin deliller ve genel mahiyette deliller olarak ikiye ayırmaktadır. Asli olaya ilişkin deliller, bugün ana hatlarıyla kabul gören doğrudan-

[564] Keyman, Selahattin, **Ceza Muhakemesinde Savcılık**, Ankara 1976, s.24, 25'ten aktaran Birtek, s.64.
[565] Yenisey/Nuhoğlu, s.533.
[566] Yenisey/Nuhoğlu, s.532, Birtek, s.70, Şahin/Göktürk, **Ceza Muhakamesi Hukuku II**, s. 35.

dolaylı delil ayrımında, doğrudan deliller kavramına karşılık gelmektedir. "Tarihi deliller" de denilen somut olaya ilişkin bu deliller, beyan ve belge delilleri olmak üzere iki çeşittir. Bunlar ile kimi zaman tanık beyanında olduğu gibi dava konusu olayın nasıl cereyan ettiği hâkim huzurunda anlatılır, kimi zaman ise delil, belge delilinde olduğu gibi geçmiş olayın yerine geçer[567]. Bunlar doğrudan maddi vakıaya ilişkindir ve suçun bütün unsurlarını ve unsurların dışında kalan öğeleri ispatlamaya elverişlidirler. Sanığın itham edilen suçtan sorumlu bulunması ve hakkında mahkûmiyet kurulması için ispatlanması gereken her öge, asli olayın parçasıdır ve bunlar asli olaya ilişkin delillerle ispat edilir. Örneğin failin kastını da açığa çıkaran rüşvet anlaşmasının yapıldığı ana tanık olmuş kişinin beyanı, asli olayı ispatlayan bir delildir[568]. Yine, bir kişinin hırsızlık suçunu işlediğini itiraf ettiği ikrar beyanı ve nasıl işlediğini açıklaması, asli olayı işaret eden bir delildir.

Genel mahiyette deliller ise sadece kanıtlanacak hususu değil, başka hususları da ispatlarlar. Genel nitelikte olmaları nedeniyle bu delillerden faydalanmak için ayrıca bir araştırma yapılarak, ispat edilecek asli olayı temsil edip etmedikleri, sağlam olup olmadıkları ele alınmalıdır[569]. Genel mahiyette olan bu deliller, fiilin tipik anlamda gerçekleştiğini doğrudan göstermeyen, ancak şüpheli veya sanığın ilgili suçu işlediği şüphesini kuvvetlendiren yan olayları ispatlar. Bu olaylar, asli olaydan önce veya sonra gerçekleşebilir, bunun yanı sıra, asli olayı içeren "olaylar zincirini" genel mahiyette temsil eden bilgiler de içerebilir. Örnek olarak, maktulün evinde şüphelinin saç telinin bulunması, kasten öldürme fiili açısından ispat edilmesi gereken asli olayın, yani suçun unsurlarından birinin parçasını oluşturmamaktadır. Daha ziyade "belirti olay" (yan olay) söz konusudur. Belirti olayların ispatında yine araç olarak deliller kullanılacaktır ve bu delillerin de yukarıda ayrıntılarıyla ele alınan, delillerin taşıması gereken niteliklere sahip olmaları gerekir.

Bu bağlamda, beyan ve belge delilleri, kimi zaman asli olaya ilişkin olsa da, kimi zaman genel mahiyet taşıyabilirler. Örneğin, bir kişiye ateş edilmesine tanık olan kişinin beyanı ilk duruma örnek iken, şüpheliyi olay anından kısa süre önce suç aleti

---

[567] Kunter, **Ceza Muhakemesi Hukuku,** s.628.
[568] Erman, Barış,"Ceza Muhakemesi Hukukunda Belirti ve İspat Değeri", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Köksal Bayraktar'a Armağan, Cilt:9, Sayı:1-1, 2010, ss.679-701, s.692.
[569] Kunter, **Ceza Muhakemesi Hukuku**, s.628, 629.

ile gördüğünü açıklayan tanık beyanı belirti olayı nitelemektedir[570]. Bu tür yan olaylar, asli olaylara ilişkin olumlu ya da olumsuz çıkarım yapılmasını sağlar. Kimi zaman belirti olaylar bir araya gelerek, bir "belirtiler dizisi" oluşturur. Bu noktada birden fazla belirtinin birbirinden bağımsız olarak aynı yan olayı temsil etmesi söz konusudur[571]. Örneğin sanık ile maktul arası borç ödenmemesi nedeniyle gergin bir ilişki bulunması, daha önce de şiddete dönüşen kavgaya tutuşmuş olmaları, olay günü sanığın maktulün evinin yakında görülmesi, belirtiler dizisi oluşturur. Belirti dizisi, temel olayın iddia edildiği şekilde gerçekleştiğini tutarlılıkla gösterdiği takdirde, mahkemenin asli olaya ilişkin vicdani kanaat oluşturmasına katkı sunacaktır[572].

Bununla birlikte asli olay veya yan (belirti) olayı kanıtlayan deliller yerine bugün doktrinde ağırlıklı olarak doğrudan delil-dolaylı delil ayrımına başvurulmaktadır. Yukarıdaki ayrıma paralel şekilde, mahkemenin çözümlemesi gereken asıl olayı ispatlayan delillere doğrudan doğruya deliler, esas olaya bağlı olan yan olayları ispatlayan delilere ise dolaylı deliller, belirti delilleri veya delil başlangıcı[573] denilmektedir. Olay yerinde kan izi, saç teli, meni bulunması, sanığın iddia edilen suçu işlediğini doğrudan göstermemekle birlikte en azından olay yerinde bulunduğunu, dolayısıyla yan olayları ispat edecektir. Yan olayları gösteren bu deliller, doğrudan suçun unsurlarını ispata elverişli değildirler, ancak doğrudan delillerin temini ve temel olayın ispatına yardımcı olurlar[574]. Doktrinde dolaylı delillerin tek başına ispat aracı olmadığı, ancak başka delillerle tamamlanması halinde delil sayılabileceklerini ileri süren görüşler bulunmaktadır[575]. Ancak bu durum dolaylı delillerin delil niteliğini ortadan kaldırmamaktadır. Ayrıca, doğrudan delillerin söz konusu olduğu durumlarda dahi, vicdani kanaat için delillerin başka delillerle tamamlanması, olaya bütüncül şekilde bakılması için gerekebilir. Bir delilin tek başına olayı ispata elverişli olup olmadığı tartışması, kanuni delil sisteminde daha fazla önem arz etmektedir. Nitekim kanuni delil sisteminin öngörüldüğü durumlarda, hangi delillerin hâkimi bağlayıcı nitelikte oldukları açıkça düzenlenmiş, öngörülen bu deliller dışındaki delillere emare adı verilerek bunlar ancak birbirlerini takviye edip tamamladıkları takdirde delil olarak

---

[570] Erman, "Ceza Muhakemesi Hukukunda Belirti ve İspat Değeri", s.693.
[571]Eroğlu, Fulya, **Beden Muayenesi ve Vücuttan Örnek Alma Suretiyle Elde Edilen Dellilerin İspat Değeri**, Yeditepe Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul 2009, s, 7,8.
[572] Eroğlu, s.9, 10.
[573] Ünver/Hakeri, s. 1455.
[574] Centel/Zafer, s. 260, Ünver/Hakeri, s. 1455.
[575] Şahin/Göktürk, **Ceza Muhakemesi Hukuku II**, s. 29.

nitelendirilmiştir. Ceza Muhakemesi Kanunu kapsamında serbest delil sistemi öngörüldüğünden doğrudan ve dolaylı delillerin delil niteliği açısından bir farkı bulunmamaktadır. Bugün örneğin ana olayı yeniden canlandıran tanık beyanı da diğer delillerle desteklenmediği takdirde tek başına hâkimin kanaat oluşturmasında yeterli olmayabilir. Aynı durum bir aracın hızını göstererek dolaylı delil teşkil eden fren izi için de geçerlidir. Bir delilin tek başına kişinin cezai sorumluluğunu tespit etmede yeterli olmaması, genel veya yan olaya ilişkin olması, delil niteliğini zedelememektedir. Dolayısıyla serbest delil sisteminde ister doğrudan ister dolaylı olsun bütün ispat vasıtaları delildir ve delillerin üç çeşidi bulunmaktadır[576]. Bunlar, beyan, belge ve belirtidir.

Profilleme teknolojilerinin delil değerinin bulunup bulunmadığı, bulunduğu takdirde hangi delil çeşidi altında incelenebileceğini tespit edebilmek adına aşağıda kısaca delil türleri üzerinde durulacaktır.

1. Beyan Delilleri

Meydana gelen somut olaya ilişkin beş duyusu ile bilgi edinmiş tanık, mağdur, müşteki, şüpheli veya sanıkların yetkili makamlar karşısında yaptığı açıklamalar beyan delili olarak kabul edilir. Bu açıklamaların beyan delili olarak kabul edilebilmesi için mahkeme önünde yapılması veya soruşturma evresinde yapıldı ise mahkeme önünde tekrarlanmaları zorunludur[577].

a) Tanık beyanı

Tanık beyanı, olayın tanığı olmuş bir kişinin olay hakkında beş duyusu ile edindiği bilgileri mahkeme huzurunda ifade etmesidir. Tanık beyanının sözlü olması gerekir, bu nedenle kanunda "tanığın dinlenmesi" ifadesine yer verilir. Mahkeme, konuşulanı dinlemek, tanığı gözlemlemek ve çelişkileri ortaya çıkarabilmek için iddia ve savunmaya imkân tanımalıdır. Tanık delilinde önemli olan olaya dair detayların okunması değildir[578]. Bu nedenle yazılı bir beyanın mahkeme veya savcılığa teslimi,

[576] Kunter, **Ceza Muhakemesi Hukuku**, s. 629, 630, Birtek, s. 75.
[577] Centel/Zafer, s.284.
[578] Kunter, **Ceza Muhakemesi Hukuku**, s. 631, Ünver/Hakeri, s. 1480.

tanık beyanı olarak kabul edilmez, kural olarak tanık, yetkili makam önünde olayı sözlü anlatmalıdır[579].

Tanık beyanıyla ispat edilmek istenen gerçekleşmiş vakıalar ve koşullar olup, tanık tahmin ettiklerini ve çıkarımlarını değil, beş duyusu ile algıladığı durumları aktardığı takdirde beyanının, olayı temsil edici olduğu kabul edilmelidir. Dolayısıyla tanığın yorumu ve kişisel değerlendirmeleri değil, şahit olduğu olaylar dikkate alınmalıdır[580].

AİHM ise tanıklığı "sanığa isnat edilen fiil hakkında bilgi veren herhangi bir kişi" olarak kabul etmekte, bu bağlamda suç ortakları[581], mağdur, bilirkişi[582] de tanık olarak kabul edilebilmektedir.

Tanıklık aynı zamanda tanıklar açısından bir ödev olup Türkiye sınırları içerisindeki herkes tanıklık etmek zorundadır. CMK m. 43 ve 47. maddelerde cumhurbaşkanı açısından görülen istisna dışında, tüm tanıklar davet edildiklerinde duruşmaya gelmek zorundadır. Elbette tanıklıktan çekinme hakkı gibi yasal nedenler ve kabul edilebilir mazeretler bu yükümlülüğe istisna oluşturur[583]. Kimsenin kendisini ve yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaması ilkesi karşısında tanık da bu istisna kapsamında kendisi ve yakınlarını suçlayıcı beyanda bulunmama hakkına sahiptir. Bu sayılan haklar haricinde tanık her zaman olaya ilişkin beyanlarını dürüst ve eksiksiz şekilde aktarmak zorundadır. Tanığın, şüpheli veya sanık gibi susma hakkı bulunmamakta, gerçeği söylememesi, cezai sorumluluğunu (TCK m. 272) doğurmaktadır. Bu durum tanık beyanı ile sanık beyanını belirgin şekilde ayrıştırır[584]. Buna rağmen, CMK m. 50/1 (c) bendi kapsamında şüphelilerin de tanık olarak dinlenebilmesinin öngörülmesi doktrinde eleştirilmektedir[585].

---

[579] Birtek, s. 11.
[580] Öztürk/Tezcan/Erdem/Gezer/Kırıt/Alan Akcan/Özaydın/Tütüncü/Altınok Villemin/Tok, s. 211, Özbek/Doğan/Bacaksız, Ceza Muhakemesi Hukuku, s.587, Birtek, s. 109.
[581] AİHM, Cardot/France, Başvuru no: 11069/84, Karar T.: 19.03.1991, para. 35, Lucà/ Italy, Başvuru no. 33354/96, Karar T. 27.02 2001, para. 41, https://hudoc.echr.coe.int/, Erişim Tarihi: 29.07.2021.
[582]AİHM, Balsyte-Lideikiene/Lithuania, Başvuru no. 72596/01, Karar T. 4.11.2008, para. 63, , https://hudoc.echr.coe.int/, Erişim Tarihi: 29.07.2021.
[583] Birtek, s. 112, 113.
[584] Özbek/Doğan/Bacaksız, s. 586.
[585] Şahin/Göktürk, **Ceza Muhakemesi Hukuku II**, s.39.

Kural olarak delillerin müştereklik unsuru uyarınca, tanık beyanının sanığın da yer aldığı duruşmada tartışmaya açılması gerekir. AİHS m. 6/3 (d) bendinde de suç ile itham edilen kişilerin iddia tanıklarını sorguya çekmek veya çektirmek, savunma tanıklarının iddia tanıklarıyla aynı koşullar altında davet edilmelerinin ve dinlenmelerinin sağlanmasını isteme hakları adil yargılanma hakkı kapsamında korunmaktadır. Sanık aleyhine tanıklık eden kişilere soru sorabilmeli, ifadelerini çürütme hakkına sahip olabilmelidir. Özellikle tanık beyanının hükme esas tek delil olduğu durumlarda, sanığın bu haklarından mahrum bırakılması adil yargılanma hakkının ihlalini teşkil edecektir[586]. Bu nedenle CMK m. 201 ile Cumhuriyet savcısı, müdafi veya vekil sıfatıyla duruşmaya katılan avukata, tanıklara doğrudan soru yöneltme hakkı tanınmıştır.

Beş duyu organı ile maddi olaya dair öğrenilmiş bilgiler, doğrudan tanıklıktır. Bununla birlikte tanıktan duyduğunu anlatan ikinci derece tanık da dinlenebilir. Bu durum dolaylı tanıklık şeklinde ifade edilmektedir. Burada dolaylı kavramı yan olayları anlatmak için kullanılmamakta, olaya birincil derecede şahitlik etmemiş olma anlamına gelmektedir. Dolaylı tanık, bir nevi "tanığa tanıklık"[587] yapmaktadır. Dolaylı tanık beyanı de maddi vakıada boşlukları doldurmak amacıyla kullanılabilir. Bu tür beyanların da delillerin taşıması gereken özellikleri bulundurdukları takdirde delil olarak değerlendirilmesinde bir engel bulunmamaktadır.

Tanıklık açısından profilleme teknolojileri ile kıyaslanabilecek üç husus üzerinde ayrıca durulmalıdır. Bunlardan ilki tanık bilirkişi kurumudur. Kişilerin tanıklıkları sırasında uzmanlıklarını içeren bilgilerini aktarmaları halinde tanık-bilirkişilik söz konusudur[588]. 2004 CMUK tasarısında 72. maddede düzenlenen tanık bilirkişi, geçmişteki olayların özel bilgi sahibi olunmaksızın değerlendirilmesi mümkün olmadığı takdirde başvurulan ve bilirkişi sıfatıyla dinlenen kişi olup bu kişilere tanıklığa ilişkin hükümlerin uygulanması öngörülmüştür. Bu düzenlemenin gerekçesinde belirtildiği üzere, belli bir muayene veya inceleme yaparken gelişmelere tanık olan kişi, tanık-bilirkişi olarak betimlenmiştir. Bu durumda kişi uzmanlığı

[586] AİHM, Vozhigov/ Russia, Başvuru no. 5953/02, 26.04.2007, para. 51, A. M./Italy, Başvuru no: 37019/97, 14.12.1999, para 25, https://hudoc.echr.coe.int/, Erişim Tarihi: 29.07.2021.
[587] Özbek/Doğan/Bacaksız, s. 586, 587, Birtek, s.129, Şahin/Göktürk, Ceza Muhakemesi Hukuku II, s.41.
[588] Özbek/Doğan/Bacaksız, s.586.

sebebiyle bilirkişi olmakla birlikte aynı zamanda ilgili olay ve duruma hâkimiyeti sebebiyle olayın tanığı olmakta, bu nedenle ayrı bir statüye sahip olması gerekmektedir. Yine gerekçede Talat Paşa'nın öldürülmesi olayına ilişkin yıllar sonra görülen davada dinlenen bilirkişi, tanık-bilirkişiye örnek olarak gösterilmektedir. Ancak ilgili düzenlemeye mevcut CMK kapsamında yer verilmemiştir[589]. Tanık bilirkişi statüsü, tanıklık ile bilirkişilik statüleri arasında köprü kurmakta, bu statüye sahip kişiler, kural olarak olaya ilişkin şahsi görüşlerini aktarmaması gereken tanıklardan ayrılmaktadır. Mevcut CMK sistematiğinde ise bilirkişi ile tanık birbirinden ayrılmıştır. Örneğin m. 22 gereği aynı davada tanık sıfatıyla dinlenen hâkim davaya bakamayacaktır. Yine CMK kapsamında bu iki kurumu birleştiren bir hüküm olmadığından, tanık ve bilirkişinin maddi gerçeği bulmada hizmeti birbirinden ayrılmıştır. Tanık, maddi vakıaya ilişkin beş duyusuna dayalı algısını beyan ederken, bilirkişi teknik bilgi gerektiren durumlarda, gözlemlerine değil, teknik bilgilerine dayanır. Hâkime, delilin çözümlenmesi ve değerlendirilmesinde yardımcı olur. Tanık ve bilirkişi beyanlarının konusu farklı olduğundan, bu iki sıfatın birleştirilmesi doktrinde mümkün görülmemektedir. Bu iki sıfatın birleşmesi, hâkimin reddi sebeplerinden biri olup, CMK m.69 gereği bilirkişiler açısından da hâkimin reddi sebepleri uygulanacağından, olaya tanıklık etmiş kişinin bilirkişilik yapması engellenmiş bulunmaktadır. Doktrinde olaya bizzat tanıklık kişinin yerini doldurmanın zorluğu sebebiyle, bu kişinin tanıklık görevini evleviyetle yerine getirmesi ve aynı davada bilirkişiye başvurmak gerekirse, farklı bir bilirkişinin tayin edilmesi gerektiği belirtilmektedir. Örneğin kaza anında olay yerinde bulunan doktorun, mağdurun yaralanma derecesine ilişkin bilgisi tanık beyanı olarak değerlendirilmelidir[590].

Üzerinde durulması gereken diğer bir husus ise kişilik tanıklığıdır. Tanık beyanının konusu, yargılama konusu uyuşmazlık yani yargılama sırasında çözüme kavuşturulmaya çalışılan maddi vakıadır. Dolayısı ile tanığın olay ile ilgili açıklama yapması gerekmektedir. Bunun dışında sanığın kişiliği, ahlaki değerleri, yaşam tarzına ilişkin tanıklık kişilik tanıklığıdır ve sübjektif kanaat içerir. Bu bilgilerin maddi vakıa ispatında kullanılması mümkün değildir. Sanığın kişiliği örneğin TCK m. 51 kapsamında kısa süreli hapis cezası söz konusu olduğunda seçenek yaptırımların

[589] Özbek/Doğan/Bacaksız, s. 586, dipnot 762.
[590] Öztürk/Tezcan/Erdem/Sırma Gezer/Saygılar Kırıt/Alan Akcan/Özaydın/Erden Tütüncü/Altınok Villemin/ Tok, s.209.

uygulanıp uygulanmayacağı[591]veya hapis cezasının ertelenmesine karar verilmesi, bunun yanı sıra TCK m. 62 kapsamında görülen takdiri indirim sebeplerine karar verilmesi sırasında dikkate alınabilmektedir[592]. Ancak kişiliğin dikkate alındığı bu durumlar suçun tespiti değil cezanın tayini ile ilgilidir. Suça konu maddi olay ispatında bu bilgiler olayın akışını ispata elverişli değildir[593].

Son olarak gizli tanık müessesesi ele alınmalıdır. Gizli tanık, suç konusu olay hakkında görgü ve bilgisine başvurulan, ancak güvenliği nedeniyle kimliği saklı tutulan kimsedir. Her olayda gizli tanık dinlenilemez. Gizli tanık deliline CMK m. 58 kapsamında yalnızca bir örgütün faaliyeti çerçevesinde işlenen suçlarda başvurulabilir. Bu tür suçlarda, tanığın korkmadan gerçeği anlatması, böylece suçun tüm unsurlarıyla ortaya çıkartılması amaçlanmıştır[594]. Bununla birlikte Tanık Koruma Kanunu ("TKK"[595]) tanık koruma tedbirlerinin uygulanmasının kapsamını genişletmiştir. TKK kapsamında, kendilerinin veya Kanun'da belirtilen yakınlarının hayatı, beden bütünlüğü veya mal varlığı ağır ve ciddi bir tehlike içinde olan ve örgütlü suçların yanı sıra ağırlaştırılmış müebbet hapis, müebbet hapis ve alt sınırı on yıl veya daha fazla hapis cezasını gerektiren suçlarla ilgili olarak tanıklık yapacak kişilere koruma tedbirleri uygulanabilir. Gizli tanık ile korunan tanıklar arası benzerlik, duruşmada dinlenme usullerine ilişkileridir. Dolayısıyla, koruma altındaki tanıkların beyanı da kovuşturma aşamasında gizli tanıkların dinlenilme usulüne göre alınacaktır[596].

CMK kapsamında gizli tanık ifadesine ancak istisnai olarak başvurulmalıdır. Maddi gerçeğe ulaşabilmek adına tanığın korunması ve ifadesinin alınması büyük önem taşımakla birlikte, itham sisteminde sanığın adil yargılanma hakkı, masumiyet karinesi ve savunma hakkının da göz ardı edilmemesi gerekir. Bu nedenle her suç örgütü kapsamında işlenen suçta gizli tanıklık müessesine otomatik olarak

---

[591] Gökhan Taneri, "Temel Cezanın Belirlenmesi", **Ankara Barosu Dergisi**, Cilt:74, Sayı:3, 2016, ss. 127-161, s.138.
[592] Taneri, s.156
[593] Birtek, s. 156, 157.
[594] Erol Tatar, "Gizli Tanık", **Ankara Barosu Dergisi**, Sayı:4, 2013, ss.285-296, s.285.
[595] 5726 sayılı Kanun, Resmî Gazete T. 5/1/2008, Sayı: 26747, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5726.pdf.
[596] Tatar, s.285, 286. Tatar CMK m. 58 dikkate alınarak yalnızca örgütlü suçlara ilişkin gizli tanık beyanlarının delil olarak kabul edilebileceğini belirtmektedir. Bununla birlikte Tanık Koruma Kanunu hem özel kanun hem de sonradan çıkan kanun olduğu için, CMK ile çelişen noktalarda TKK'nin dikkate alınması gerektiğini ileri süren görüşler de bulunmaktadır. Cadide Şentürk/Tuğba Bayzit, "Gizli Tanık", **Türkiye Barolar Birliği Dergisi**, Cilt:25, Sayı:101, ss. 103-166, s.141.

başvurulmaması gerekir[597]. Bu tür suçlarda gizli tanık, kendisinin veya yakınlarının can güvenliğine yönelik bir tehdit bulunması halinde, CMK m. 58 f. 2. uyarınca kimlik bilgilerini saklı tutabilecektir. CMK m. 58/3 gereği hazır bulunanların huzurunda dinlenmesi, tanık için ağır bir tehlike teşkil edecek ve bu tehlike başka türlü önlenemeyecekse veya maddî gerçeğin ortaya çıkarılmasında somut bir tehlike söz konusu olacak ise; hâkim, hazır bulunma hakkına sahip bulunanlar mahkemede bulunmadan tanığı dinleyebilir. Bununla birlikte tanığın dinlenmesi sırasında ses ve görüntülü aktarma yapılacak ve soru sorma hakkı saklı tutulacaktır.

Avrupa İnsan Hakları Mahkemesi gizli tanık beyanlarının adil yargılanma hakkını ihlal edip etmediğini tespit ederken üç unsuru dikkate almaktadır. Bunlardan ilki tanığın kimliğini gizlemek için yeterli nedenlerin oluşmuş olmasıdır. İkincisi hüküm oluşturulurken yalnızca gizli tanık beyanlarına dayanılıp dayanmadığıdır. Üçüncü olarak eğer gizli tanık beyanları tek başına hükme esas alındıysa veya hüküm açısından belirleyici delil olarak değerlendirildiyse, silahların eşitliğini sağlamak adına ek tedbirler alınması büyük önem taşımaktadır. Bu bağlamda savunmanın beyan delillerinin doğruluğu ve güvenilirliğini tartışmaya açamadığı, bu delillerin sağlamlıklarının özenle irdelenemediği hallerde AİHS m. 6'nın ihlali söz konusu olacaktır[598].

Yargıtay kararlarında gizli tanığın hâkim huzurunda ifade vermesi gerektiği ve buna dair tutanakların CMK m. 217 maddesi uyarınca duruşmada sanık ve müdafiine okunup diyeceklerinin sorulması gerektiği vurgulanmaktadır[599]. Bunun yanı sıra Tanık Koruma Kanununun m. 9/8 uyarınca kimliği gizlenerek veya duruşmada hazır bulunması gereken kişiler olmaksızın dinlenen veya ses veya görüntüsünün değiştirilerek özel ortamda dinlenen tanıkların beyanının tek başına hükme esas alınamayacağına ilişkin düzenleme dikkate alınmalıdır. Buna aykırı şekilde "olayın sübutu açısından tek delilinin bir tanığın açıklamalarından ibaret olması, ayrıca bu tanığın bir de gizli tanık olması halinde", gizli tanığın duruşmada mutlaka dinlenmesi

---

[597] Ersan Şen, "Gizli Tanıklık", **Nevşehir Barosu Dergisi**, Cilt:1, Sayı, 1, Mart 2014, ss. 273-283, s.276.
[598] AİHM, Ellis, Simms, Martin/ Birleşik Krallık, Başvuru no: 46099/06, 46699/06, Karar Tarihi: 10.04.2012, para. 73-89, Al-Khawaja ve Tahery/Birleşik Krallık, Başvuru no: 26766/05,22228/06, Karar Tarihi: 15.12.2011.
para. 130-147, https://hudoc.echr.coe.int/, Erişim Tarihi: 29.07.2021.
[599] Yargıtay 16. CD, E. 2019/9663, K. 2021/1071, T. 15.2.2021, Yargıtay 16. CD, E. 2019/5644, K. 2021/154, T. 27.1.2021, https://lib.kazanci.com.tr/, Erişim Tarihi: 29.07.2021.

gerektiğinin altı çizilmekte, bu durumda tanığın önceki beyanlarının okunması ile yetinilmesinin hukuka aykırı olacağı belirtilmektedir[600]. Yargıtay, ayrıca savunmaya gizli tanık delillerini erişim ve sorgulama hakkı tanınmasından bağımsız olarak, ispat gücü açısından gizli tanık beyanlarının tek başına yeterli ve kesin kanaat vermeye elverişli olmadığını, yan delillerle desteklenmeksizin tek başına mahkûmiyete esas alınmasını kabul etmemektedir. Bu durumda, Yargıtay yeterli değerlendirme yapmaksızın hüküm kurulmuş olduğuna hükmetmektedir[601].

Sonuç olarak tanıklar, özellikle örgütlü suçlarda beyanda bulunmalarının ardından eski hayatları ile irtibatlarını koparma, yeni bir yere yerleşme gibi tedbirlere katlanmak zorunda kalmakta, bunun yanı sıra kimliklerini gizlemedikleri takdirde kendileri veya yakınlarına yönelik büyük tehlikelerle karşı karşıya kalmaktadır. Bununla birlikte, salt tanık haklarına öncelik tanındığı takdirde sanıklar, adeta hayali bir tanığın beyanı ile mahkûm edilmektedir. Bu nedenle sanık ve tanık haklarının bağdaştırılması adına gizli tanık beyanının başka delillerle doğrulanması ve savunmanın gizli tanık beyanlarına erişimi ve sorgulama hakkı tanınması adil yargılanmanın tesisi için büyük önem taşımaktadır[602].

b) Profilleme Teknolojilerinin Tanık Beyanı Kapsamında Değerlendirilmesi

Yukarıda ele alındığı üzere tanık beyanı, tanıkların somut olaya ilişkin beş duyuları ile edindikleri bilgileri içerir ve bu beyanlar çelişmeli yargı ve savunma hakkına uygun şekilde tartışmaya açılır. Böylelikle varsa beyandaki çelişkiler veya tanığın taraflı yorumları ortaya çıkartılır. Profilleme teknolojileri ise beyanlarının doğruluğuna dair "yemin edemeyen" yazılımlardan oluşur, dahası bu beyanların

---

[600]Yargıtay 16. CD, E. 2020/1489, K. 2020/5527, T. 9.11.2020, https://lib.kazanci.com.tr/, Erişim Tarihi: 29.07.2021.

[601] Örneğin bir davada Yargıtay "kafatası içinde bulunan ve birden çok parçalara ayrılmış metal parçalarının doğrudan kafatası kemiğine kulak arkasından girerken mi parçalara ayrıldığı yoksa bir yerlerden mi sektiği …hususun aydınlatılması, dosyadaki gizli tanık beyanlarının güvenilirliğini de kesin şekilde etkileyecektir. Zira olay gecesi birçok kişinin düğün kutlaması için ateş ettikleri dosya kapsamından anlaşılmaktadır" diyerek gizli tanık beyanlarını tek başına kanaat oluşturmaya yeterli ve kesin delil olarak kabul etmemiştir, Yargıtay 1. CD.,E. 2018/2023, K. 2020/2528, T. 26.10.2020, https://lib.kazanci.com.tr/, Erişim Tarihi: 29.07.2021. Gizli tanık beyanlarının tek başına mahkumiyet hükmüne esas alınamayacağına ilişkin ayrıca bkz. Yargıtay 16. CD., E. 2019/11482, K. 2020/3665, T. 16.7.2020, https://lib.kazanci.com.tr/, Erişim Tarihi: 29.07.2021.

[602] Şentürk/Bayzit, s. 128, 129.

doğruluğunun savunma ve iddia tarafından tartışmaya açılması mümkün olmamaktadır. Yabancı doktrinde, bilişim araçları kullanılarak varılan deliller açısından gerçek kişi tanığın beyanıymışçasına düzenlemeler öngörülmesi tartışma konusu olmuştur[603].

Özellikle bilişim sistemlerinin ve yazılımların kişiye bir suç itham etmek amacıyla kullanıldığı durumların, kişi aleyhine tanık beyanı ile benzeştiği ileri sürülmektedir. Ancak tanık beyanından farklı olarak, otomatik olarak işleyen sistemlerde, bu sistemlerin doğruluğu ve güvenilirliğini ele almak daha güç olmakta, buna rağmen yapay zekâ veya bilişim sistemlerinin vardığı sonuçlar, mutlak tarafsız bir beyanmışçasına ele alınmaktadır. Yine yazılım üreticilerinin fikri mülkiyet haklarını ileri sürerek yazılıma ilişkin bilgi paylaşmamaları veya bu yazılımların vardıkları sonuçların insanlarca takip ve analizinin güç olması, yazılımları "gizli tanık" kavramına yaklaştırmaktadır[604]. Nitekim şeffaf olmayan makine öğrenmesi yöntemleri kullanıldığı veya açıklanabilir yazılımlara dayanılsa da yazılım kodunun mahkemeler ile paylaşılmadığı durumlarda, savunmanın sürece dâhil olarak yazılımın çalışma usulünü ve dayandığı verileri sorgulaması mümkün olmamaktadır. Bu nedenle profilleme teknolojileri karşısında savunma, adeta gizli tanık beyanına benzer bir durumla karşı karşıya kalmaktadır. Oysa savunma hakkı açısından oldukça tartışmalı bir kurum olan gizli tanık kurumu, yukarıda tartışıldığı üzere gerçeğin açığa çıkarılabilmesi için son çare olup gizli tanığa yalnızca belirli suç tiplerinde ve tanığın veya yakınlarının can güvenliğine yönelik gerçek bir tehlike söz konusu olduğunda başvurulabilir. Profilleme teknolojileri, her tür suç tipinde ve herhangi bir hayati tehlike söz olmaksızın kullanılabilmeleri bakımından, son çare olan gizli tanık kurumu ile örtüşmemektedirler. Silahların eşitliği tesis için gizli tanık beyanlarında olduğu gibi gizliliğe karşı ek güvenceler profilleme teknolojileri açısından da öngörülmemiştir. Her ne kadar yazılımlar ile gerçek bir kişi gibi fiziksel olarak yüzleşmek mümkün olmasa da mahkemeler bunların işleyişi ve vardıkları sonucun güvenilirliğini ele alabilmeli ve silahların eşitliği ilkesi çerçevesinde savunma ve iddianın yazılımların

---

[603] Sergey Bratus/Ashlyn Lembree/Anna Shubina,"Software on the Witness Stand: What Should It Take for Us to Trust It?" İçinde: **Trust and Trustworthy Computing**, Ed. Alessandro Acquisti/Sean W. Smith/Ahmad Reza Sadeghi, Springer: Berlin, 2010, ss.396-416, s.397, 398.

[604] Aleš Završnik,"Criminal Justice, Artificial Intelligence Systems, and Human Rights", **ERA Forum**, Cilt:20, 2020, ss. 567-583, s.577. Doktrinde bu durumu tanıkla yüzleşmenin mümkün olmadığı yazılı beyan sistemine (affidavit) benzeten yazarlar da bulunmaktadır, bkz. Andrea L. Roth, "Machine Testimony", **Yale Law Journal**, Cilt: 126, Sayı: 1, 2017, s..1972-2053, s.2041, 2042.

işleyişi ve vardıkları sonuçlara karşı görüş sunabilmesini mümkün kılmalıdır[605]. Bunun için yazılımın kodları kadar, hangi verilerin girdi olarak kullanıldığı, modelleme ve kullanılan öğrenme yöntemi paylaşılmalıdır[606].

Otomatik işleyen sistemler, farklı şekillerde çalışmaktadır, bu nedenle tanık beyanı ile farkları çalışma usulleri dikkate alınarak ortaya konulmalıdır. Örneğin hız sınırını tespit eden bir kamera, olayın içeriğine ilişkin bir kanıt teşkil eder, bu yönüyle maddi olayı anlatan bir tanık beyanı ile daha fazla benzerlik göstermektedir. Ancak farklı veri tabanlarını birleştirerek kişinin karakteri, tercihleri, bulunduğu ve bulunacağı yerleri öngörmeye çalışan profilleme teknolojileri, olaya ilişkin bilgi sahibi olan ve maddi gerçeği aydınlatmaya çalışan tanık beyanlarından tamamen ayrışmaktadır. Nitekim kabul edilebilir bir tanık beyanından bahsedebilmek için tanığın olaya ilişkin gerçek bir bilgisi, şahsi bir gözlemi söz konusu olmalıdır. Aksi halde beyan delilinin olayı aydınlatmaya katkısı olmayacaktır[607]. Beyan delilleri açısından üzerinde durulması gereken diğer bir husus da bu tür delillerin maddi olayı iz ve emareler gibi objektif şekilde göstermemesidir. Olay aracı bir kişi tarafından, onun algıladığı şekilde aktarılmaktadır. Delil kaynağı olan tanığın olayı hatalı veya eksik gözlemlenmesi veya yanlış bir şekilde yorumlaması beyan delilin sağlamlığı açısından tartışma doğuracaktır. Profilleme teknolojileri de çoğu zaman doğrulanmamış ve güncellenmemiş verilere dayanabilmekte, bu duruma rağmen tamamen objektif ve bilimsel sonuçlara vardıkları kabul edilmektedir. Bu veriler ve verilere dayalı sonuçlar, müşterek tartışmaya kapatılmıştır. Bu nedenle tanık beyanlarına nazaran profilleme teknolojileri ile varılan sonuçların sağlamlıkları çok daha tartışmalıdır.

Profilleme teknolojileri maddi olay ile bağlantılı tanık beyanından ziyade kişilik tanıklığına daha yakındır. Kişinin değiştirmesi ve seçmesi mümkün olmayan aile yapısı, ait olduğu sınıf, mahalle gibi pek çok unsur üzerinden gelecekte suç işleme potansiyeli belirlenmeye çalışmaktadır. Ancak CMK sisteminde sanığın kişiliği, ahlaki değerleri, yaşam tarzına ilişkin sübjektif kanaat içeren bu tür bir tanıklık, maddi olayın ispatında kullanılmamalıdır[608].

---

[605] Roth, s.1983, 1984.
[606] Završnik, s.578.
[607] Roth, s. 1984.
[608] Birtek, s. 156, 157.

Dolayısıyla profilleme sonucu elde edilen ve kişi aleyhine sonuç doğuran veriler, ceza muhakemesinde tanık delili ile örtüşmemekte, maddi olayın fail tarafından işlendiğini göstermemektedir. Bununla birlikte, bu teknolojilerin kullanılması halinde, tanık ve özellikle gizli tanık beyanında olduğu gibi, mutlaka ceza muhakemesi süjelerinin de sürece katılarak profilleme teknolojilerini ve bunların vardıkları sonuçları müşterek bir şekilde değerlendirebilmeleri gerekir. Nitekim AİHS kapsamında da bu durum güvence altına alınmış, m. 6/3/(d) uyarınca iddia makamının tanıklarını sorgulamak veya sorgulatmak hakkı salt tanık kavramı ile sınırlı olmaksızın geniş şekilde yorumlanmıştır. Buna göre adil yargılanma hakkının tesisi için sanığın hüküm almasına yol açabilecek her türlü bilirkişi, uzman görüşü, mağdur beyanı, bilgi ve belgelerin değerlendirilmesi ve bunlara karşı çıkılabilmesi gerekir. Her ne kadar profilleme tanık kapsamında değerlendirilemese de m. 6'daki güvencelerin ceza muhakemesinde şüpheli/sanık aleyhine sevk edilen profilleme teknolojileri için de geçerli olduğunun altı çizilmelidir[609].

2. Bilimsel Deliller

a) Genel Olarak Bilimsel Delillerin Değerlendirilmesi

Vicdani delil sisteminin yerini bilimsel delil sistemine bırakacağı ve bu sistemin çok daha objektif olacağı iddiası geçmişten bugüne değin ceza adaleti tartışmalarının gündeminde olmuştur. Oysa bilimsel delilin keyfi kararları ortadan kaldıracağı, kanıtlanmamış bir iddiadır. Bilimsel delil diye adlandırılan örneğin DNA analizi yapılması, bilimsel konulara ilişkin mütalaa verilmesi gibi pek çok husus yine insan faktörü içermekte ve bu yönüyle sübjektif bir yönü kaçınılmaz şekilde barındırmaktadır. Dolayısıyla, bilimsel verilerin de her zaman hata payı bulunacağı göz ardı edilmemelidir. Örneğin kan grupları dolayısıyla kan bağı bulunmadığı kanıtlanan kişiler açısından aksini iddia etmek bilime ve mantığa aykırı olacaktır. Ancak hâkim her zaman kan tahlili sırasında tüplerin karışması gibi ihtimalleri hesaba katmalı, şüphe ortadan kalkıncaya kadar bilimsel delilleri mutlak doğru olarak kabul etmemelidir[610].

---

[609] Završnik, s.577.
[610] Kunter, **Ceza Muhakemesi Hukuku**, s.591, 592.

Bilimsel deliller çoğunlukla suçun işlenmesinden sonra geriye kalan ve dolaylı şekilde yan olaylara işaret eden kan, tükürük, meni, parmak izi gibi hususlardan yola çıkar. Bunun yanı sıra ses kayıtları ve bilgisayarda suç izini gösteren veriler gibi sayısal deliller de bilimsel delil kapsamındadır[611]. Örneğin suni delil olarak bilgisayar internet protokol numarası (IP kayıtları), iletişimin tespitinde haberleşmeye ilişkin kayıtlar, roaming (dolaşım bilgisi) kayıtları sayısal delil olarak gösterilebilir. Bilimsel delil ile dijital veya tabii bulguların bir nevi "konuşturularak" maddi gerçek hakkında bilgi edinilmesi söz konusudur. Bu tür tabii ve suni izler hâkim tarafından gündelik yaşam deneyimlerine göre değerlendirilemeyeceğinden bunların bilimsel metotlarla incelenmesi zorunlu olmaktadır[612]. Bu bağlamda adli tıp, adli bilişim ve kriminalistik alanları, bulguların değerlendirilmesi ve anlaşılır hale getirilmesinde önemli rol oynamaktadır.

Bugün insanlık tarafından üretilen bilgilerin çoğunluğu sayısal olarak bilişim sistemlerinde oluşturulmakta veya saklanmaktadır. Bilgi toplumunda enformasyon, farklı bir format olan veri şeklinde bilişim sistemlerinde yer almaktadır. Bunların maddi olayı temsil edici özelliği olması halinde delil olarak kabul edilmesi ve insanlar tarafından okunur veya anlaşılır hale getirilmesi gerekir[613]. Bu tür delillere sıklıkla başvurulması ve profilleme teknolojileri ile ilgili olmaları nedeniyle sayısal (dijital) delillerin üzerinde ayrıca durulmalıdır.

Tarihsel gelişim içinde sayısal veriler, ilkin en önemli bilişim aracının bilgisayar olması göz önüne alınarak bilgisayar delili olarak isimlendirilmiştir. Teknolojinin gelişimi ile bilgisayar delili kavramı yetersiz kalmış verilerin, salt bilgisayarlardan değil, farklı bilişim sistemlerinden de elde edilerek kullanılabileceği anlaşılmıştır[614]. Nitekim bilgisayar kavramı da günümüzde fonksiyonel açıdan yaklaşılarak genişletilmekte, laptop veya sabit bilgisayarların ötesine geçilerek, benzer programlama ve veri işleme sistemine sahip, kişilerin rahatlıkla sayısal veri

[611] Birtek, s. 203.
[612] Birtek s.207.
[613] Olgun Değirmenci, "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği", **Terazi Hukuk Dergisi**, Cilt: 9, Sayı:97,Eylül 2014, s. 15, 16.
[614] Değirmenci, s. 16.

üretebildiği cep telefonu, navigasyon sistemleri, akıllı araçları hatta akıllı mikro dalga fırınları içerek şekilde algılanmaktadır[615].

Sayısal veya "dijital" veri, elektronik cihazlar içerisinde temelde 1 ve 0 değerlerinden oluşan ikili sayı sistemi ile kaydedilmektedir. Dijital verilerin temelini oluşturan bu sayı sisteminin anlamlandırılması ve okunabilmesi için programlara ihtiyaç duyulmaktadır. Sayısal veriler, cihazlar içinde var olduğundan kolluk personelinin olay mahalline gittiğinde ilk temas edeceği deliller, sayısal verileri içeren elektronik cihazlardır[616]. Örneğin kolluk tarafından elde edilen ve suç ile ilişkisi araştırılacak olan USB belleği bir elektronik delil niteliğindedir. "Elektronik delil" hem elektronik cihazı hem de bu cihaz içerisinde bulunan sayısal verileri kapsayan daha geniş bir kavramdır[617]. Yürütülmekte olan bir soruşturma veya kovuşturmaya esas olmak üzere, bilgisayar, mobil telefon, dijital fotoğraf makineleri, dijital faks makineleri gibi tüm bilişim sistemleri ve bu özellikteki depolama aygıtlarını ve bunlar üzerinden elde edilen adli delilleri ifade eder. Dolayısıyla elektronik delil, bilişim teknolojisi içeren her türlü donanımı, bu donanım içerisindeki yazılım tarafından işlenen her türlü veri ile bilişim teknolojisi tarafından kullanılan her türlü elektronik sinyali kapsar[618]. Her ne kadar elektronik ve dijital (sayısal) delil kavramlarının birbirlerinin yerine kullanıldığı görülse de sayı esasına dayanan ve ancak belli programlar aracılığıyla anlaşılır hale gelen sayısal delil, elektronik delilden daha dar bir kavramdır.

Delillerin klasik olarak belge, beyan, belirti şeklinde üçlü ayrıma tabi tutulduğu görüldüğünde, sayısal deliller ayrı bir grup oluşturmamaktadır. Bunların bazen belge, bazen belirti olarak değerlendirilmesi mümkündür. Örneğin bir olayın oluş şeklini kaydeden kameradaki sayısal veri, maddi olayı temsil eden bir belge delili olarak kabul edilebilecekken, hacklenen bir bilgisayarda saldırı sonrası bulunan sayısal izler, bir belirti delili olarak kabul edilebilecektir[619].

---

[615] Eoghan Casey, **Digital Evidence and Computer Crime**, Elsevier Yayınevi: Waltham, 2011, s. 8.
[616] Yusuf Başlar, **Ceza Yargılamasında Elektronik Delil**, Sakarya Üniversitesi Siyaset ve Kamu Yönetimi Anabilim Dalı, Doktora Tezi, Sakarya, Mayıs, 2015, s.63.
[617] Başlar, s. 64.
[618] Başlar, s. 65.
[619] Değirmenci, s. 19.

Ceza Muhakemesinde en güvenilir delil, elbette delilin aslıdır. Bu delilin ayrıca diğer delillerle birlikte ele alınarak doğruluğunun sağlanması gerekir. Sayısal veriler ise imajları alınarak birebir kopyalanabilme özelliğine sahiptir ve özellikle adli bilişimde bu tür deliller üzerinde yapılacak incelemeler orijinal delil üzerindeki verilerin değişmemesi amacıyla çoğunlukla delilin adli kopyası üzerinden yapılmaktadır[620]. Yine bu verilerin 0-1 formatından anlaşılabilir bir formata geçirilmesi için araç programların kullanılma zorunluluğu bulunmaktadır. Örneğin kelime işlemci dosyasında bulunan veri, ancak bir program ile açıldığında bilgisayar ekranında okunabilir hale gelmektedir. Sayısal verinin bu şekilde okunabilir hale getirildiği hâl verinin aslı olarak kabul edilmektedir. CMK özelinde delillere ilişkin şekli kurallar öngörülmediğinden, okunabilir hale getirilmiş verilerin ekran görüntüsü veya çıktısının alınması da delil olarak kabul edilmektedir[621]. Bununla birlikte çıktı veya ekran görüntüleri, sayısal delillerin oluşturuldukları, kopyalandıkları ve değiştirildikleri zaman gibi önemli bilgileri içeren üst verileri (metadata) göstermez. Bu nedenle sayısal verinin bilişim sisteminde bulunan hali, delil olarak değerlendirilmesi gereken halidir ve bu halde verinin içeriği kadar, veri hakkında bilgi veren üst veri de tespit edilebilir[622].

Bugün eczaneden alınan ilaçlar, vatandaşlık bilgileri, Facebook, Twitter gibi sosyal medya platformlarında kişilerin günlük faaliyetleri, fotoğrafları, bulundukları yerlerin bilgisi gibi pek çok veri sayısal olarak kaydedilmektedir. Bu durum deliler açısından fiziksel delillerden çok sayısal delilere doğru bir geçişe neden olmuştur[623].

Ancak sayısal verilerin, delil olarak kabul edilebilmesi için, diğer delillerde bulunması gereken gerçekçi olma, akılcı olma, temsil edicilik, sağlamlık, erişilebilir olma, müştereklik, hukuka uygun elde edilme unsurlarını içermeleri gerekmektedir. Sayısal veriler özellikle gerçek ve sağlam olma unsurları açısından tartışmalıdır. Nitekim tahrip edilme ihtimalleri çok yüksek olup bulundukları bilişim sistemi içinde incelenmeleri ve başka kaynak ile teyit edilmeleri gerekir. Kaynağın doğruluğu ve orijinalliği açısından, örnek alma işlemi veya diğer işlemler sırasında verilerin

---

[620] Murat Özbek, "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", **1st International Symposium on Digital Forensics and Security (ISDFS'13)**, Mayıs 2013, s.2
[621] Değirmenci, s. 20.
[622] Değirmenci, s.21.
[623] Değirmenci, s. 20, 21.

değiştirilmediği kanıtlanmalıdır. Ardından delil olarak kullanılmak istenen verinin gerçekten iddia edilen kaynaktan elde edilmiş olduğu kanıtlanmalıdır. Son olarak kaynağın kaydedilmiş olduğu tarih gibi muhakeme açısından önem arz edecek bilgilerin teyit edilmesi gerekir. Özellikle çıktısı alınmış ve belge haline getirilmiş sayısal verilerin orijinalliğinin dikkatle değerlendirilmesi gerekir[624]. Bir verinin kopyasının aslı ile aynı olup olmadığını kıyaslayabilmek için hash değerine başvurulmaktadır. Hash değeri hesaplanırken, bir veri veya veri depolama biriminin ilk sektörden başlanıp son sektöre kadar tamamı, belirli bir algoritmik fonksiyondan geçirilir. Bu işlem sonucu ortaya çıkan değer, o veriye ait hash değeri olarak isimlendirilmektedir. Hash tek yönlü bir algoritmik fonksiyon olup iki verinin hash değerleri eşleştiği zaman, bu verilerin birbirlerinin tam bir kopyasının olduğu kabul edilmektedir. Hash değerlerinde uyumsuzluk olduğu takdirde ise, veri üzerinde değişiklik yapıldığı gerekçesiyle ilgili veri, sayısal delil olarak kabul edilmemektedir[625].

Bununla birlikte örneğin sayısal verilerin kaydedildiği optik diskler farklı katmanlara sahip olup bunlardan yansıtıcı olan katman, havaya maruz kaldığında oksitlenir. Yine kullanım ve muhafaza şartlarına bağlı olarak disk bozulabilir. Dolayısıyla adli kopyası alınarak hash bilgisi kaydedilen elektronik delil niteliğindeki bir optik diskten bir süre sonra tekrar adli kopya alma işlemi yapıldığında bu kez hash değerleri birbirini tutmayabilmektedir[626]. Yine açık olan sistemler, örneğin cep telefonları üzerinde kayıtlı verilerin kopyaları alınırken sistem çalışmakta olduğu için veriler üzerinde değişiklik oluşabilir[627]. Bu durum yine hash değerlerini karşılaştırmada farklı sonuçlara ulaşılmasına yol açacaktır.

Bunun yanı sıra, adli bilişim alanında yapılan araştırmalar, belirli şartlar altında yeni bir dosyanın, orijinal dosyaymışçasına aynı hash değerine sahip olacak şekilde üretilebileceğini göstermiştir. Sonradan başka kaynak tarafından üretilen dosyanın aynı hash değerine sahip olabilmesi hash değeri hesaplayan MD5, SHA-1 gibi algoritmalara gölge düşürmüştür[628]. Bu nedenle kimi durumlarda iki dosyanın aynı

[624] Casey, s.13, 14.
[625] Özbek, s.2.
[626] Özbek, s.3.
[627] Özbek, s.5.
[628] Casey, s. 23.

hash değerine sahip olması, belgenin orijinalliğini kanıtlamaya tek başına yeterli olmayabilecektir. Buna çözüm olarak, belgenin birebir kopyasının alınıp alınmadığını tespit etmede iki farklı hash algoritması kullanılmakta, örneğin belgenin hem MD5 hem SHA-1 hash değeri alınarak sağlamlığı daha güvenilir şekilde tespit edilmeye çalışılmaktadır[629].

Dolayısıyla sayısal deliller, sağlamlığı kanıtlanması oldukça güç delillerdir. Bu deliller hard diskte karışık ve katmanlı şekilde kaydedilmiş olarak bulunmaktadır. Bunun yanı sıra içerdikleri verinin yalnızca ufak bir bölümü görülmekte olan davaya ilişkindir. Tüm delillerden ilgili kısmın süzülmesi ve bozulmadan aktarılması kadar bu verilerin uygun şekilde saklanması da güçtür.

Sayısal veriler, sanal bir obje ya da olayın soyut olarak göstergesinden ibarettir. Örneğin bir bilgisayara e-posta gönderme komutu verildiğinde, bu işlem belli izler bırakmaktadır, ancak salt bu izlerden yola çıkılarak geriye yönelik tespitte bulunulduğunda, yapılan aktivitelerin bir bölümü anlaşılabilmektedir. Dolayısıyla yalnızca hizmet sistemindeki kayıtlar (server-log) ve e-posta mesajları belli bir fikir verebilmekte ancak tüm süreç aydınlatılamamaktadır.

Bunun yanı sıra sayısal veriler, çoğunlukla yan olaylara ilişkin belirtiler olup fiil ile fail arasındaki ilişkiyi kanıtlamaları tek başına mümkün olmamaktadır. Örneğin bir kişinin bilgisayarı aracılığıyla hukuka aykırı faaliyetlerin gerçekleştirildiği tespit edilse dahi, davada ayrıcı bu faaliyetlerin bizzat ilgili kişi tarafından gerçekleştirildiği kanıtlanmalıdır. Nitekim bilişim aracı, başka bir kişi tarafından kullanılmış olabilir. Benzer şekilde, truva atları gibi zararlı yazılımlar, kişinin bilgisayarının suç işlemede araç olarak kullanılmasına yol açmış ve ardından geriye yönelik tüm izleri silmiş olabilir[630]. Dolayısıyla başka deliller olmaksızın sayısal deliller tek başına şüpheli veya sanığın dava konusu fiili işlediğine dair vicdani kanaat oluşturmaya yeterli olmayacaktır[631].

---

[629] **Ibid.**
[630] Başlar, s.94.
[631] Casey, s. 25, 26.

Yargıtay da dijital bulguların delil değeri taşıyabilmesi için bunların kanuna uygun şekilde toplanmış ve yargı makamına bozulmamış şekilde sunulmuş olması gerektiğinin altını çizmektedir[632]. Dijital delillere harici müdahalenin teknik olarak mümkün olması nedeniyle bu delillere çoğunlukla kim tarafından hangi tarihte müdahale yapıldığının belirlemek güçtür. Bu nedenle el koyma işlemi sırasında olay mahallinde imaj alınmadığı ve orijinal medyanın şüpheliye bırakılmadığı hallerde, delilin sağlamlığına dair şüphe doğmaktadır. Örneğin sanığın evinde ve işyerinde yapılan aramalarda elde edildiği iddia olunan tüm dijital medyalarla ilgili imaj alınmadan, ilgilisine kopyası verilmeden ve gerekçesi tutanağa yazılmadan el koyma işleminin yapıldığı olayda Yargıtay CMK m. 134'e aykırı delil toplandığını ve bu delillerin tek başına mahkûmiyete esas alınamayacağını belirterek verilen hükmü bozmuştur[633].

Bununla birlikte, sayısal delilin değiştirilmesi ya da fail tarafından tahrif edilmeye çalışılması halinde, adli bilişimin karşılaştırma yaparak bu durumu tespit etmesi mümkündür. Sayısal delillerin silinmesi veya sabit diskin formatlanması halinde dahi delil yine kurtarılabileceğinden elektronik delillerin yok edilmesi fiziksel delillere göre çok daha zordur. Dolayısıyla suçlular delili yok etme girişiminde bulunduklarında farkında olmadan bunun kalıntılarını, kimi zaman ise dosyanın kopyasını bilişim sisteminde bırakmaktadırlar[634]. Bu özelliği, ceza muhakemesinde sayısal verileri fiziksel verilere göre daha avantajlı kılmaktadır.

Ancak elektronik delilin incelemesi, değerlendirilmesi ve analizi teknik bilgi gerektirdiğinden, fiziksel delilden farklı olarak bilirkişi görüşüne başvurulması veya delillerin bilimsel yöntemlerle açıklanır hale getirilmesi gerekir. Elde edilen elektronik verilerin delile dönüştürülmesi, belli bir usulü takip etmeyi gerektirir[635]. Nitekim Yargıtay, "soruşturma aşamasında temin edilen olay anı ve öncesine ilişkin görüntüleri içeren güvenlik kamerası görüntülerinin bilirkişiye çözümlettirilmesi ile çözüm

---

[632] Bu yönde bkz. Yargıtay 6. CD, T. 19.07.2010, E.2010/6992, K. 2010/13757, aktaran Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi", **Ceza Hukuku ve Kriminoloji Dergisi**, Cilt: 3, Sayı: 2, ss. 253-266, s.263. İlgili kararda sanığın işyerine ait güvenlik kamerası kayıtlarının orijinalliğine ve bu kayıtlara ekleme yapılıp yapılmadığına ilişkin bilirkişi raporu alınmaksızın ilgili kayıtların delil olarak kullanılması bozma nedeni yapılmıştır.

[633] Yargıtay 16. CD, E. 2015/2056, K. 2017/5023, T. 21.9.2017, https://lib.kazanci.com.tr/, Erişim Tarihi: 20.07.2021.

[634] Başlar, s. 93.

[635] Başlar, s. 90.

tutanaklarının duruşma sırasında taraflara okunması ve diyeceklerinin sorulması gerektiğine", aksi halde duruşma heyetince ilgili tutanakların ne zaman ve nerede incelendiği anlaşılamayan görüntülere dayanarak mahkûmiyet kararı verilemeyeceğine işaret etmiştir[636].

Sayısal delillerin müşterek olarak tartışılması, bu delillerin gerçekliği ve sağlamlığının tesisinde ayrıca önem taşımaktadır. Savunmanın bu delillerin değiştirildiği, tahrip edildiğine ilişkin iddiaları sunabilmesine imkân tanınmalıdır. Savunmanın bu iddialarını destekleyen uzman görüşlerine itibar edilmediği takdirde nedeni Mahkeme tarafından gerekçeleriyle açıklanmalıdır. Verilerin güvenilirliğine dair şüphe oluştuğu durumlarda yeniden bilirkişi raporuna başvurulmaksızın veya savunmanın sunduğu bilimsel mütalaalar dikkate alınmaksızın bu verilerin hükme esas alınması, gerekçeli karar hakkını, silahların eşitliği ilkesini ve dolayısıyla adil yargılanma hakkını ihlal edecektir[637].

Sonuç olarak bilimsel deliller, bilim ve teknik alanındaki prensiplerden yola çıkarak mahkemelerin sayısal veriler, nötron aktivasyonu analizi, ses analizi, psiko-linguistik alanı gibi pek çok hususta başvurduğu yöntemlerden biri olmuştur. Bilim ve teknolojiye dayalı bir toplumda, gerçeğin açığa çıkartılması ve maddi olayın çözümlenmesi açısından yeni delillere ve bu delilleri açıklayan bilimsel teorilere başvurmak kaçınılmaz hale gelmiştir[638].

Bilimsel bilgi mahkemelerde iki şekilde kullanılmaktadır. Bunlardan ilki, teknik ve bilimsel bilgiye sahip olmayan kişiler açısından anlamlandırılması mümkün olmayan iz ve delillerin bilimsel yöntemlerle açıklanır hale getirilmesidir. Örneğin bir cinayet mahallinde bulunan kan izlerinin insan kanı mı olduğu, insan kanı ise hangi kan grubu olduğu ancak tıp biliminin devreye girmesi ile açıklanabilir. Bilimsel deliller çoğu durumda, bu delilleri anlamlandırmak için genel öneri ve teoremleri olaya uygulamak üzere bilirkişiye başvurulmasını da gerektirir[639]. Bu nedenle delil değerlendirme aracı olan bilirkişiler ile bilimsel deliller arasında çoğu durumda bir bağ

[636] Yargıtay 1. CD, T. 16.01.2012, E. 2008/10249, K. 2012/48, aktaran Arslan, s.261.
[637] AYM, Sencer Başat ve Diğerleri Başvurusu, Başvuru No: 2013/7800, Karar Tarihi: 18.06.2014, para. 69-72, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7800, Erişim Tarihi: 30.07.2021.
[638] Paul C. Giannelli, "The Admissibility of Novel Scientific Evidence: Frye v. United States, a Half-Century Later," **Columbia Law Review**, Cilt: 80, Sayı: 6, Ekim 1980, ss. 1197-1250, s. 1198.
[639] Giannelli, s.1200, dipnot:19.

bulunmaktadır. Dolayısıyla varılan sonucun kabul edilebilirliği ve güvenilirliği için hem bilimsel delillere hem bilirkişiye yönelik belli kıstasların aranması gerekmektedir.

Bilimsel bir delilin, mahkemenin maddi gerçeğe ulaşma amacına hizmet edebilmesi ve güvenilir olması için üç unsur birlikte aranmalıdır. Bunlardan ilki bir delil bilimsel olarak kabul edilebilir olmalıdır. İkincisi bu ilkeye dayanarak uygulanılan teknik bilimsel olarak geçerli olmalıdır. Üçüncüsü, söz konusu tekniğin somut olaya doğru uygulanmış olması gerekir. Bu son unsur olaya uygulama sırasında kullanılan tüm tekniklerin uygunluğunu, bu tekniklere başvuran kişinin niteliklerini ve ardından sonuca varılmasında bilimsel görüşüne başvurulan kişinin niteliklerini değerlendirmeyi gerektirir[640]. Nitekim çoğu durumda testi veya metodu, somut olaydaki bilimsel verilere uygulayan kişi, aynı zamanda sonuca varan kişidir ve bu kişinin nitelikleri bilimsel verinin delil olarak kabul edilmesinde rol oynamaktadır.

Bu değerlendirmeler sırasında mahkemeler tarafından kimi zaman geçerlilik ve güvenilirlik kavramları iç içe geçecek şekilde kullanılmaktadır. Ancak bu kavramların bilim jargonunda oldukça farklı karşılıkları bulunmaktadır. Geçerlilik, bir metodun doğruluğunun test edilebileceğine, güvenilirlik ise bu tür bir testin her defasında aynı sonuçlara götüreceğine, başka bir değişle tutarlılığa işaret eder[641]. Örneğin bir kişinin ses izi/ses renginin bilimsel delil olarak kullanılabilmesi, herkesin kendine has ve başkalarından tamamen farklı bir sesinin olduğu görüşüne dayanmaktadır. Bu verinin bir delil teşkil edebilmesi için öncelikle dayandığı teorinin doğru olduğu tespit edilmeli, başka bir deyişle iki kişinin aynı sese sahip olamayacağı geçerli bir iddia olmalıdır. Sesin benzersizliği savı doğru olmadığı noktada, sesten yola çıkan delil geçersiz olacaktır. İkinci aşamada, herkesin kendisine has ve emsalsiz bir sesi olduğu kabul edildiğinde, bu sefer ses analizinde kullanılan tekniğin geçerliliği ve güvenilirliği ispatlanmalıdır. Kullanılan tekniğin geçerliliği kanıtlanmakla birlikte, bu tekniği uygulayabilmek adına kullanılan araç, örneğin spektograftaki bir kusur veya tekniğin uygulanması sırasında öngörülen usullere uyulmaması, varılan sonucun hatalı olmasına yol açabilecektir. Dolayısıyla tekniğin bilimselliği kadar, başvurulan araçlar ve yöntem de irdelenmeli, ilgili veri ancak tüm bu sürecin sonunda delil olarak kabul

[640] Giannelli, s. 1201.
[641] Giannelli, s. 1201, dipnot:20.

edilmelidir[642]. Mahkemeler tarafından kabul görülenlerin dışında yeni teknikler ve yöntemlere başvurulduğu takdirde ise bu alanda uzman kişilerin görüşleri ve açıklamaları önem kazanmaktadır. Bilirkişi başlığı altında tartışılacağı üzere, böyle durumlarda bilirkişi görüşüne başvuran mahkemeler, bu görüşü otomatik olarak benimsemek zorunda değildir[643].

Sonuç olarak bilimsel delillerin hükme esas alınması için bu delillerin, tüm delillerde aranan unsurları, özellikle de gerçeklik, sağlamlık ve müştereklik unsurlarını karşılaması gerekir. Akla ve mantığa uygun, doktrince benimsenmiş bilimsel uygulamaların ceza muhakemesi sürecinde yol gösterici olması gerekir. Bununla birlikte, bilimsel delillerin belirti oldukları, somut olaydaki maddi gerçekliği bütün olarak yansıtmayabilecekleri ve tahrip edilmeye elverişli oldukları mutlaka dikkate alınmalıdır. Ceza muhakemesinin amacı maddi gerçeğe ulaşmaktır, ancak maddi gerçek bilimsel gerçek kavramı ile bütünleşmemelidir. Nitekim bilimsel gerçeğin kesin ve objektif olduğu iddiası, çürütülebilir bir iddiadır. Bu hususta mahkemelerin maddi gerçeğe ulaşana kadar bilimsel delilleri sorgulaması ve somut davadaki vakıa ile bütünleştirmesi büyük önem göstermektedir. Bugün bilimsel delillerin klasik anlamda delillerin yerine geçtiğini söylemek mümkün değildir. Bilimsel delil sistemine ulaşıldığı ihtimalde dahi maddi vakıanın ispatında diğer deliller ile tutarlılığın sağlanması ve "insan aklının" değerlendirmesiyle vicdani kanıya varılması gerekir[644].

b) Profilleme Teknolojilerinin Bilimsel Deliller Kapsamında Değerlendirilmesi

Profilleme teknolojileri ile kişilerin hayatlarının farklı alanlarına dair sayısal verilerden yola çıkarak failin tehlikeliliği veya yeniden suç işleyeceğinin tespitine ilişkin varılan sonuçların bilimsel delil olarak değerlendirilip değerlendirilemeyeceği ele alınmalıdır. Bu değerlendirme yapılmadan önce, profilleme teknolojilerinin ceza muhakemesi alanında kullanılmasına öncülük eden Amerika Birleşik Devletleri bünyesinde bilimsel delillerin değerlendirilmesinde emsal teşkil eden Frye davası

[642] Giannelli, s. 1202.
[643] Giannelli, s. 1204.
[644] Birtek, s. 206.

incelenecektir. Bu dava ile öngörülen ve diğer ülkelerde de yankıları bulunan kabul edilirlik kıstaslarına değinilecek, ardından risk analizi yapan profilleme teknolojilerinin bu unsurları karşılayıp karşılamadığı ele alınacaktır.

Frye/Amerika Birleşik Devletleri davasında[645] yalan makinesinin öncüsü olan bir teknolojiye başvurulmuş ve bu makinenin vardığı sonucun bilimsel delil olarak kabul edilip edilemeyeceğine ilişkin unsurlar emsal olacak şekilde belirlenmiştir. Mahkeme, bilimsel bir ilkenin veya keşfin deneysel bir aşamada mı yoksa ispat edilebilir bir aşamada mı bulunduğunu tartışmıştır. Bu tür durumlarda mahkeme bilirkişinin dayandığı görüşün ve bizzat incelenen şeyin ilgili alanda "genel kabul görmüş olması" gerektiğini vurgulamaktadır. Dolayısıyla başvurulan teori ve bu teorinin olaya uygulanmasında kullanılan teknik, bilim camiası tarafından kabul edilmiş olmalıdır. Yeni bir teori ve teknik bilimsel olarak sınanmadan, eleştirilmeden ve genel kabul görmeden mahkemelerce kullanılamayacaktır[646].

Bununla birlikte Frye testi ile belirli sorulara cevap bulmak güçtür. Bilimsel bir delilden bahsedebilmek için bu delilin hangi bilim dalında kabul edilirliğinin ele alınacağı kimi durumda tartışmalı olacaktır. Başka bir deyişle, hangi bilim dalının ilgili delili inceleme yetkinliğinin bulunduğu tespit edilmesi dahi güç bir hususdur. Örneğin kişinin konuşmasının değerlendirilmesi, anotomi, fizyoloji, piskoloji ve dilbilim ile ilişkilidir. Özellikle değerlendirilen hususa göre, söz konusu alan özel uzmanlık gerektiren çok dar bir alan olabilecek ve bu alanda yetkin az sayıda kişinin onayı, "genel kabul görme" unsurunu karşılamış sayılabilecektir. İkincil olarak bilimsel delil için başvurulan ilgili teori ve pratiğin genel kabul görmesi unsuru, bu görüşlere karşı olan ve ileride haklı çıkabilecek azınlık fikirlerinin değerlendirilmemesine veya otomatik olarak kabul görmemesine yol açabilecektir[647]. Yeni bilimsel fikirler ya da yöntemler ortaya çıktığında ise bunların genel kabul görmesi değil ancak deneysel olarak veya çıkarımlarla doğrulanması mümkündür. Bu durumda yeni teknolojilerin ilgili sonuca varmayı sağlayıp sağlamadığı tümdengelim ve bilimsel toplulukta çoğunluğun görüşü üzerine kanıtlanamayacaktır, sonucun geçerliliği ancak ampirik

---

[645] 293 F. 1013 (D.C. Cir. 1923), http://www2.law.columbia.edu/fagan/courses/law_socialscience/documents/ Spring_2006/Class%203-Developments%20in%20Federal%20Rules%20of%20Evidence/Frye_v_US.pdf, Erişim Tarihi: 01.08.2021.

[646] Gianelli, s.1204, 1205.

[647] Gianelli, s.1208-1210.

(deneysel) şekilde gösterilebilecektir[648]. Örneğin parmak izi delilleri ve ateşli silah tespitleri mahkemeler tarafından deneysel olarak varılan sonuçlar üzerine kabul edilmiştir. Bu tür bir doğrulama yöntemi yeni bir soruyu doğurmaktadır: Mahkeme yeni teori, teknik ve bunlarla ulaşılan delilleri, ne kadar deneme üzerine doğru ve güvenilir bulmalıdır[649]? Bu soruya henüz yeknesak bir uygulamayı mümkün kılacak bir cevap verilememiştir. Bu nedenle bilirkişi başlığı altında tartışılacağı üzere, içtihatlarda bilimsel delilin ne zaman ve ne şekilde kabul edileceğinden ziyade, bunları yorumlayan bilirkişilerin nitelikleri ve görüşlerinin bilimselliği üzerinde durulmaktadır.

Frye testinin veya genel olarak delillerin güvenilirliği ve geçerliliği unsurlarının sosyal bilimlere uygulanabilirliği oldukça tartışmalıdır. Hafızayı hipnozla geri getirme, travma sonrası stres bozukluğunu tespit, cinsel istismar sonrası sendromları teşhis etme gibi alanlarda istisnai olarak[650] psikolojik teorinin bilimsel geçerliliği açısından Frye testinin uygulanması mümkün olabilecektir. Yine de hukuk ile diğer sosyal bilimlerin kesiştiği her noktada, söz konusu delilin niteliği ve değerlendirilmesinin Frye testinin gerektirdiği keskinlikte yapılması mümkün olmayacaktır. Bu nedenle söz konusu alanlarda ileri sürülen teorinin kesin doğruluğu ve güvenilirliğinden bahsetmek daha güç olup, bu alanlarda sunulan delillere daha fazla çekinceyle yaklaşılması gerekmektedir.

Frye testinin barındırdığı boşlukları doldurmak adına bilimsel delil ve görüşlerin değerlendirilmesinde başvurulan ilkeler zaman içinde değişikliğe uğramıştır. Bu hususta emsal niteliği taşıyan diğer bir dava Daubert/Merrell Dow Pharmaceuticals davasıdır[651]. Frye ilkeleri, bir delilin geçerliliği ve sağlamlığını bir grup bilim insanının çoğunluğu tarafından kabul görmesine bağlı olarak ele alırken, Daubert ile bir delilin güvenilirliğini tespit etmek yeniden hâkimlere bırakılmıştır. Buna göre, bilimsel bir görüş sunan ya da bilimsel bir delili yorumlayan kişilerin dayandıkları teorinin, mantık yürütme şekillerinin ve metodolojilerinin bilimsel olarak doğruluğu ve bunların dava konusu olaya doğru uygulanıp uygulanmadığı hâkimin takdirindedir. Delillerin

---

[648] Gianelli, s. 1212.
[649] Giannelli, s. 1213.
[650] David E. Bernstein,"Frye, Frye, Again: The Past, Present, and Future of the General Acceptance Test", **Jurimetrics**, Cilt:41, Sayı: 3, Bahar 2001, ss. 385-408, s. 401.
[651] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993), https://supreme.justia.com/cases/federal/us/509/579/, Erişim Tarihi: 27.07.2021.

bilimselliğini tespit, geçerliliklerine ilişkin bir değerlendirme iken, olaya doğru şekilde uygulanıp uygulanmadıklarını tespit "olayı temsil etme", "olay ile ilgili olma" unsuruna ilişkin bir değerlendirmedir[652]. Daubert kararı ile güvenilirlik ve temsil ediciliğin tespiti, bilimsel olarak geçerlilik testinin önüne geçmiştir. Bunun yanı sıra bilirkişi görüşü, bu karar ile belli kıstaslara tabi tutulmuştur. Bilirkişi açıklamaların test edilebilir olması, incelemeye ve değerlendirmeye tabi tutulabilir olması ve sunulan bilginin hata oranının istatistiksel olarak belirlenebilir olması aranmıştır. Ancak Frye ilkelerinin etkisi yine devam etmiş, bu sayılan unsurların yanı sıra tartışılan bilgilerin, ilgili bilim çevresinde kabul görmüş olması aranmaya devam etmiştir[653].

Tüm bu ilkeler ışında risk analizi yapan profilleme teknolojilerinin bilimsel delil oluşturup oluşturmadığı ele alınmalıdır. Profilleme teknolojileri, dijital verilere dayanarak oluşturulan mekanik kurallarla ileride gerçekleşecek riskin sayısal olarak tahmin edilmesine yöneliktir. Nitekim bu teknolojiler ve yaptıkları tahminlerin bilimsel delil kapsamında ele alınması sonucu Amerika'da 2019 yılında hâkimler için oluşturulan "Bilim Kitabı"nın bir bölümü, risk değerlendirme teknolojilerinin delil olarak kabul edilip edilemeyeceği tartışmasına ayrılmıştır. Bu kitapta Daubert kararına paralel şekilde, bilimsel delillerin ceza tayininde dikkate alınıp alınmayacağına ilişkin asli denetimin hâkimler tarafından yapılacağı vurgulanmıştır[654]. Dolayısıyla, profilleme teknolojileri değerlendirilirken, bilimsel deliller için aranan unsurlar bu teknolojiler açısından da aranmalıdır. Buna göre öncelikle ceza muhakemesinde başvurulan profilleme teknolojilerinin test edilebilir olması, incelemeye ve değerlendirmeye tabi tutulabilir olması gerekir. Bu unsurları karşılayabilmek adına, yazılımcıların ve istatistik uzmanlarının öncelikle programlama sırasında hangi değişkenlere başvurduklarını ve bunların sonuca etkisini paylaşmaları gerekmektedir. Bu hususta ilk engel, kişilerin yazılımları ve kodlamaları fikri mülkiyet hakları ile koruma altına almaları ve paylaşmaktan kaçınmalarıdır. İkinci engel ise makine öğrenmesi ile algoritmaların, gittikçe daha fazla veri üzerinden kendini geliştirmesi ve daha iyi tahminlere varabilmek adına farklı değişkenleri tespit etmeleri veya orijinal

---

[652] Eric S. Janus /Robert A. Prentky, "Forensic Use of Actuarial Risk Assessment with Sex Offenders: Accuracy, Admissibility and Accountability", **American Criminal Law Review**, Cilt: 40, Sayı: 4, Güz 2003, ss. 1443-1500, s.1460, 1461.

[653] Ertan Demirkapı,"Anglo-Amerikan Hukukunda Bilirkişilik Kurumunda Yeni Eğilimler", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 5, Sayı: 2, 2003, ss. 39 - 76, s.66.

[654] Ayrıntılı bilgi için bkz. Bridget Mary McCormack, "Scientific Evidence", https://www.judges.org/wp-content/uploads/Chapter3-SBBr.pdf , Erişim Tarihi: 03.08.2021, s. 14 vd.

formülden sıyrılarak bazı değişkenlerin sonuç açısından daha önemli olduğunu saptamalarıdır. Dolayısıyla kimi modeller açısından profilleme teknolojileri bazı değişkenlere kendiliğinden ağırlık vermektedir. Bu durumda kendi kendine öğrenen algoritmalar kullanıldığı takdirde ve özellikle kara kutu modeli ile işleyen sistemlerde, yazılımcının dahi açıklaması mümkün olmayan bir aşamaya erişilebilmektedir. Örneğin yazılımcı sürecin başında yüz değişken ortaya koymuş ve bunları hâkime sunmuş olsa dahi, sürecin sonunda algoritmalar bunlardan yalnızca beşine ağırlık verebilir ve sonuca bunlar üzerinden yapılan değerlendirme ile ulaşabilirler[655]. Ayrıca bu teknolojilerinin gerçek bir değerlendirmeden geçirebilmesi için öğrenme sürecinde hangi verilere başvurulduğu da bilinmelidir. Nitekim öğrenme açısından temel olan bu verilerin güncelliğini yitirmiş, hatalı ya da ayrımcı olması, varılacak sonuç açısından büyük önem taşımaktadır. Söz konusu verilerin salt kolluk tarafından toplanmış olduğu ihtimalde bu verilere ulaşmak ve denetlemek daha kolay olabilecekken, günümüzde pek çok farklı kanaldan farklı amaçlarla toplanan verilere erişmek ve bunları profilleme kapsamında kullanmak mümkündür. Ancak bir hâkimin özellikle profilleme teknolojilerine girdi olarak sunulan verilerin ayrımcılık yasağına konu ırk, din, sendikal aidiyet gibi unsurlara dayanmadığını mutlaka kontrol edebilmesi gereklidir[656]. Yine bu verilerden hangi şekilde yararlanılarak sonuca varıldığının denetlenmesinin mümkün olmaması halinde profilleme teknolojilerinin bilimsel delil olarak kabul edilmesi güç olacaktır.

Frye ve Daubert ilkelerinin neredeyse uluslararası standartlar haline geldiği göz önüne alınmalı, bilimsel delil açısından geçerlilik ve güvenilirlik değerlendirilmesi mutlaka yapılmalıdır. Delillerin bilimselliğini tespit, geçerliliklerine ilişkin bir değerlendirme iken, bilimsel yöntemin ayrıca olaya doğru şekilde uygulanıp uygulanmadığını tespit etmek gerekir.

Bir bilimsel delilin yapılan yargılamada geçerli olması için üç boyutlu bir incelemeye tabi tutulması gerekir. Bu delil, sevk edilen amaçla uyumlu olmalı, doğru sonuçlara varmalı ve güvenilir olmalıdır. Öncelikle profilleme teknolojilerinin sevk edilen amaçla uyumlu olması, yani olayın şartlarını anlamaya ve maddi olaya uygun

---

[655] Ric Simmons, "Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System", **Michigan State Law Review**, Sayı: 4, 2016, ss. 947-1018, s. 996, 997.
[656] Simmons, s. 998.

sonuç çıkarmaya elverişliliği değerlendirilmelidir. Aslında "fitness" olarak ifade edilen bu unsur profilleme teknolojilerinin ceza yargılamasında varılmak istenen amaca uygunluğunun dışsal bir şekilde denetlenmesini ifade eder. Bu bağlamda kişinin gelecekte suç işleyeceğini istatistiksel olarak gösterme iddiasındaki bir profilleme teknolojisi, dava konusu suçun işlenip işlenmediğini tespit etmeyi amaçlayan ceza muhakemesi süreci için uygun bir araç olmayacaktır. Nitekim bir kişinin tehlikeliliği, mevcut davada suçlu olduğunu ispat etmez. Bu tarz algoritmalar, suçun tespitinden ziyade suçun infaz şekline, örneğin kişiye uygun bir rehabilitasyon yönteminin belirlenmesine uygun bir araç olabilir. Yine kişiye ne tür denetim tedbirlerinin uygulanacağını belirlemede yeniden suç işlemeye meyilli olup olmadığı dikkate alınabilir. Kendi içerisinde doğru ve geçerli sonuca varsa da belirli bilimsel metotlar, farklı amaçlara hizmet etmeye elverişli değildir. Örneğin suçu tespit etmek üzere sevk edilen bir yöntem, infaz amacına uyumlu olmayabilir. Yine ticari amaçlı potansiyel müşterilerin profilini çıkaran teknolojilerin, ayrımcılık yasağı, masumiyet karinesi, susma hakkı gibi pek çok hak ve ilke ile donatılmış ceza muhakemesinde kullanılması uygun değildir. Nitekim bu değerlendirme en bilinen profilleme teknolojilerinden COMPAS'ın ele alındığı Wisconsin davasında yapılmış, mahkeme bu teknolojinin ceza muhakemesi alanında kullanımını tamamen yasaklamamakla birlikte amaca uygunluk açısından önemli değerlendirmeler yapmıştır. Mahkemeye göre, daha çok kaçma ve yeniden suç işleme riskini belirleyen COMPAS yazılımı, bir sanığın hapis cezası alıp almaması gerektiğinin tayininde kullanılırsa "amaca uyumsuz" bir araçtır.[657]. Yine Indiana Yüksek Mahkemesi, verdiği kararda risk analizi yapan profilleme teknolojilerinin, cezanın süresi ve verilecek cezanın hafifletilmesi veya ağırlaştırılmasını tayin için uygun bir araç olmadıkları, bunların ancak infaz rejimi hususunda dikkate alınabileceğini belirtmiştir[658]. Benzer şekilde bir kişinin duruşmalara katılmama riskini tespit eden profilleme teknolojilerinin suçluluğun ve cezanın tespitinde kullanılmaması, yine şiddete eğilim ve akıl sağlığı tespit eden profilleme teknolojilerinin tüm nüfusa yönelik uygulanmaması gerekir[659].

[657] State v. Loomis, 881 N.W. 2d 749, 768 (Wisc. 2016), aktaran Melissa Hamilton, "Judicial Gatekeeping on Scientific Validity with Risk Assessment Tools", **Behavioral Science Law**, Cilt:38, Sayı:3, 2020, ss 226–245, s. 228.
[658] Malenchik v. State, 928 N.E.2d 564, 575 (Ind. 2010), aktaran Hamilton, "Judicial Gatekeeping", s. 229.
[659] Hamilton, "Judicial Gatekeeping", s.229.

Amaca uygunluğun yanı sıra, bilimsel deliller mutlaka kabul görmüş ve ilgili alanda geçerliliği kanıtlanmış olmalıdır. Geçerlilik unsuru, bir grubu diğer gruptan doğru ayırt edebilmeyi ve gerçek koşullara uygun olmayı içerir. Bununla birlikte risk değerlendirme teknolojilerinin bilimsel geçerliliği, yazılımcılar tarafından değerlendirilirken, rastgele bir tahmine nazaran daha yüksek oranda, yani yüzde elli bir tahmin başarısı bulunan algoritmaların yeterli olarak addedildiği görülmektedir[660]. Oysa profilleme teknolojilerinin, yarıdan yüksek oranda başarı göstermeleri, kişi hak ve özgürlüklerinin büyük ölçüde kısıtlandığı ceza muhakemesi alanında yetersizdir. Bununla birlikte hangi oranda doğruluk payı yakalandığında hâkimlerin ilgili profilleme uygulamasını bilimsel olarak yeterli kabul etmesi gerektiğine ilişkin açık bir norm bulunmamaktadır.

Yargılamada başvurulan profilleme teknolojileri değerlendirilirken, ilkin profilleme teknolojilerinin uygulandığı alan dikkate alınmalı, örneğin itiyadi suçlu olma-olmama, duruşmalara katılma-katılmama gibi tespit edilmek istenen grupların başarılı şekilde ayrılıp ayrılamadığı değerlendirilmelidir. Eğer algoritmaların tekrar suç işleyeceğine dair riskli bulduğu kişiler suç işlemezse veya örneğin bir ülkede çoğunluğu oluşturan gruplar, yeniden suç işlediği halde algoritma tarafından "tehlikesiz kişi" olarak atfedilmişse ilgili teknolojinin ayırt etme ayırma başarısının düşük olduğu kabul edilecektir. Örneğin COMPAS uygulaması, vardığı sonuçlarda Hispanik kökenli kişilere ilişkin yüksek risk göstergesinde sapmalar içermekte[661], bu durumun hâkimler tarafından daha ihtiyatlı değerlendirmeye tabi tutulması gerekmektedir.

Son olarak profilleme teknolojileri bilimsel delillerin güvenilir olması unsuru açısından değerlendirilmelidir. Yukarıda tartışıldığı üzere ayırt etme ve doğruluk kapasiteleri yeterli olmayan profilleme teknolojilerinin güvenilirlik unsurunu tartışmaya gerek kalmaksızın bilimsel delil niteliği taşımadıkları kabul edilmelidir. Güvenlik unsuru, bu iki unsur karşılandıktan sonra değerlendirilmesi gereken bir husus olup, profilleme sisteminin doğru şekilde işlediğini kanıtladıktan sonra bireysel olaylara özgülenmesini ele alır. Bu aşamada insan müdahalesi gerekir, nitekim profilleme sisteminin özel olarak belli kişilere yönelik uygulanması söz konusudur.

[660] Hamilton, "Judicial Gatekeeping", s.230.
[661] Hamilton, "Judicial Gatekeeping", s.230, 231.

Varılan sonuçlar, hukuki bir karara temel olacağından, adli bir merci tarafından değerlendirilmelidir. Böylelikle sistemin çalışma şekli gözetimden geçirilmiş ve sonuç bireyselleştirilmiş olur. Bu aşamalar, yargılamada klinik psikologların geleneksel şekilde takip ettiği aşamalara benzemektedir. Kişilik veya akıl sağlığı incelemesi yapan psikologların değerlendirme yöntemleri de bir nevi profillemedir. Psikologlar öncelikle genelgeçer risk faktörlerini dikkate alır, ardından bilgi ve tecrübelerini olaya uygularken ilgili kişinin semptomlarını, karakterini ve mevcut sorunlarını öncelikli olarak değerlendirir ve buna göre çözüm üretirler. Profilleme teknolojilerinin de olay özelinde ilgili kişiye göre belli hususları ağırlıklı olarak dikkate almaları gerekebilir. Örneğin ilgili kişinin eğitim hayatında yaşadığı güçlükler, ailevi sorunlar, sosyal problemleri yapılacak değerlendirmede öncelikli önem taşıyabilir. Bu bağlamda, kullanılan profilleme teknolojisinin ışık tutulmak istenen hususla ilişkili ve buna uygun bir teknoloji olması ve yine yargılama konusu kişinin bireysel özelliklerini göz ardı etmeden, onun özel durumunu içeren faktörleri de barındırması gerekir. Aksi halde profilleme ile varılan sonuçlar genellemelerden ibaret olacaktır. Ancak her hâlükârda ilgili teknolojinin işleyişi ve bu işleyişin dayandığı teori bilimsel olarak geçerli değilse, söz konusu uyarlama ve bireyselleştirme aşamasına gerek kalmaksızın profilleme sonuçları bilimsel delil olarak kabul edilmemelidir[662]. Profilleme teknolojilerinin dayandıkları teorilerin bilimsel geçerliliğinin henüz kanıtlanmadığı görülmektedir. İleride bu teoriler kanıtlansa dahi bu teknolojilerin, gruplara dayalı genel istatistikler çıkarması, dolayısıyla ilgili kişiye ait verileri, bağlamı ile birlikte ele almaksızın hakkında puanlamalar yapması, bireysel bir değerlendirme yapmaya elverişli olmadıklarını göstermektedir.

Sonuç olarak profilleme teknolojilerinin vardığı sonuçların ceza muhakemesinde bilimsel delil olarak değerlendirilmesi pek çok sorunu barındırmaktadır. Bunlardan ilki sayısal (dijital) delillerin bile sağlamlığı ve güvenilirliğinin güçlükle teyit edilmekteyken, profilleme teknolojileri milyonlarca sayısal veriye dayanmasıdır. Profillemede kullanılan verilerin kaynağını, orijinalliğini, güncelliğini ve hukuka uygun elde edildiğini teyit etmek mümkün olmamaktadır. Her ne kadar kişisel verileri koruma kanunları bu hususta bir güvence oluştursa da bu kanunlar temelde kişilerin bireysel haklarını kullanmaları üzerine inşa edilmiştir. Oysa

[662] Hamilton, "Judicial Gatekeeping", s. 240.

pek çok kişi hala verilerini talep etme, güncelleme veya silinmesi için başvurma haklarına sahip olduklarından habersizdir. Bunun yanı sıra söz konusu hakların ceza muhakemesi alanında kısıtlanmaları mümkündür.

Kullanılan verilerin yanı sıra, bu teknolojilerin vardığı sonuçların bilimselliği de tartışmalıdır. İlkin reklamcılık ve ticaret amaçlı sevk edilen profilleme teknolojileri, bugün artık failin gelecekte işleyeceği suçları veya yeniden suç işleyip işlemeyeceğini tespit gibi oldukça genel ve gerçekleştirilmesi güç bir amaca soyunmuştur. Ancak bu amacın, failin zamansal olarak geçmişte kalan suçu işleyip işlemediğini tespit etme veya cezasını tayin etme amacı ile örtüştüğünü söylemek mümkün değildir. Kaldı ki bu sistemlerin geleceğe yönelik riskleri tespit etme amaçlarına ulaşmada başarısı ve doğruluk payı amprik olarak henüz kanıtlanmamış, aksine belli kişiler açısından hatalı yüksek puan (false positives), yine belirli gruplar açısından hatalı tehlikesiz puan (false negatives) öngördükleri anlaşılmıştır. Bunun yanı sıra üzerinde sıklıkla durulan "kara kutu" problemi nedeniyle, kendine kendine öğrenen sistemlerin kullanılması halinde, bu yazılımların hangi verileri ne şekilde değerlendirerek ilgili sonuçlara ulaştığının açıklanması ve bilimselliklerinin denetlenmesi oldukça güç olmaktadır. Dolayısıyla profilleme teknolojileri ile ulaşılan sonuçlar bilimsel geçerlilik, doğruluk ve sağlamlık unsurlarını karşılayamamaktadır. Bu nedenle söz konusu sonuçların bilimsel delil olarak kabul edilmemesi gerekir.

C. Delil Aracı Olarak Profilleme Teknolojileri

1. Bilirkişilik

a) Genel Olarak Bilirkişilik Kavramı

Muhakeme süjelerinin, maddi uyuşmazlığın konusu tüm olay ve olguları ve bunları temsil eden delilleri anlamlandırmaları ve bu yolla maddi gerçeğe ulaşmaları için hayat tecrübeleri her zaman yeterli olmayacaktır. Nitekim her konu hakkında bilgi sahibi olmaları bu süjelerden beklenemez. Böyle durumlarda, başkalarının bilimsel ve teknik bilgisine başvurmaları gerekir. Bir delilin içeriğinin öğrenilmesi veya değerlendirilebilmesi için, bilimsel veya teknik bilgi gerektiğinde veya çözümü

uzmanlık veya özel bilgiyi gerektiren bir sorunla karşılaşıldığında, aranan tecrübe ve bilgiye sahip olan ve mahkeme veya savcı tarafından atanan kişi bilirkişidir[663].

Bilirkişiden yalnızca uzmanlık alanına dair tecrübe kurallarını ve teorik bilgilerini aktarması talep edilebilir. Örneğin, hangi dozda uyuşturucunun vücuda alınması halinde öldürücü olacağına dair bilgi bilirkişiden talep edilebilir. İkinci olarak, bilirkişiden, ancak sahip olduğu özel bilgi sayesinde belli olguları veya durumları saptaması istenebilir. Örneğin, ölen kişinin kanında morfin olup olmadığını saptama konusunda bilirkişinin görüşüne başvurulabilir. Son olarak bilirkişiden belli bir konuda sahip olduğu bilgi ve tecrübe ile tümevarım yöntemi kullanarak analiz yapması ve sonuç çıkarması talep edilebilir. Bu duruma örnek olarak bir kişinin yalnız kalp ritminde aksaklık olmasını belirlemek değil, kalp ritmindeki aksaklık nedeniyle ölüp ölmediğinin tespit etmek için bilirkişiye başvurulabilir. Bilirkişiden bu üç tespit türünü birlikte yapması da talep edilebilir. Sonuç olarak bilirkişi, kanunda bilirkişi atamaya yetkili olarak gösterilen merci tarafından, maddi uyuşmazlıkla ilişkili bir konuda, uzmanlığı, özel veya teknik bilgisi nedeniyle çeşitli saptamalar yapması veya sonuç çıkartması istenen, böylelikle delil değerlendirme araçlarını sunan kişi olarak tanımlanabilir[664].

Uygulamada "teknik müşavir", "taraf bilirkişisi" olarak anılan ve kanunda uzman olarak adlandırılan kişi ise yine bilirkişi gibi özel veya teknik bilgisi nedeniyle kendisinden değerlendirme yapması ve belli sonuçlara varması beklenen kişidir. Bu kişinin bilirkişiden farklı şekilde nitelendirilmesinin nedeni, uzman mütalaasına soruşturma evresinde savcı, kovuşturma evresinde hâkim dışındaki kişilerce başvurulabilmesidir[665]. CMK m. 67 uyarınca uzman mütalaasına, kesin hüküm verilinceye kadar yargılama konusu olayla ilgili olarak veya bilirkişi raporunun hazırlanmasında dikkate alınmak üzere başvurulabilir. Yine CMK m. 67/6 uyarınca bilirkişinin verdiği rapor hakkında da uzman mütalaası alınabilir.

Maddi gerçeğe ulaşmaya hizmet etme ve silahların eşitliğini tesis etme bakımından uzman mütalaası büyük önem taşımaktadır. Böylelikle çözümü özel bilgi

---

[663] Öntan, s.17.
[664] Öntan, s. 18, 19.
[665] Centel/Zafer, s. 332.

gerektiren bir konuda daha fazla tartışma alanı açılmış, iddia ve savunma tezlerini güçlendirme ve çelişkileri giderme fırsatı yakalamış olur[666]. Kanunda yetkili merci tarafından atanan bilirkişiden ayırmak adına uzman ifadesine ayrıca yer verilmiş olsa da tarafların başvurduğu uzmanlar da aslında bilirkişidir ve bu nedenle yetki ve yükümlülükleri atanan bilirkişilerden farklı değildir[667]. Nitekim CMK m. 68/3'e göre, bilimsel mütalaa hazırlayan uzmanın duruşmada dinlenmesi hususunda bilirkişiye ilişkin hükümler uygulanacaktır.

Uzmanın ve bilirkişinin duruşmaya davet edilerek dinlenmesi mümkündür. CMK m. 178 uyarınca uzmanın veya bilirkişinin çağrılması hakkındaki dilekçe reddedilse dahi, sanık veya katılan, uzmanı doğrudan duruşmaya getirebilecek ve bu halde uzmanın dinlenmesi zorunlu olacaktır[668]. Yine CMK m. 201 gereğince, bilirkişiye ve uzmana soru yöneltilebilecektir. Bilirkişi raporu ve uzman mütalaası yetkili mercii bağlayıcı değildir, ancak bunlar tartışılmadan veya hükme neden esas alınmadıkları gerekçelendirilmeden karar verilirse, eksik değerlendirme ile sonuca varılmış olur.

Dolayısıyla yetkili merciin atadığı bilirkişinin, tarafların başvurduğu uzmana karşı herhangi bir üstünlüğü yoktur. Bu nedenle tekrar edilmesi mümkün olmayan, yalnızca bir kez incelemenin mümkün olduğu delillerin söz konusu olduğu istisnai durumlar hariç, bilirkişi kadar uzmanın da inceleme yapması mümkün kılınmalı, yaptığı değerlendirmeler dikkate alınmalıdır[669]. Bununla birlikte uzmanlara iddia ve savunma tarafından başvurulmuş ve mütalaa ücretinin taraflarca karşılanmış olması nedeniyle uzmanların ilgili tarafın tezlerini güçlendirecek mütalaa vereceği veya aksi halde bu mütalaanın mahkemede taraflarca ileri sürülmeyeceği iddia edilebilir. Bu iddia, uzmanın bilirkişiye nazaran daha taraflı olma ihtimalini gündeme getirmektedir. Bununla birlikte uzmanların da akılcı, bilimsel, objektif görüşleri ile maddi gerçeğe hizmet etmekle yükümlü olduğu unutulmamalıdır. Yine uzmanların, bilirkişi raporunda gözden kaçan hususlara parmak basabileceği, eksikleri giderebileceği, farklı bilimsel açıklamalarla sürecin aydınlatılmasına katkı sunabileceği dikkate alınmalıdır. Nitekim bilimsel nitelikleri taşıyan bir mütalaanın uzman tarafından

[666] Öntan, s. 193, 194.
[667] Centel/Zafer, s. 332.
[668] Centel/Zafer, s.333.
[669] Öntan, s.196.

hazırlanmış ve sunulmuş olması, bilirkişi mütalaasından daha az önemde olmasını gerektirmeyecek ve delil değerlendirme aracı olarak kabul edilmesine engel olmayacaktır[670].

Son olarak bilirkişi kavramı ile tanık bilirkişi kavramının ayrımı üzerinde durulmalıdır. Tanık beyanı başlığı altında irdelendiği üzere tanık bilirkişi, maddi olaya şahit olan ve aynı zamanda olayda çözümü özel bilgi gerektiren sorunu çözecek uzmanlığa sahip kişidir. Örneğin bir patlama anına şahit olan ve patlayıcılar hakkında uzman olan bir kişi, tanık bilirkişidir. Ancak bir olaya şahit olan kişinin yerine başka tanık bulmanın güçlüğü karşısında, tanıklık sıfatı ön plana geçecek, bu kişi bilirkişiden ziyade tanık sıfatıyla muhakeme sürecine katılacaktır[671].

Bilirkişi görüşünün hukuki niteliği ulusal ve uluslararası doktrinde tartışmalıdır. Doktrinde bir görüş bilirkişinin sahip olduğu özel ve teknik bilgi ile hâkimin yardımcısı olarak görev aldığını belirtmektedir[672]. Bu görüşe göre, bilirkişi teknik konularda neticeler çıkartarak hâkime yol göstermektedir. Delillerin takdiri her zaman hâkim tarafından yapılacağından bilirkişi "yardımcı" konumunda kalacaktır. Bu önemli ödevi nedeniyle hâkimin reddedilmesine ilişkin hükümler bilirkişiler açısından da geçerlidir[673]. Ancak bilirkişiliğin hukuki niteliğini yargıcın ve savcının yardımcılığına indirgemek yeterli değildir. Bilirkişinin görüş ve değerlendirmelerinden, muhakeme süjelerinin hepsi yararlanmaktadır. Bu yüzden, bilirkişi, yalnızca kendisini görevlendiren yetkili merciin değil tüm muhakeme süjelerinin yardımcısıdır. Nitekim CMK m. 67 ile iddia ve savunma da bilirkişi görüşlerini değerlendirebilecek ve bu görüşlere itiraz edebilecektir. Yine aynı madde ile uzman görüşleri bilirkişi mütalaasına eş görülmüş, bilirkişi raporunun hazırlanmasına yardımcı olacak veya verilmiş rapora karşı çıkacak şekilde uzman görüşü alınması mümkün kılınmıştır. Bu durum çelişmeli yargı ilkesinin gereği olup bilirkişinin yalnızca kendisini görevlendiren yetkili merciin yardımcılığının ötesinde bir ödevi olduğunu göstermektedir[674].

---

[670] Öntan, s. 197.
[671] Öntan, s.20, 21.
[672] Cihan, Erol/Yenisey, Feridun, **Ceza Muhakemesi Hukuku**, Beta Yayınevi: İstanbul, 1998, s. 195.
[673] Erem, **Ceza Muhakemesi Hukuku**, s. 433.
[674] Öntan, s. 11.

Yine bilirkişinin tanıklara benzer şekilde değerlendirilmesi gerektiği doktrinde ileri sürülmüştür[675]. Tanıklar da bilirkişiler gibi adli makamlar önünde beyanda bulunurlar ve dinlenme ile davet edilme usulleri açısından ortak hükümlere tabidirler. Bununla birlikte mahkeme veya savcı, bilirkişiye ancak lüzum görürse başvurur ve bilirkişi açısından ilgili teknik bilgiye sahip herhangi bir kimsenin seçilmesi mümkündür. Başka bir deyişle bilirkişi ikame edilebilir. Ancak olaya bizzat şahit olmuş tanığın dinlenmesi gerekir ve bu kişi yerine başkasının dinlenmesi mümkün değildir. Bunun yanı sıra bilirkişilik için belli tahsil ve bilgiye sahip olmak zorunlu iken, maddi olayı beş duyusuyla algılamış herhangi bir kişinin tanık olabilmesi mümkündür. Dolayısıyla bu iki müessese birbirine benzemekle birlikte farklıdırlar[676]. Bilirkişi maddi olay hakkında bilgi sahibi değildir. Yalnızca teknik bilgisini sunar ve bu bilgi, delil içeriğinin öğrenilmesi ve tecrübe kuralları ile olayın irdelenmesi için kullanılır[677].

Bilirkişiliği bir ispat aracı olarak görmeyen, ancak bir delil değerlendirme aracı olarak bulan görüş de dikkate alınmalıdır[678]. Kunter bilirkişiyi bir belgeyi okumaya yardım eden gözlüğe benzetmekte, belgeyi okumaya yarayan gözlük nasıl delil değilse, bilirkişi ve onun mütalâasının da delil olamayacağını belirtmektedir[679]. Şayet muhakeme süjeleri, muhakeme sürecinde geçmişte olan olayların yeniden inşası için iz ve eserleri ancak bilirkişiye başvurmak suretiyle öğrenebiliyorlarsa, bu durumda bilirkişi görüşü delile ulaşma aracıdır. Örneğin, vücudun muayene edilerek delile ulaşılması veya vücuttan örnek alınması sürecinde bilirkişilik kurumu, bir delile ulaşma aracıdır. Eğer bilirkişi delile ulaşılmasının ardından konuyla ilgili bir tecrübe kuralını açıklıyor veya buna dayalı saptamalar yaparak sonuç çıkartıyorsa, bilirkişi görüşü delil değerlendirme aracıdır. Örneğin yargılama konusu olayda, mağdurun işitme duyusundaki azalmanın yaralama fiili sonucu gerçekleştiğini tespit eden bilirkişi, delil değerlendirme aracıdır[680]. Dolayısıyla, bilirkişi incelemesinin delillere ulaşmak veya delilleri değerlendirmek için bir araç olduğunu, bilirkişi incelemesi

---

675 Löwe, Ewald/ Roenberg, Werner StPO Grosskommentar, 24. Auflage Berlin 1987'den aktaran Öztürk, Bahri/ Erdem, Mustafa Ruhan/ Özbek, Veli Özer, **Uygulamalı Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, 2004, s. 495.
676 Erem, **Ceza Muhakemesi Hukuku**, s. 434, 435.
677 Kunter, **Ceza Muhakemesi Hukuku**, s. 610.
678 Erem, **Ceza Muhakemesi Hukuku**, s. 433, Kunter, **Ceza Muhakemesi Hukuku**, s. 611.
679 Kunter, s. 611.
680 Handan Yokuş Sevük, "Ceza Muhakemesi Hukukunda Bilirkişilik", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 64, Sayı: 1, 2006, ss. 49 - 107, s. 51.

sonucu elde edilen iz, eser veya emarenin ise delil olduğunu söylemek mümkündür[681]. Nitekim olayı temsil yeteneğine sahip olmayan bilirkişi raporunun bizzat bir delil olarak nitelendirilmesi mümkün değildir. Bu raporu sunan bilirkişi, yalnızca gerçeğe ulaşmak için başvurulan bir araç ya da köprü görevi görmektedir[682].

Her ne kadar bilirkişi raporu, bizzat olayı temsil eden bir delil olmasa da delillerde aranması gereken diğer özellikleri haiz olmalıdır. Bu bağlamda, akla, mantığa uygun olma, güvenilir ve sağlam olma, hukuka uygun olma ve müştereklik bilirkişi raporlarında da mutlaka söz konusu olmalıdır[683].

Kural olarak bir konuda bilirkişiye başvurmanın gerekli olup olmadığını soruşturma aşamasında savcı, kovuşturma aşamasında da mahkeme takdir edecektir. Bununla birlikte kanun koyucu bazı hallerde özel hükümlerle teknik ve özel bilgi gerektiren durumları önceden öngörmüş ve yetkili merciin bu konuların çözümü için bilirkişi gerekip gerekmediğine dair takdirini sınırlandırmıştır[684]. Örneğin para ve benzeri değerlerde sahteciliğin tespiti (CMK m. 73), gözlem altına alma kararı için kişinin akıl sağlığının incelenmesi (CMK m. 74), moleküler genetik incelemelerin yapılması (CMK m.78), zehirlenmenin tespiti (CMK m.89) bilirkişi incelemesi yapılmasının zorunlu olduğu hallerdir. Bu durumlarda bilirkişi raporu dışında başka bir araçla olayın çözümlenmesine izin verilmemiştir[685].

Bununla birlikte, bilirkişi görüşüne başvurmanın zorunlu olduğu hallerde dahi hâkim bilirkişi görüşü ile bağlı değildir. Bu hallerde yalnızca hâkimin bilirkişi görüşüne başvurmadan hüküm vermesi mümkün olmamaktadır[686]. Buna rağmen, hâkim, bilirkişinin raporunu çelişkili veya yetersiz bulabilir, yeni bir görüş alınması veya sunulan görüşün hükme esas alınmamasına karar verebilir. Nitekim zorunlu tutulan veya tutulmayan tüm bilirkişi görüşleri açısından hâkim şüphe ortadan kalkıncaya kadar yeni delil ve delil araçlarına başvurmalıdır. Bununla birlikte bilirkişi

[681] Centel/Zafer, s. 321.
[682] Birtek, s. 217, 218, Öntan, s. 16.
[683] Birtek, s. 218.
[684] Centel/Zafer, s.324.
[685] Bu nedenle doktrinde söz konusu hallerde bilirkişi incelemesi olmadan hüküm kurulmasının mümkün olmadığı, bir nevi yasal delil sisteminin yaratıldığı belirtilmektedir, bkz. Centel/Zafer, s. 334.
[686] Birtek, s. 224.

raporlarının yetersiz bulunması ve hükme esas alınmamasını gerekçeleriyle açıklamalıdır[687].

Adil yargılanmanın tesisi için bilirkişi raporları, uzman mütalaaları ve bunların müşterek şekilde tartışılması büyük önem taşımaktadır. Bilirkişi raporları ve mütalaaların birbirleriyle ve dosya içeriğindeki delillerle çelişmemesi, çelişkiler bulunduğu takdirde bu çelişkilerin giderilmesi gerekir. Yine bilirkişi raporları ve uzman mütalaaları hâkimin değerlendirme süzgecinden geçmeli, doğrudan delilmişçesine ele alınmamalıdır. Aksi halde bilirkişinin görüşü, hâkimin hukuki bilgisinin süzgecinden geçmeksizin ceza adaletini bilirkişi adaletine dönüştürecektir[688]. Nitekim CMK m. 67/3 de açıkça bilirkişilerin, özel veya teknik bilgiyi gerektiren hususlar dışında açıklama yapamayacağını, hukukî nitelendirme ve değerlendirmelerin hâkim tarafından yapılacağını düzenlemektedir.

b) Profilleme Teknolojileri ile Bilirkişiliğin Karşılaştırılması

Suçlu profili çıkarılması aslında akıllı sistemlerden çok önce suçla mücadelede sıkla başvurulan bir yöntemdir. Ancak Kıta Avrupası'nda mahkeme önünde suçluların kişisel nitelikleri ve psikolojilerini irdeleyerek profil çıkaran uzmanların dinlenmesine sıklıkla başvurulmamıştır. Amerika Birleşik Devletleri ve İngiltere'de ise kolluğun daha önce işlenen suçlar ve mevcut olaya ilişkin çıkardığı profiller dikkate alınmaktadır. Bu profiller çıkartılırken, mağdur-fail arası bağ, suç mahalli, coğrafi analiz, fiziksel delil ve suçun işleniş şekli gibi pek çok özellik birleştirilmiş ve bu bilgilerle faillerin yaşı, cinsiyeti, eğitim seviyesi, sosyal statüsü, sosyoekonomik durumu ortaya çıkarılmaya çalışılmıştır. Çıkartılan fail profilinin nitelikleri ile eşleşen kişilere yönelik koruma tedbirleri uygulanmış veya dava sırasında profile uygunluk aleyhe bir görüş beyanı olarak sunulmuştur[689]. Bugün profilleme yazılımları, sınırlı sayıda dava dosyası ile kalmayıp dijitalleştirilmiş milyonlarca veri üzerinden işlemektedir. Aslında kolluk görevlileri tarafından klasik anlamda gerçekleştirilen profillemenin, teknoloji eliyle büyük ölçekli hale geldiğini söylemek mümkündür.

---

[687] Birtek, s. 226.
[688] Birtek, s. 228, 229.
[689] Caroline B. Meyer, "Criminal Profiling as Expert Evidence?: An International Case Law Perspective", İçinde **Criminal Profiling: International Theory, Research, and Practice**, Ed. Richard N. Kocsis, Humana Press: New Jersey, ss.207-247, s.209.

Bununla birlikte otomatik yöntemlerle profil çıkarma, geleneksel suçlu profillemesinden farklar barındırmaktadır. Aşağıda öncelikle geleneksel profillemeye dayanan bilirkişi görüşleri ve bunların karşılaştırmalı hukukta ne şekilde değerlendirildiği ele alınacak, ardından tezin konusu kapsamındaki otomatik yöntemlerle gerçekleştirilen profillemeye ilişkin değerlendirme yapılacaktır.

Failin davranışsal açıdan değerlendirilmesi, özellikle mağdur ile fail arasında çıkar çatışmasının bulunmadığı ve suçun saikinin aydınlatılamadığı durumlarda söz konusu olur. Başka bir deyişle geleneksel anlamda profilleme, içinde psikopatolojik ögeler barındıran seri katil, ölü sevici gibi faillerin bulunduğu veya bombalama, rehin alma, ayinsel suç teşkil eden eylemler gibi belli tür eylemlerin gerçekleştiği olaylarda ağırlıklı olarak kullanılmaktadır[690]. Suçlu profilleme, özellikle 1970li yıllarda Amerika'da Federal Soruşturma Bürosu (FBI) çerçevesinde sistematik bir şekilde gerçekleştirilerek bir nevi "bilimsel temellere" oturtulmaya çalışılmış ve Davranış Bilimleri Ünitesi (Behavioral Science Unit)[691] kurularak bu birimde çalışan psikolog, psikiyatrist, kriminalist, istatistikçi, sosyolog, doktor ve kolluk görevlilerinin görüşleri kimi davalarda dikkate alınmıştır. İngiltere'de ise soruşturma sırasında psikolojik profil çıkarmaya yoğunlaşan "investigative psychology" isimli ayrı bir dal oluşturulmuştur[692]. Ceza muhakemesinde profillemeye konu hipotez ve istatistiksel analizler, denetlenmeye, dolayısıyla doğrulanma ve yanlışlanmaya açık yöntemlere dayanmaktadır. Buna rağmen, suç soruşturmalarının kesin formüllerle çözülmesi mümkün değildir. Her olayın kendine özgü yönleri ve her suç yolunun kendine has ayrıntıları vardır. Bu nedenle, genel geçer suçlu profilleri bir olayda rol oynarken, başka olayda, olaya özgü verilerin farklılığı veya yetersizliği nedeniyle etkisi az olabilir. Dolayısıyla suçlu profilleme, suçu aydınlatamaz, ancak soruşturma aşamasında yardımcı olabilir. Nitekim profilleme, kesin bir bilim değildir[693], profillemenin otomatik olarak belirlenen sonucu da matematiksel keskinlik içermemektedir.

---

[690] Aydın, Fatih, **Suçlu Profilleme**, Adalet Yayınevi: Ankara, Mayıs 2011, s.4
[691] Suçlu profillemenin tarihine ilişkin daha detaylı bilgi için bkz. Aydın, s. 9 vd.
[692] Aydın, s. 13. Benzer şekilde Kanada, Rusya, İrlanda, Hollanda, Güney Afrika, Yeni Zelanda ve Malezya'da da soruşturmalarda suçlu profillemenin kullanıldığı görülmektedir, bkz. Aydın, s.10.
[693] Aydın, s. 18.

ABD ve Kanada'da suçlu profilleme genellikle bilirkişi görüşü olarak ele alınmaktadır. Bu alanda uzman görüşleri de bilirkişi mütalaasına ilişkin içtihatlara uygun şekilde ele alınmaktadır. Bununla birlikte delil olarak kabul edilebilmesi için bilirkişi görüşünün belli ölçütlere uyması aranmıştır. Bu ölçütlerin oluşmasında bilimsel delillere ilişkin Frye ve Daubert kıstasları, bilirkişi görüşü açısından da büyük önem taşımaktadır. Yukarıda ele alındığı üzere 1923 tarihli Frye/Amerika Birleşik Devletleri davasında Columbia Bölgesi Temyiz Mahkemesi, yalan makinesinin öncüsü olan bir teste dayanarak oluşturulan delilin hükme esas alınmamasını yerinde bulmuştur. Mahkeme kararında bilirkişi raporunun bilim dünyasında genel kabul görmüş bir ilke ya da keşiften yola çıkması gerektiğini belirtmiştir[694]. 1923 tarihli bu karara kadar mahkemeler, bilirkişi delilinin değerlendirilmesinde yalnızca iki kıstas gözetmişlerdir. Bunlardan ilki zaten bilirkişiye başvurmak için ön koşul olan, olayı çözümlemek için genel bilginin yanı sıra uzmanlık gerektiren bir alanda bilgiye ihtiyaç duyulmasıdır. İkinci olarak ise ilgili bilirkişinin alanında tanınması ve belli nitelikleri taşıması aranmalıdır. Eğer alanında ünlü ve başarılı bir kişi söz konusu ise, görüşleri delil olarak kabul edilmektedir. Ancak Frye kararı, yalnız bilirkişinin niteliklerinin değil, söylediklerinin içeriğinin de denetlenmesini gerektirmiştir. Özellikle ileri sürdüğü görüş, yeni bir bilimsel iddia taşımakta ise, bu iddia deneysel aşamada kabul edilmeli ve mahkeme bu tür bir iddiayı kabul etmeden önce, bu iddianın aynı alandaki diğer bilim insanlarınca onaylanıp onaylanmadığını dikkate alınmalıdır. Yalnızca bilim dünyasında genel kabul gören iddialar bilimsel olarak değerlendirilebilir ve karara esas alınabilir[695].

"Genel kabul görmüş olma" kriteri bir nevi mahkemelerin bilimsel olguları değerlendirmesi ve ilgili alanda bilim insanlarının çoğunluğunun bir görüşü benimsediğinin hukuki olarak tasdik etmesi anlamına gelmektedir. Frye kriteri, bu nedenle eleştiriye uğramış, bir teori ya da metodun genel kabul görmesinin bilimsel bir değerlendirme olduğu, ancak bu değerlendirmenin ilgili delilin hükme esas alınabilmesi için yeterli olmadığı ileri sürülmüştür. Frye kararında öngörülen ilkelere alternatif olarak bilirkişinin uygun donanım ve bilgiye sahip olduğu durumlarda bilirkişi görüşünün doğrudan Amerikan hukuk sistemi özelinde jüriye sunulması önerilmiştir. Başka bir deyişle, ilgili raporun içeriği Frye kriterine dayanarak

[694] 293 F. 1013 (D.C. Cir. 1923). 27, kararı aktaran Bernstein, s. 388.
[695] Meyer, s.209.

değerlendirilip baştan elenmemeli, öncelikle jüri önüne taşınarak tartışmaya açılmalıdır[696].

1975 tarihinde yürürlüğe giren Federal Delil Kuralları da benzer şekilde bilirkişinin niteliklerini ön plana çıkarmakta, ancak bilirkişi raporunun hangi şartlarda kabul edilebileceğine dair yeterli kıstaslar öngörmemektedir. Bununla birlikte bu düzenleme bünyesindeki 702. madde dikkate alınmalıdır. İlgili madde uyarınca bilimsel, teknik ve özel bilgi gerektiren alanlarda uyuşmazlık konusunu ortaya çıkarmaya, maddi olaya ilişkin delilleri anlamlandırmaya ve olgusal gerçekleri aydınlatmaya yardımcı olabilecek yetkinlikte kişiler görüş bildirebilir[697]. İlgili maddede beyanın yeterli veri veya olgulara dayalı olması, güvenilir ilke ve metotlara dayanması ve ayrıca bilirkişinin bu ilke ve metotları somut olaya yerinde bir şekilde uygulamış olması aranmaktadır. 702. madde, yalnızca bilirkişi tarafından yararlanılan teori ve metotları mercek altına almakla kalmamış, ayrıca bunların olayın maddi koşullarına uygun şekilde uyarlanıp uyarlanmadığının kontrol edilmesini aramıştır. İlgili kural bilirkişi görüşlerinin delil olarak değerlendirilmesinde büyük önem taşımaktadır[698].

Bilirkişi görüşleri ve aynı zamanda uzman mütalaaları için önemli şartlar öngören diğer bir dava ise Daubert/Merrell Dow Pharmaceuticals davasıdır[699]. Hamilelik sırasında mide bulantısı ilaçlarının bebeklerin kol ve bacaklarında deformasyon yaratıp yaratmadığına ilişkin pek çok bilirkişi raporu ve uzman mütalaaları sunulmuştur. Mahkeme müştekinin sunduğu uzman mütalaalarını ele alırken bunların dayandığı görüşlerin bir değerlendirmeden geçirilmemiş veya bilimsel dergilerde yayınlanmamış olduğunu belirtmiştir. Dolayısıyla, bu görüşler yayın yoluyla ilgili alanda paylaşılarak eleştirilere tabi tutulmamıştır. Mahkeme bu gerekçelerle uzman mütaalalarını delil olarak kabul etmemiştir[700]. Daubert kararı, bilirkişi görüşünü değerlendirirken dikkate alınması gereken unsurlara yaptığı katkı açısından oldukça önemlidir. Bu unsurlar bilirkişi görüşünün temelini teşkil eden teori

[696] Bernstein, s. 389.
[697]Maddenin orijinal metni için bkz. https://www.rulesofevidence.org/article-vii/rule-702/, Erişim Tarihi: 03.08.2021.
[698] Quattrocolo, s. 163.
[699]Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993), https://supreme.justia.com/cases/federal/us/509/579/, Erişim Tarihi: 27.07.2021.
[700] Bernstein, s. 393.

ve tekniğin test edilebilir veya test edilmiş olması, bu teori ve tekniğin bilimsel bir dergide yayınlanmış ve bilim insanları tarafından değerlendirilmiş olması, bu teori veya tekniğin uygulanmasında bilinen veya tahmin edilen hata oranının yüksek olmaması ve son olarak bu teori ve tekniğin ilgili alanda genel olarak kabul edilmiş olmasıdır[701].

Yine bilirkişiliğe ilişkin diğer önemli bir dava olan General Electric Co./Joiner davasında[702] Mahkeme, bilirkişi raporunda birden fazla hususun kontrol edilmesi gerektiğine dikkat çekmiştir. İlkin bilirkişi tarafından başvurulan metot bilimsel olmadır ve ayrıca bu metot ile varılan sonuç da akla, bilime, mantığa uygun olmalıdır. Bu karara göre, kullanılan yöntem kadar, bu yöntemi ilgili olaya uyarlamak için başvurulan mantık ve muhakeme ve ayrıca varılan sonuç da mahkemeler tarafından irdelenmelidir. Dolayısıyla bilirkişinin başvurduğu yöntem, muhakeme ve vardığı sonuç, söz konusu alanda genel olarak kabul görecek nitelikte olmalıdır. Aksi halde bilirkişi raporunun dikkate alınmaması gerekir[703].

Bu içtihatlar ışığında özetle, bir bilirkişi raporunun hükme esas alınabilmesi için, bilirkişinin ilgili alanda uzmanlığı, ilgili olayı değerlendirmeye ilişkin yeterli niteliklere sahip olup olmadığı, raporun dayandığı görüşlerin bilimselliği ve yine izlenen yöntem ve varılan sonucun bilimsel olarak doğrulanabilir ve kabul edilebilir olup olmadığı ve hata payları ele alınmalıdır. Ancak ilgili görüşün bilimselliği kadar, olay ile ilgisi ve olaya doğru şekilde uygulanıp uygulanmadığı da mutlaka değerlendirilmeli, maddi konuya ışık tutmayan görüşler bilimsel olsa dahi kabul edilmemelidir.

Profillemenin hem geleneksel hem otomatik şeklinin en sık başvurulduğu ülke olan ABD'de bu sayılan ilkeler esas alınarak kapsamlı bir içtihat oluşturulmuştur. Bu içtihatlar, profillemenin bilirkişi görüşü olarak hükme esas alınıp alınamayacağına ışık tutmaları bakımından önemlidir.

---

[701] Casey, s.73.
[702] 69. 522 U.S. 136, 146-47 (1997), https://supreme.justia.com/cases/federal/us/522/136/, Erişim Tarihi: 27.07.2021.
[703] Bernstein, s. 396, 397.

Örneğin Commonwealth/DiStefano davasında[704] bilirkişi, olaydaki sanığın, katillerin genel profiline uygun kişilik özellikleri sergilediğine dair görüş bildirmiştir. Mahkeme bilirkişi görüşünün olasılıklara dayalı, spekülatif nitelikte bir profillemeye dayandığını belirtmiş, Frye ilkelerine göre yaptığı incelemede, bilirkişi görüşüne temel olan teorinin bilim insanlarının çoğunluğu tarafından kabul görmediğinin altını çizmiştir. Bunun yanı sıra Mahkeme, yalnızca tahmine dayalı suçlu profillemenin, sanığa karşı önyargı yarattığı belirtmiş ve bu nedenle katillerin kişisel özellikleri ile olaydaki sanık arası bağ kurarak sanık hakkında ceza verilmesi yönünde kanaat uyandıran bilirkişi görüşünü değerlendirme dışı bırakmıştır. Mahkeme, bilirkişi görüşünün, olasılıklara ve spekülasyonlara yer vermeksizin, olay ile olguları bilimsel ve şüpheyi ortadan kaldıracak şekilde aydınlatmaya yardımcı olması gerektiğinin altını çizmiştir[705]. Dolayısıyla profilleme, kolluk görevlileri açısından kapsamlı bir tahmine izin vererek soruşturma sürecinde yol gösterici olmakla birlikte, yargılama aşamasında bu tür olasılıksal bilgiye dayanılan bilirkişi görüşü sağlam ve güvenilir bir delil teşkil etmeyecektir.

State v. Parkinson davasında[706] Idaho Temyiz Mahkemesi cinsel suçlulara ilişkin profilleme yapılmasını ve olayda bu profilleme yöntemlerine dayanılarak gerçekleştirilen ve sanık lehine olan uzman beyanlarının dosyadan çıkarılmasını incelemiştir. Mahkeme, sanığın cinsel suçluların profiline uymadığını belirten uzman görüşünün davanın maddi konusunu çözmediğini, nitekim dava konusunun sanığın karakteri üzerine olmadığını, bu tür bir tespitin olaya ilişkin delilleri anlamaya yardımcı olmadığını belirtmiştir. Mahkeme ayrıca genel profillerden yola çıkarak sanığın bu profile uyup uymadığını belirtmenin uzman kişinin sanığın suçlu olup olmadığına ilişkin görüş bildirmesi anlamına geldiğinin altını çizmiştir. Ayrıca cinsel suçlu profili ve bir kişinin buna uyup uymadığının tespiti henüz ilgili alanda çoğunluk görüşü tarafından geçerliliği kabul edilmiş bir teoriye dayanmamaktadır. Mahkemenin bu son tespiti günümüzde otomatikleşmiş profilleme teknolojilerine de ışık tutmaktadır. Mahkeme, cinsel suçluların psikolojik değerlendirmesi için farklı testlere başvurulduğunu, kimi zaman birden fazla testin bir arada kullanıldığı ancak bunların hiçbirinin ilgili fiilin sanık tarafından işlenip işlenmediğini veya bir gün sanık

[704] Commonwealth of Pennsylvania v. DiStefano, No. 96-CR-737, April 5, 1999, https://caselaw.findlaw.com/pa-superior-court/1314461.html, Erişim Tarihi: 09.08.2021.
[705] Meyer, s. 216, 217.
[706] State v. Parkinson, 128 Idaho 29; aktaran Meyer s.227.

tarafından işleneceğini tespit etmeye elberişli olmadığını vurgulamaktadır. Dolayısıyla Temyiz Mahkemesi, henüz kanıtlanmamış bir teori üzerine inşa edilmiş profillemeye dayalı bilirkişi görüşünün reddedilmesini yerinde bulmuştur. Son olarak mahkeme, profillemenin nasıl gerçekleştirildiğinin, hangi teknikleri kullanıldığı, test edilip edilmediği, gösterdiği sonuçların doğruluk oranı, psikoloji alanında profillemede kullanılan teorilerin genel kabul görüp görmediği gibi unsurların mahkemeye sunulması gerektiğinin altını çizmiştir[707].

Birleşik Krallık'ta görülen R./Stagg davasında[708] yine profillemeye ilişkin önemli tespitler yapılmıştır. Mahkeme profillemenin temelde, belli dava ve durumlardan yola çıkarak analoji oluşturduğunu, bu nedenle en baştan sorgulanır bir yöntem olduğunu ve "bilirkişi görüşü" olarak ele alınmasının yerinde olmadığını vurgulamaktadır. Nitekim profilleme yöntemi, çoğu durumda davada ele alınması gereken maddi gerçeklerden bağımsız, hatta bunlarla ilgisiz olup failin belli niteliklerine yoğunlaşılarak olayın maddi boyutundan uzaklaşılmasına yol açmaktadır. Başka bir deyişle, profilleme ikincil nitelikte tartışmalar yaratmakta, bu durum sanığa taraflı ve ön yargılı yaklaşılmasına yol açmaktadır. Yine Mahkeme, oluşturulan bir profilin her zaman için olasılıklara dayandığını ve hiçbir zaman bir "gerçek" olarak ele alınamayacağını, dolayısıyla doğru ya da yanlışlığının tartışılması ve kanıtlanmasının güç olacağını belirtmektedir[709].

Profilleme teknolojileri bugün gelinen teknolojik sıçrama ile sınırlı sayıda dosyanın birleştirilmesinden oluşan geleneksel profillemeye göre çok daha fazla veriye dayanmaktadır. Ancak dayandıkları veriler ceza muhakemesindeki dava dosyalarının sınırlarını aşmış, şüpheli statüsünde dahi olmayan milyonların davranışlarının istatistiksel analizine dönüşmüştür. Kapsamın bu denli genişlemesi, aslında ceza muhakemesinin maddi gerçeği tespit amacından sapılmasına yol açmıştır. Bunun yanı sıra otomatik işleyen yazılımlar çok daha hızlı şekilde tarama yapmakta, dosyaları tek tek inceleyen gerçek bilirkişiye yer bırakmamaktadır. Bu durum, bağlamdan uzaklaşılmaya, olayın şartlarından ziyade veriler arası istatistiksel bağlara dayanmaya yol açmıştır. Bu şekilde varılan sonuçların bir nevi kriminolojik uzman

[707] Meyer, s. 227-229.
[708] R v. Stagg, Central Criminal Court, 14 Eylül 1994, aktaran Meyer, s. 235.
[709] Meyer, s. 235, 236.

görüşü teşkil edip etmeyeceği oldukça tartışmalıdır. Ayrıca otomatik profilleme sonucu ile karakter analizi üzerinden tehlikelilik oranını tespit edebildiği kabul edilse dahi bu tespit, failin suç teşkil eden fiili işleyip işlemediğini kanıtlamamaktadır[710]. Nitekim bir kişinin "kötü bir karaktere sahip olduğunu" kanıtlamakla onun suçun faili olduğunu kanıtlamak arasında büyük fark vardır[711]. Yukarıdaki içtihatların da gösterdiği üzere Anglosakson hukukunda, soruşturma sürecinde failin izini sürmek amacıyla profillemeye başvurulmakla birlikte, kovuşturma aşamasında profillemeye dayanan bilirkişilerin rapor ve beyanları hükme esas alınmamıştır. Bu hususta Kıta Avrupası hukukunda sınırlayıcı hükümlere de rastlanılmaktadır. Örneğin İtalyan Ceza Usul Kanunu kapsamında 220. madde gereğince güvenlik tedbiri ve infaz rejimini belirleme amacı dışında, failin itiyadı, suçu meslek edinme hali, suça eğilimi, kişiliği, karakteri ve psikolojik durumunun analizi için bilirkişi görüşüne başvurulamayacağı belirtilmiştir[712]. Dolayısıyla kişinin karakterinin ve bunu irdeleyen bilirkişi görüşünün, suçun ve cezanın belirlenmesinde delil niteliği arz etmeyeceği açıkça düzenlenmiş bulunmaktadır. Mahkemeler, aynı sonuca açık düzenleme olmasa dahi, delilin sahip olması gereken unsurları tartışarak da varabilirler. Ancak İtalya'da olduğu gibi bu tür açık bir normun bulunması, COMPAS ve SAVRY gibi profilleme teknolojilerinin bir uzman görüşü olarak hükme esas alınmasının önünde daha net bir engel teşkil edecektir[713].

CMK kapsamında bilirkişi raporunun konusu açısından karakter analizini engelleyen nitelikte bir kısıtlamaya gidilmemiştir. Bununla birlikte uygulamada bu tarz profilleme teknolojileri ile yapılan değerlendirmelerin hükme esas alınmasına henüz rastlanmamıştır. Nitekim TCK m. 61'de, ceza tayin edilirken, failin şahsi niteliklerinden ziyade somut olayın işleniş şekli, kullanılan araçlar, işlendiği zaman ve yer, suçun konusunun önemi, failin kusurunun ağırlığı gibi somut olayda fiil ile birlikte açığa çıkan ve suç ile ilişkili unsurlara dayanılması gerektiği öngörülmektedir. Bununla birlikte ancak suçun işlendiğinin tespit edilmesi ve suçun cezası tayin edildikten sonra cezanın infaz şekline ilişkin olarak failin kişiliği önem kazanabilmektedir. Örneğin TCK m. 50 kapsamında suçlunun kişiliği, sosyal ve

[710] Quattrocolo, s. 172.
[711] Roderick Munday, **Evidence**, Oxford University Press: Oxford, Temmuz 2017, s. 255.
[712]Maddenin orijinal metni için bkz. Codice Di Procedura Penale, https://www.legislationline.org/download/id/4357/file/Italy_CPC_updated_till_2012_Part_1_it.pdf, Erişim Tarihi: 10.08.2021.
[713] Quattrocolo, s.174.

ekonomik durumu, yargılama sırasında duyduğu pişmanlık gibi sübjektif unsurlar, suç ve cezaya ilişkin tespitin yapılmasının ardından kısa süreli hapis cezası yerine seçenek yaptırımlar öngörülmesinde dikkate alınmaktadır. Yine TCK m. 51/b kapsamında hapis cezasının ertelenmesi hususunda kişinin yargılama sürecinde gösterdiği davranışlar ve pişmanlığı dikkate alınmaktadır. Son olarak CMK m. 231/6 (b) maddesinde hükmün açıklanmasının geri bırakılması için mahkemece, sanığın kişilik özelliklerinin ve duruşmadaki tutumlarına dayanılarak yeniden suç işlemeyeceği hususunda kanaate varılması gerekir. Ancak henüz daha suç işlenmeden ve suçun işlendiği tespiti yapılmadan uygulanan otomatik profilleme teknolojileri bu maddeler ile uyumlu değildir. Yukarıda da açıklandığı üzere, bu maddeler ancak kişinin suç işlediğinin tespitinin ardından, bireysel özellikleri ve somut olayın şartları dikkate alınarak hâkim tarafından tespit edilen şahsi niteliklere işaret eder ve kişiye cezanın veya bir yaptırımın ne şekilde uygulanacağını belirleyen bir etki doğurur. Yine ilgili maddeler kapsamında failin niteliklerinin değerlendirilmesi otomatik teknolojilere veya bilirkişi görüşüne değil, hâkimin takdir yetkisine bırakmıştır.

Sonuç olarak günümüzde kullanılan profilleme teknolojileri karakter analizi yapmaktadır. Ancak bu analizlerin dayandığı kriminolojik ve sosyolojik teorilerin ilgili bilim dallarında genel kabul gördüğünü söylemek mümkün olmadığı gibi yazılımların bu teorilere sadık kaldığını söylemek de mümkün değildir. Nitekim özellikle kendi kendine öğrenen algoritmalar, her seferinde veriler üzerinden optimum sonuca ulaşmak için değişmekte, modeli dönüştürmekte ve dolayısıyla kurdukları bağlantıları takip etmek güçleşmektedir[714]. Dolayısıyla algoritmalar aslında başvurulan tekniğin bilimselliğini analiz etmeyi imkansız hale getirebilmektedir. Profillemenin ilk aşamasında, algoritmaların eğitim sürecine insan tarafından müdahale söz konusudur. Bu süreçte profillemeye sunulan girdi verilerin kontrol edilmesi mümkündür. Ancak profilleme ile varılan sonuçlar otomatik olup bu sonuçların bilimselliği ve geçerliliği kanıtlanmaya muhtaçtır. Profilleme ile varılan bu sonuçların bilirkişinin görüşünden en önemli farkı, bir insanın teknik bilgi ve tecrübesi ile süzülmüş, insani muhakeme ile verilmiş bir sonuç olmamalarıdır. Nitekim TCK ve CMK kapsamında çeşitli hallerde cezanın uygulanışı sırasında failin kişiliği önemli

[714] Nizan Packin Geslevich/Yafit Lev Aretz, "Learning Algorithms and Discrimination", İçinde **Research Handbook of Artificial Intelligence and Law,** Ed. Woodrow Barfield/Ugo Pagallo, Edward Elgar Publishing: Cheltenham, 2018, ss.88-113, s.99.

olabilmekte ve hâkim tarafından değerlendirme süzgecinden geçirilebilmektedir. Oysa profilleme teknolojileri, cezanın uygulanışı değil, bizzat suçun tespiti sırasında da devreye girmektedir. Yargılama sürecinde yazılımlar tarafından yapılan değerlendirmelerin bilirkişi görüşü olarak dikkate alındığı ve hükme esasa alındığı ihtimalde, maddi olayın ve failin şahsi nitelikleri dikkate alınmamış olacaktır. Bu durum suçluluğu belirlemede fiilden değil failden yola çıkan ve aynı zamanda istatistiki genellemeler ile hâkimi etkileyerek cezanın şahsiliği ilkesini çiğneyen uygulamaların muhakeme sürecinde sızmasına yol açacaktır. Bu nedenle profilleme teknolojilerinin yaptığı değerlendirmeler, bilirkişi görüşü olarak hükme esas alınmamalıdır.

D. Hukuka Aykırı Delil Kapsamında Profilleme Teknolojileri

Yukarıda delil başlığı altında tartışıldığı üzere bir bulgu ya da verinin delil niteliğini haiz olması için aranan özelliklerden biri hukuka uygun olmasıdır. Hukuka aykırı olarak elde edilmiş bir delil, delil olarak nitelendirilemeyecek ve hükme esas alınamayacaktır. Hukuka aykırılık kuşkusuz ki yalnızca ceza hukuku değil tüm hukuk sistemine aykırılığı ifade eder. Dolayısıyla hukuka aykırılığa ilişkin düzenlemeler, Ceza Muhakemesi Hukuku ile Kişisel Verileri Koruma mevzuatı arasında bir köprü teşkil edecektir. Nitekim kişisel verilerin işlenmesi usulüne aykırı şekilde elde edilmiş verilerin profilleme teknolojilerine sunulması halinde, bu teknolojiler ile varılan sonucun hukuka uygun bir delil olarak kabul edilmesi mümkün değildir. Dolayısıyla, profilleme teknolojileri açısından, hukuka aykırı delil kavramı, kişisel veriler ve ceza muhakemesi usulüne ilişkin mevzuatların birlikte ele alınmasını sağlamakta, önemli bir kesişim noktası teşkil etmektedir. Hukuka uygunluğun değerlendirilmesi, kişisel veriler mevzuatının ceza hâkimlerince bilinmesini zorunlu kılmakta, veri işleme ve profillemeye ilişkin bir önceki bölümde yapılan değerlendirmeleri, ceza muhakemesinin işleyiş süreciyle bütünleştirmektedir.

Aşağıda öncelikle Ceza Muhakemesi alanında hukuka aykırı delil kavramına ilişkin düzenlemeler ulusal ve uluslararası mevzuat çerçevesinde irdelenecek, ardından profilleme teknolojilerinin bu kapsamda tüm hukuk sistemine uyumu ve delil niteliği değerlendirilecektir.

1. Hukuka Aykırı Delil Kavramı

Otoriter sistemlerde ceza muhakemesinin temel amacı ne pahasına olursa olsun şüpheli veya sanığın cezalandırılmasını tesis etmektir. Bu tür sistemlerde her türlü delil elde etme yöntemi kullanılabilmekte, sanık hakları ve evrensel insan hakları kavramı, kamu düzeninin tesisi için göz ardı edilmektedir[715]. Aydınlanma Çağı düşünürleri ile birlikte hürriyet kavramının insanın en temel varlığı olduğu vurgulanmış ve hürriyetinden yoksun kılınmasının sanığa verilecek en büyük ceza olduğunun altı çizilmiştir. Yine işkencenin insan haysiyeti kavramı bağdaşmadığı ve mutlaka yasaklanması gerektiği aydınlanma dönemiyle vurgulanmıştır[716].

Kişilerin hak ve özgürlüklerine dayalı hukuk devletlerinde, adil yargılanma hakkı ve insan haklarına saygı esas alınarak maddi gerçeğe ulaşma yöntemlerine sınırlar getirilmiştir. Delil yasaklarının doğumu, her türlü işlem ve eylemde hukuka saygı gösterilmesi ile ilişkilidir. Hukuka aykırı deliller, yargılama sonucu ulaşılan hükmün meşruiyetini zedeleyeceğinden bu tür delillerin hükme esas alınmayacağı kabul edilmektedir. Nitekim hukuk devleti, suçun aydınlatılması ve suçlunun cezalandırılması amacıyla dahi hukuktan sapmamalıdır. Delil yasaklarının insan onuru ile olan bağı, özellikle temel haklara yoğun müdahale içeren ceza muhakemesinde evleviyetle dikkate alınmalıdır. İnsan onuru kavramı, sanık haklarının ve tüm hakların üstünde bir kavram olup salt insan olmaktan ötürü her insanın sahip olduğu, herhangi başka bir hakla kıyaslanamaz, karşılığında herhangi bir "değer biçilemez" bir kavramdır. Kant'ın insan onurunu tanımlarken kullandığı "değer biçilemez" kavramının iki karşılığı vardır: Bunlardan ilki, insan onuru karşısında herhangi bir amaç ya da menfaatin meşruiyet zemini oluşturamaması, örneğin kamu düzeninin tesisi gibi ereklerin insan onuruna karşı herhangi bir müdahaleyi haklı kılmasının mümkün olmamasıdır. İkinci olarak, bu kavramın kişiler üstü olması, bir kişinin onurunun diğer insanlarla kıyaslanmasına izin vermemektedir. Başka bir deyişle, insan onuru, salt bir bireyin onurunun ötesinde bir kavram olup bir kişinin onurunun daha fazla sayıda kişinin onuru ile kıyaslanması söz konusu olamayacaktır[717].

---

[715] Devrim Aydın, **Ceza Muhakemesinde Deliller**, Yetkin Yayınevi: Ankara, 2014, s.197.
[716] Aksoy Retornaz, "Beccaria'nın Hapis Cezasına Bakışı Üzerine Bir Değerlendirme", s.94.
[717] Bernd Ladwig,"Menschenwürde als Grund der Menschenrechte? Eine Kritik an Kant und über Kant hinaus", **Zeitschrift für Politische Theorie**, Cilt:1, 2010, ss.51-69, s.52.

İnsan onurunu ve hukuk devletini teminat altına alan en önemli olan yasaklardan biri hukuka aykırı delilin hükme esas alınamaması yasağıdır. Hukuka aykırı delil, hukuk sistemine ve bu sistemi oluşturan kurallara aykırı şekilde elde edilmiş delildir. Bu bağlamda, hukuka aykırı delil tespit edilirken bir ülkede uygulanmakta olan kanunlar kadar ulusları aşan hukuk kuralları, sözleşmeler ve evrensel hukuk ilkeleri de dikkate alınmalıdır. Anayasa Mahkemesi'nin de açıkça belirttiği üzere[718] anayasaya, usulüne uygun olarak kabul edilmiş uluslararası sözleşmelere, kanunlara, kanun hükmünde kararnamelere, tüzüklere, yönetmeliklere, içtihadı birleştirme kararlarına ve teamül hukukuna aykırı uygulamaların tümü hukuka aykırı olarak nitelendirmelidir. Hukuka aykırılığın tespitinde, hukukun genel ilkeleri ayrıca önem taşımaktadır. Hukukun genel ilkeleri hukuk devletinin güvencesi olup yasa koyucu tarafından bile ortadan kaldırılamayan ilkelerdir. Nitekim Nazi Almanya'sında pozitif yasalar meclis tarafından çıkartılmış, hukukun temel ilkelerine aykırı yasamanın varabileceği sonuçlar hukuki pozitivizmin sınırlanması gerektiğini açıkça göstermiştir. Bu nedenle "hukuka aykırılık", "yasaya aykırılıktan" daha derin bir anlama sahiptir, bir delilin hukuka aykırılığı denetlenirken, pozitif hukuk metinlerinin ötesine geçilerek evrensel hukuk ilkelerine aykırılığın söz konusu olup olmadığı da mutlaka değerlendirilmelidir[719].

Bununla birlikte uygulamada aşağıda ele alınacağı üzere farklı devletlerin hukuka aykırı deliller konusunda farklı yaklaşımlar sergilediği görülmektedir. Bunlardan ilki Türkiye'nin de benimsediği mutlak değerlendirme yasağı görüşüdür. Bu görüş, hukuka aykırı şekilde elde edilen delilleri mutlak bir aykırılık olarak kabul etmekte, bunları ceza muhakemesi sürecinde tamamen değerlendirme dışında tutmaktadır. Bu tür sistemlerde, yasaya aykırı her türlü yöntem hukuka aykırı kabul edilir, bir hukuk normunun "az" ya da "çok" ihlalinin söz konusu olamayacağı, bunların hükme etki edip etmediği tartışmaya açılmaksızın devre dışı bırakılmaları gerektiği savunulur[720].

İkinci görüş ise nispi değerlendirme yasağı olarak adlandırılabilir. Başta Almanya olmak üzere Kıta Avrupası'nda kabul edilen bu görüş, delillerin elde

[718] AYM, E:1999/2, K:2001/2, aktaran Güçlü Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", **Türkiye Barolar Birliği Dergisi**, Sayı:102, ss.61-82, 2012, s. 63.
[719] Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", s. 63.
[720] Akyürek, s. 77.

edilmesi sırasında ihlal edilen hak ile delilin kabul edilmesi ile elde edilecek çıkar arasında bir değerlendirme yapmaktadır. Sanığın ihlal edilen hakkı ilgili suçun cezalandırılmasından üstün ise delil değerlendirme dışı bırakılmakta, aksi halde ilgili delil hukuka aykırı elde edilmiş olsa da dikkate alınmaktadır[721].

Bunun yanı sıra karşılaştırmalı hukukta, hukuka aykırı delillerin uzak etkisi bakımından da farklı yaklaşımlar söz konusudur. Gerek doktrinde gerekse yargı kararlarında hukuka aykırı delillerden yola çıkarak elde edilen delillerin hükme esas alınıp alınamayacağı tartışmalıdır. Delillerin uzak etkisi veya delillerin dolaylı etkisi olarak ifade edilen bu tartışmayı doğuran husus, delil değerlendirme yasaklarının doğrudan elde edilen delillerin yanı sıra bu delillerden elde edilen diğer delilleri kapsayıp kapsamadığı üzerinedir[722]. Bu tartışma ilkin Anglo-sakson hukukunda alevlenmiş olup "zehirli ağacın meyvesi" metaforu ile anılmaktadır[723]. Örneğin hipnoz etkisi altına alınarak konuşturulan şüphelinin itirafı, zehirli ağaç olup bu itiraftan yola çıkılarak bulunan silah veya ceset, zehirli ağacın meyvesi olarak ifade edilecektir. Hukuka aykırı deliller açısından mutlak ve nispi yasaklar şeklinde farklı yaklaşımlar sergilendiği göz önüne alındığında, delillerin dolaylı etkileri yönünden de farklı sonuçlara varılması kaçınılmazdır. Bu bağlamda Amerikan hukukunda hukuka aykırı delillerden türetilen delilleri de yargılama sürecinden dışlama eğilimi baskınken, Kıta Avrupası'nda yine somut olayın özellikleri ve ilk delili elde etmede hangi tür kuralların çiğnendiği dikkate alınmaktadır. Türkiye'de ise hukuka aykırı delilleri düzenleyen ve ileride daha detaylı şekilde ele alınacak olan Anayasa m. 38, CMK m.217 ve m. 289 gibi hükümlerin hukuka aykırı delilleri ve bunlar marifetiyle elde edilen delilleri kapsadığı görüşü baskındır[724]. Bu tartışmalar, ceza muhakemesi ve kişisel verilerin korunması mevzuatına aykırı şekilde toplanmış verilere dayanan veya profillemeye ilişkin hükümlere aykırılık teşkil eden risk değerlendirme teknolojilerini değerlendirirken büyük önem taşımaktadır. Aşağıda hukuka aykırı deliller ve bunların uzak etkileri, önce Türkiye, ardından karşılaştırmalı hukuk ve AİHM kararları çerçevesinde detaylı şekilde ele alınacaktır.

---

[721] Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu" s. 66-68.
[722] Mehmet Gödekli, "Türk Ceza Muhakemesinde Maddi Gerçeğe Ulaşmanın Ön Koşulu Olarak Hukuka Aykırı Delillerin Değerlendirilmesi Yasağı", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:65, Sayı: 4, 2016, ss.1815-1924, s.1880, 1881.
[723] Volkan Dülger, **Ceza Muhakemesi Hukukunda Dışlama Kuralı Ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağaçların Meyvesi Öğretisi),** Seçkin Yayınevi: Ankara, Eylül 2014, s.107.
[724] Birtek, s.336-338.

a) Bazı Hukuk Sistemlerinde Hukuka Aykırı Delil ve Delillerin Uzak Etkisi

Karşılaştırmalı hukukta hukuka aykırı delillere ilişkin üç temel teori bulunmaktadır. Bunlardan ilki, hukuka aykırı delillerin değerlendirilmesinde kolluk güçleri ve idarenin hukuka aykırı eylemlerini dizginleme ve caydırma amacını temel almaktadır. Özellikle Amerika Birleşik Devletleri'nde kolluğun aşırı güç kullanması, konut dokunulmazlığı ve özel hayatın gizliliğini ihlal eden eylemlerinin cezai soruşturmalar ve hukuk davaları yoluyla dahi durdurulamaması sonucu, bu tür eylemlerle elde edilen delillerin değerlendirme dışında tutulması anlayışı hâkim olmuştur[725]. Bu bağlamda örnek teşkil eden davalardan biri olan Boyd/Amerika Birleşik Devletleri davasında[726] hukuka aykırı delilleri "dışlama kuralı"nın temeli atılmıştır. İlgili davada, hukuka aykırılığın hükümetin hukuka aykırı eylemlerinden de kaynaklanabileceği, bununla birlikte "her türlü tiranlığa karşı" yargılamanın hukuktan yana duruş sergilemesi gerektiği vurgulanmıştır. Ayrıca hukuka aykırı delilleri dışlama kuralının özellikle masumiyet karinesi ile ilişkili olduğu ve yine kimsenin kendi aleyhine tanıklığa zorlanamayacağının güvencesi olduğu belirtilmiştir. Nitekim kişilerin özgürlük ve güvenlik haklarının ihlal edilmesi için mutlaka kapılarının kırılması, çekmecelerinin karıştırılması gerekmemektedir. Ufak gözüken ihlallerle de kişinin özel hayatının gizliliği ve diğer hakları ihlal edilebilir. Bu nedenle, gerek kolluk gerekse idare tarafından her türlü hukuka aykırı eylem ve işlemle elde edilen delillerin dışlanması gerekir[727]. Nitekim Brown/Missisipi davasında "çivili bir kemerle devamlı dövülen" sanığın ifadesinin hukuka aykırı delil kabul edilerek geçerli sayılmaması[728], Mapp v. Ohio davasında hâkim kararı olmaksızın konut araması yapan kolluğun elde ettiği delillerin kabul edilmemesi[729], Alderman v. United States[730] davasında iş yerinin hukuka aykırı şekilde dinlenilmesi sonucu elde edilen delillerin ulusal güvenlik ile

[725] Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", s. 65.
[726] 116 U.S. 616, 625 (1886)
[727] Scott E. Sundby/Lucy B. Ricca, "The Majestic and the Mundane: The Two Creation Stories of the Exclusionary Rule", **Texas Tech Law Review**, Cilt:43, 2010, ss. 391-433, s.395.
[728] Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", s. 65.
[729] İlgili kararda "hiçbir şey bir hükümeti kuralları uygulamamaktan daha hızlı çöküşe götüremez" ifadesi ile hukuka aykırı delillerin yargılama dışında tutulmasının önemi belirtilmektedir, bkz. 367 U.S. 643, 656-57 (1961), aktaran Sundby/Ricca, s. 404.
[730] 394 U.S. 165 (1968), https://caselaw.findlaw.com/us-supreme-court/394/165.html, Erişim Tarihi: 12.09.2021.

ilgili suçlarda dahi kullanılamayacağının kabulü, bu anlayışla alınmış kararlardır. Dolayısıyla Amerikan sisteminde, hukuka aykırı delillerin değerlendirilmemesinde, "onarıcı"dan ziyade hak ve hürriyetlerin ihlalini "önleyici" amaç baskındır. Ancak son yıllarda "kolluğun hataen tutuklama kaydını sistemden kaldırmayı unutması nedeniyle süresi dışında uygulanan koruma tedbiri sonucu elde edilen delilin kullanılması"[731], "hukuka aykırı arama ile ulaşılan tanığın arama hukuka aykırı olsa da ifade vermek zorunda bırakılması"[732] şeklinde kararlar alınarak mutlak delil değerlendirme yasağının dışına çıkıldığı görülmektedir. Mahkemeler, son dönem kararlarında kolluğun ağır ihlal teşkil etmeyen ve kasıtlı olmayan hareketlerinin söz konusu olduğu durumlarda, disiplin amaçlı delil dışlamanın gerekli olmadığını kabul etmektedir. Yine kolluğun hukuka aykırı hareketinin "göz ardı edilebilir" olduğu durumlarda, bu delilleri kabul etmeyerek ceza muhakemesinin işleyişine müdahalenin yarardan ziyade zarar getireceği ileri sürülmektedir[733]. Bu durum, hukuka aykırı delillerin salt disiplin amacına indirgenmesinden kaynaklanmakta, mutlak değerlendirme yasağının hukuk devletine saygı ilkesi ile temellendirilmemesi, ilkeden sapmaları mümkün kılmaktadır.

Kıta Avrupası'nda ise delil değerlendirme yasaklarının düşünsel yapısını daha ziyade "hak alanı teorisi" oluşturmaktadır. Bu teori uyarınca, hukuka aykırı işlem ile anayasal hak ve özgürlükler, özellikle sanığın temel hak ve özgürlükleri ağır şekilde ihlal edilirse, bu işlem sonucu elde edilen delil hukuka aykırı kabul edilmektedir. Özellikle Alman Yüksek Mahkemesi tarafından uygulanan bu teoriye göre hukuka aykırı bir delilin hükme esas alınıp alınmayacağı tespit edilirken, hukuka aykırılığın sanığın haklarını ne ölçüde ihlal ettiği değerlendirilir. İhlal edilen normun ihdas amacına bakılarak, bu normun ihlalinin sanığın hukuki durumunda ne tür değişiklikler yarattığı irdelenir. Bu bağlamda susma hakkının kullandırılmaması, ifade yasaklarına başvurulması gibi hallerde sanık haklarına yönelik ihlalin büyüklüğü tartışmasızdır[734]. Ancak bu görüş, haklar arası hiyerarşi yapılmasına yol açmakta, temel hakları ve sanık haklarını koruma şiarına dayansa da her somut olayda farklı değerlendirmeyi mümkün kılarak ceza hukukunun en temel özelliklerinden olan öngörülebilirliği imkânsız

[731] Herring v. United States, 555 US 135, https://www.oyez.org/cases/2008/07-513, Erişim Tarihi: 12.09.2021.
[732], United States v. Calandra, 414 US 338 (1974), https://www.oyez.org/cases/1973/72-734, Erişim Tarihi: 12.09.2021.
[733] Jenia Turner Iontcheva, "Regulating Interrogations and Excluding Confessions in the United States: Balancing Individual Rights and the Search for the Truth", İçinde **Do Exclusionary Rules Ensure a Fair Trial?**, Ed: Sabine Gless/Thomas Richter, Springer, 2019, ss. 93-129, s.104.
[734] Yenisey/Nuhoğlu, s.572.

kılmaktadır. Bunun yanı sıra, bu teori kapsamında sanık dışındaki süjelerin haklarının ihlal edilmesi halinde, hukuka aykırılık tartışmaya dahi açılmaksızın ilgili delil kabul edilebilmektedir[735]. Kıta Avrupası ve AİHM kararlarında ayrıca hakların dengelenmesi teorisine ("Abwägungstheorie") de başvurulduğu görülmektedir. Bu teoriye göre her somut olayda ihlal edilen normun koruduğu hukuksal değer ile kamu menfaati arasında bir değerlendirme yapılır[736]. Bu durumda ihlal edilen normun koruduğu değer, ilgili suçun ağırlığı, delilin bu suçu aydınlatmada taşıdığı rol gibi pek çok unsur tartılarak hukuka aykırı delilin değerlendirilip değerlendirilmeyeceği belirlenir[737]. Bununla birlikte, sanığa özellikle susma hakkı, hakkındaki suçlamalara karşı çıkma hakkı ve herhangi bir beyanda bulunmadan önce müdafiiden yararlanma hakkı gibi hakların hatırlatılmaması halinde, sanık hakları baskın kabul edilmekte, bu tür durumlarda elde edilen deliller hükme esas alınmamaktadır[738].

Ülkeler özelinde incelendiğinde, mutlak değerlendirme yasağına benzer yasakların Fransa ve İtalya'da uygulandığı görülmektedir. Fransa'da hukuka aykırı deliller, Ceza Muhakemesi Kanunu'nun[739] 171 maddesinde düzenlenmiştir. Bu maddede Fransız Ceza Muhakemesi Kanunu veya diğer kanunlardaki usulün çiğnenmesi ve bu durumun taraflardan birinin korunan değerlerini ihlal etmesi halinde delilin tamamen geçersiz olacağı (nullité) düzenlenmiştir. 171. madde yalnız Fransa'daki CMK düzenlemesi kapsamında değil tüm hukuk sistemine uygunluğun öneminin altını çizmektedir. İlgili madde ilk bakışta mutlak değerlendirme yasağı gibi görünse de aynı zamanda hukuka aykırı delilleri değerlendirme yasağını, tarafların haklarının ihlal edilip edilmemesine bağlı tutmuştur[740]. Bununla birlikte hâkimin tarafların haklarının ihlal edildiğini değerlendirmesi ile birlikte derhal delili

---

[735] Örneğin tanığın çekinme ve aleyhine delil göstermeme hakkının ihlal edilmesine rağmen, tanık beyanının delil olarak değerlendirildiği kararlar için bkz. Almanya Federal Mahkemesi (BGHSt) 11, 213, 21 Ocak 1958; BGHSt 38, 214, 27.02.1992, aktaran Sabine Gless, "Truth or Due Process? The Use of Illegally Gathered Evidence in the Criminal Trial", İçinde **German National Reports to the 18th International Congress of Comparative Law**, 2010, ss. 675-709, s. 686, dipnot 48.

[736] Vera Warnking, **Strafprozessuale Beweisverbote in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und ihre Auswirkungen auf das deutsche Recht**, Peter Lang GmbH: Frankfurt am Main, 2009, s.33, Dülger, **Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağaçların Meyvesi Öğretisi),** s.99

[737] Özellikle Almanya Federal Mahkemesi bu teoriye başvurmaktadır, bkz. BGHSt 42, 170, 21 Mayıs 1996, aktaran Gless, "Truth or Due Process?", s. 683, dipnot 32.

[738] Örnek karar içi bkz. BGHSt 38, 372, 29 Ekim 1992, aktaran Gless, "Truth or Due Process?", s. 684, dipnot 35.

[739] Code de procédure pénale, Sayı: 57-1426, Tarih: 31 Aralık 1957, https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/, Erişim Tarihi: 20.09.2021

[740] Chenchen Wang, **Encadrement de la Liberté de la Preuve dans la Procédure Pénale: Étude comparée France-Chine,** Université de Bordeaux, Hukuk Fakültesi Doktora Tezi, Kasım 2019, s. 236.

değerlendirme dışı bırakması gerekir. Dolayısıyla bu ihlalin azlığı ya da çokluğu, korunan diğer çıkarlarla dengelenmesi gibi hususlar ele alınmayacaktır. Yine bazı hükümlerde delillerin derhal geçersiz olduğu açıkça öngörülmektedir. Örneğin Fransız CMK m. 100-7 uyarınca belli kişilerin telefonlarının dinleme usulü düzenlenmiş, bu usule uyulmadığı takdirde yalnızca dinleme sonucu elde edilen delillerin değil, bunların uzak etkisi ile elde edilen delillerin de hükme esas alınamayacağı öngörülmüştür[741]. Fransa'daki diğer CMK hükümleri incelendiğinde, 59. maddede düzenlenen arama hükümlerine aykırı elde edilen delillerin hukuka aykırı kabul edileceği, 78-3 maddesinde kimlik tespitine ilişkin usule uyulmaması hakinde ilgili delilin kullanılamayacağı, 100-5 maddesinde avukat ile müvekkil arası konuşmaların kaydedilmesinin hukuka aykırı delil teşkil ettiği düzenlenmektedir.

İtalya'da da Fransa'ya benzer şekilde bazı hükümlerde düzenlenen usule aykırılık halinde doğrudan bu yolla elde edilen delili değerlendirme yasağı açıkça düzenlenmektedir[742]. Örneğin İtalyan Ceza Muhakemesi Kanunu'nun[743] 526. maddesi, kanun kapsamında öngörülen usullere uyulmadan yapılan arama, el koyma, iletişimin denetlenmesi tedbirleri ile elde edilen delillerin kullanılamayacağını belirtmektedir. Yine 188. madde, kişilerin serbest iradesini etkileyen yöntemlerin kullanılmasını yasaklamaktadır. Bu madde ilgili kişinin iradesini maddi ve manevi şekilde manipüle eden veya baskı altına alan eden her türlü yönteme ilişkin genel bir yasak koymaktadır[744]. İlgili Kanun'un 191. maddesi "kanunla öngörülen düzenlemelerin ihlal edilmesi suretiyle elde edilen delillerin kullanılamayacağı" şeklinde genel bir yasak öngörmektedir. Bu genel yasak kapsamında, İtalyan yargısı yalnızca usul kanunlarına aykırılığı değil, anayasal normların da ihlal edilip edilmediğini dikkate almaktadır[745]. Bununla birlikte uygulamada belirli maddelerde kesin değerlendirme yasağı öngörülürken diğer usul kuralları açısından özel düzenleme olmaması kimi zaman karışıklık yaratmaktadır. Hatta kimi zaman yargı kararlarında kanunda açıkça değerlendirilemeyeceği belirtilmeyen delillerin hükme esas alındığı görülmektedir. Delillerin uzak etkisi açısından ise genel bir düzenleme

---

[741] Warnking, s.39.
[742] Giulio Illuminati, "Italy: Statutory Nullities and Non-usability", içinde **Exclusionary Rules in Comparative Law**, Ed. Stephan C. Thaman, Springer: Dodrecht, 2013, ss. 235-259, s.236.
[743]Codice di Procedura Penale, https://www.legislationline.org/documents/section/criminal-codes/country/22/Italy/show, Erişim Tarihi: 21.09.2021.
[744] Illuminati, s. 251.
[745] Illuminati, s. 237.

olan 191. maddenin bu hususu açıkça düzenlemediği ileri sürülerek, hukuka aykırı delillerden türetilen delillerin yargılamada kullanabilmektedir[746]. Bununla birlikte hâkimin hukuk düzeninde öngörülen usullere aykırı şekilde toplanmış delillere dayanarak hüküm kuramayacağı açık şekilde düzenlenmiştir. Bu nedenle İtalya özelinde de hukuka aykırı delillerin mutlak olarak değerlendirme yasağının yumuşatılmasının kanundan değil, uygulamadan kaynaklı olduğunu söylemek mümkündür.

Almanya ise Alman Ceza Muhakemesi Kanunu[747] (Strafprozeßordnung) kapsamında hukuka aykırı delilleri değerlendirme yasağına ilişkin genel bir kural bulunmamaktadır[748]. Belli delillerin muhakeme sürecinden dışlanmasına ilişkin özel hükümler bulunmakla birlikte Türkiye'de CMK m. 206 ve m. 217'nin muadili bir düzenleme bulunmamaktadır. Bununla birlikte insan onurunu ihlal eden işkence ve kötü muamele, yine kişilerin özerk birey olarak varlıklarını koruması ile ilişkili görülen özel hayatın gizliliği ve kişilerin verileri üzerinde hâkimiyet haklarına müdahale içeren hususlar[749] Alman Ceza Muhakemesi Kanunu'nda açıkça düzenlenmekte, bunlara aykırı usullerle elde edilen deliller hükme esas alınamamaktadır. Bu kapsamda Nazi rejimi sonrası, insan onurunu korumak üzere tesis edilmiş en önemli hükümlerden biri Alman Ceza Muhakemesi kanunu 136a maddesi olup bu maddede ifade ve sorgu yasakları gösterilmiş, bunlara aykırı alınan ifadelerin hükme esas alınamayacağı belirtilmiştir[750]. Yine özel hayatın gizliliğine ilişkin 100 a maddesindeki iletişimin denetlenmesi, 100 b maddesindeki uzaktan bilişim sistemi yoluyla arama ve 100 c maddesindeki akustik yöntemlerle özel yerleşim yerinin dinlenmesi tedbirleri açıkça düzenlenmiştir. Bu tedbirlerle elde edilen delillerin hangi hallerde kullanılamayacağına ilişkin açık düzenleme ise 100 d maddesinde yapılmıştır. Soruşturma kapsamı suç dışındaki delillere el konulması halinde değerlendirme yasağı öngören m. 108/2, kişiden kan örneği almayı sınırlayan m. 81 c/3 hükümleri açıkça delil elde etme ve değerlendirme yasakları

---

[746] Illuninati, s. 258.

[747] Strafprozeßordnung ("StPO"), G v. 12.9.1950, bkz.https://www.gesetze-im-internet.de/stpo/StPO.pdf, Erişim Tarihi: 12.09.2021.

[748] Gless, "Truth or Due Process?", s. 678.

[749] Almanya'da Amerika'dan farklı olarak özel hayatın gizliliği ve kişisel verilerin korunması, "yalnız bırakılma hakkı"ndan yola çıkarak değil, insan onuru, bireylerin kişiliğini ve otonom varlığını koruması ile temellendirilmekte, bu nedenle daha özel bir koruma rejimine tabi tutulmaktadır, Gless, "Truth or Due Process", s. 688.

[750] Gless, "Truth or Due Process?", s. 678.

öngörmektedir[751]. Bu şekilde Anayasa hükümleri ve özel hükümler bünyesinde delillerin değerlendirilemeyeceği açıkça öngörülen hallere "selbstständige Beweisverwertungsverbote" (bağımsız delil yasakları) denilmektedir[752]. Özel hükümlerle açıkça öngörülen delil yasakları haricinde hangi delillerin ceza muhakemesinden dışlanması gerektiğine dair doktrin ve uygulama tarafından bazı kurallar ortaya konulmuştur. Almanya Federal Mahkemesi, örneğin özel hayata ilişkin açıkça düzenlenmiş yasaklayıcı normlar dışında kalan müdahaleler söz konusu olduğunda, orantılılık ilkesi çerçevesinde inceleme yaparak, delil elde etme sırasında bu hakka orantısız müdahale olduğuna kanaat getirdiğinde toplanan delilleri hükme esas almamaktadır. Bu bağlamda örneğin uyuşturucu tedavisi yapan bir merkezin hastalarına ilişkin belgelerine el konulması orantısız bulunmuş ve bu nedenle hukuka aykırı kabul edilmiştir[753]. Yine sanığın ihlal edilen hakları ve hakların dengelenmesi teorisine uygulamada sıklıkla başvurulduğu görülmektedir[754]. Delillerin uzak etkisi açısından ise doktrin ve uygulamada genellikle hukuka aykırı delillere ilişkin düzenlemelerin ve teorilerin, bu delillerden yola çıkarak elde edilen diğer delilleri kapsamadığı kabul edilmektedir. Örneğin hukuka aykırı bir dinleme üzerinden bir tanığın bilgilerinin öğrenildiği kararda, bu tanığın bulunarak dinlenilmesi hukuka uygun bulunmuştur[755]. Bununla birlikte hakların dengelenmesi teorisi, farklı olaylarda delillerin uzak etkisi bakımından da farklı sonuçlara varılmasına yol açabilmektedir. Örneğin hem basın ve ifade özgürlüğünün, hem özel hayatın gizliliğinin ihlal edildiği olayda, bir gazetecinin hukuka aykırı şekilde iletişiminin tespit edilmesinden yola çıkarak elde edilen deliller hükme esas alınmamış, sanığın birden fazla hakkına yönelik ihlal daha baskın bulunmuştur[756]. Doktrinde çoğunluk görüşü, ifade ve sorguya ilişkin kuralları düzenleyen 136. maddenin ihlaline dayanan delillerin yanı sıra bu delillerden türetilen diğer delillerin kullanılmaması gerektiği yönündedir[757]. Bununla birlikte aşağıda daha detaylı şekilde ele alınacak Gäfgen kararı, ifade ve sorgu

---

[751] Warnking, s.31

[752] Gless, "Truth or Due Process?", s. 658.

[753] BVerfGE 44, 353,24 Mayıs 1977. Benzer yönde orantılılık prensibine dayanılan kararlar için bkz. BVerfGE 209, 7, 15 Ocak 1958, BVerfG, NJW 1962, 2243, 9 Kasım 1962, BVerfG NJW 1963, 147, 18 Aralık 1962, Gless, "Truth or Due Process", s.680.

[754] BGHst 19, 325, BverGE 80, 367, aktaran Grünwald, Gerald, Das Beweisrecht der Strafprozeßordnung, Nomos Verlagsgesellschaft: Baden Baden, 1. Baskı, 1993, s.157.

[755] 77 BGHSt 32, 68, 24 Ağustos 1983,aktaran Gless, "Truth or Due Process?", s. 693. Benzer yönde hukuka aykırı arama sonucu elde edilen delillerden yola çıkarak ele geçirilen dolaylı delillerin kabul edildiği kararlar için: BVerfGE 2 BvR 2225/08, 2 Haziran 2009; BGHSt 27, 355 at 358, 22 Şubat 1978, BGHSt 32, 68 at 71, 24 Ağustos 1983.

[756] Spiegel kararı, BGHSt 29, 244, aktaran Yenisey/Nuhoğlu, s. 576.

[757] Gless, "Truth or Due Process?", s.693.

yasakları söz konusu olsa dahi delillerin uzak etkisi açısından istisnai kararların alınabildiğini göstermektedir.

b) Türk Mevzuatı Kapsamında Hukuka Aykırı Delil ve Delillerin Uzak Etkisi

Türkiye'de delil değerlendirme yasağına ilişkin ilk somut düzenleme, mülga Muhakemeleri Usulü Kanunu'nun "delilleri takdir salahiyeti" başlıklı 254. maddesinin ikinci fıkrasıdır. İlgili hüküm uyarınca soruşturma ve kovuşturma organlarının hukuka aykırı şekilde elde ettikleri deliller hükme esas alınamayacaktır. 2001 yılında bu yasak 1982 Anayasası'nın 38. maddesine "kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez" ifadesinin eklenmesi ile anayasal niteliğine kavuşmuştur. İlgili maddede kanuna aykırı ifadesi, hukuk düzenine aykırılık şeklinde okunmalıdır. Yine bu maddede kanuna aykırı "delilden" değil, "bulgudan" bahsedildiği, bulgunun ise bulunan şey, olaydan geriye kalan iz ve eseri gösteren emareleri çağrıştırdığı görülmektedir. Bununla birlikte kanuna aykırı bulgu kavramı, maddenin düzenleniş amacı gözetilerek hukuka aykırı "delil" şeklinde anlaşılmalıdır[758]. Nitekim Anayasa Mahkemesi de hukuka aykırı delillere ilişkin değerlendirmelerini emare kavramı ile sınırlı tutmamaktadır. İlgili madde hukuka aykırı delili ceza muhakemesi süreci ile sınırlamaksızın düzenlemiştir. Bu durum anayasa yargısı, medeni yargı, idari yargı, askeri yargı hatta disiplin soruşturmalarını kapsayacak şekilde tüm yargılama hukuku açısından kullanılacak delillerin hukuka uygun olmasını zorunlu kılmaktadır[759].

Ceza muhakemesinde de delil elde edilmesi ve değerlendirilmesi işlemleri, "delil yasakları" ile sınırlanmıştır. Delil yasakları doktrinde Alman hukukundan esinlenilerek "delil elde etme yasakları" (Beweiserhebungsverbote) ve "delil değerlendirme yasakları" (Beweisverwertungsverbote) olmak üzere iki gruba ayrılmaktadır[760]. Buna göre delillerin elde edilmesine ilişkin, kimi zaman delillerin konusu, kimi zaman ise delile erişim amacı açısından sınırlar öngörüldüğünde, bunlar

---

[758] Gödekli, s. 1823, Centel/Zafer, s.859.
[759] Gödekli, s. 1824, Ünver/Hakeri, s.1581.
[760] Caner Yenidünya, "Ceza Muhakemesinde Delillerin Değerlendirilmesi, Delil Yasakları ve Hukuka Aykırı Delillerin Ceza Yargılamasında Vaziyeti", 25.06.2019, https://caneryenidunya.medium.com/ceza-muhakemesinde-delillerin-de%C4%9Ferlendirilmesi-delil-yasaklar%C4%B1-ve-hukuka-ayk%C4%B1r%C4%B1-delillerin-ceza-bff814552eb4, Erişim Tarihi: 10.09.2021.

delil elde etme yasağı olarak nitelendirilir. Toplanmış delillerin ceza muhakemesinde ortaya konulması, değerlendirilmesi ve hükme esas alınmasına ilişkin yasaklar ise "delil değerlendirme yasağı" olarak nitelendirilir[761].

Örneğin CMK m. 147'de öngörülen ifade alma ve sorguya ilişkin usullere uyulmadan beyan alınması, bunun yanı sıra tanıklıktan çekinme hakkı olanlara bu hak hatırlatılmaksızın ifadelerinin alınması veya iletişimin denetlenmesi sırasında CMK m. 135'te öngörülen düzenlemelere uyulmaması gibi hususlar delil elde etme yasaklarıdır[762]. Delil değerlendirme yasağı ise ceza yargılamasında bir delilin yargılama konusunu ispat etmede kullanılamaması, hüküm verilirken bu delilin esas alınamamasını ifade eder. Delil değerlendirme yasakları hukuka aykırı şekilde elde edilmiş delilleri içerebileceği gibi kimi durumda hukuka uygun şekilde uygulanan bir tedbir aracılığıyla edilmiş olsa dahi delillerin değerlendirilmesini engelleyen kurallar söz konusu olabilir. Örneğin işkence ile alınmış bir ifadenin ispat faaliyetinde dikkate alınamaması, hukuka aykırı araçlara başvurularak elde edilmiş delilin kullanılamamasına örnek teşkil eder. Bununla birlikte hukuka uygun bir iletişimin dinlenmesi kararına istinaden kayda takılan görüşmede, şüpheli ile tanıklıktan çekinebilecek kişi arasındaki iletişimin delil olarak kullanılamaması, ikinci tür değerlendirme yasağına örnektir. Bu örnekte delilin elde edilme aracı hukuka aykırı olmamakla birlikte CMK m. 135/3 kapsamında açıkça yasaklandığından yine değerlendirilemeyecektir[763].

CMK m. 206/2 (a) kapsamında, kanuna aykırı elde edilmiş delillerin ikame edilmesi yasağı açıkça düzenlenmektedir. Dolayısıyla delillerde hukuka aykırılığın genel sonucu ilgili maddede gösterilmektedir. CMK m. 217/2 ise mutlak bir değerlendirme yasağı öngörmekte, hukuka aykırı delillerin hükme esas alınamayacağını, dolayısıyla ilgili delilin olayın ispatında kullanılamayacağını belirtmektedir[764]. Bu maddelerde hukuka aykırılığın şekli veya maddi olması, sanık haklarını ağır ya da hafif şekilde ihlal edilmiş olması gibi ayrımlara gidilmemiş,

---

[761] Gödekli, s.1825.
[762] Ahmet Gökçen/Kerem Çakır, "Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi Ve Delil Yasakları", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Durmuş Tezcan'a Armağan, Cilt:21, Özel Sayı, 2019, ss. 2911-2951, s.2934; Gödekli, s.1825.
[763] Yenidünya, "Ceza Muhakemesinde Delillerin Değerlendirilmesi, Delil Yasakları ve Hukuka Aykırı Delillerin Ceza Yargılamasında Vaziyeti".
[764] Centel/Zafer, s. 860, Birtek s. 298.

hukuka aykırı her türlü delil için ikame ve değerlendirme yasağı öngörülmüştür. Dolayısıyla hukuka aykırı yöntemle elde edilen delilin kullanılamayacağı konusunda mutlak bir değerlendirme yasağı söz konusudur[765]. Kanun koyucu bu konuda hâkime takdir hakkı tanımamıştır. Bununla birlikte kimi Yargıtay kararlarında ileride tartışılacağı üzere mutlak değerlendirme yasağının esnetildiği görülmektedir.

Delil değerlendirmeye ilişkin genel yasakların yanı sıra bazı özel düzenlemeler de bulunmaktadır. Örneğin şüpheli ve sanığın beden muayenesi ve vücudundan örnek alınması tedbiri için hâkim kararı bulunmadığı ve hâkim tarafından 24 saat içinde onay verilmediği durumlarda söz konusu yöntemlerle elde edilen delillerin ceza muhakemesinde kullanılamayacağı CMK m.75/1 kapsamında açıkça düzenlenmektedir. CMK m. 148/3 kapsamında yasak usullerle elde edilen ifadelerin rıza ile verilse dahi delil olarak değerlendirilemeyeceği ve yine aynı maddenin 4. fıkrasında müdafi hazır bulunmaksızın kollukça alınan ifadelerin, hâkim veya mahkeme huzurunda şüpheli veya sanık tarafından doğrulanmadığı hallerde hükme esas alınamayacağı açıkça düzenlenmiştir[766].

Farklı amaçlarla toplanan verilerin, profilleme teknolojilerinde kullanılması halinde, diğer bir yasak olan PVSK ek madde 7 de önem kazanmaktadır. PVSK m. 7'de telekomünikasyon yoluyla iletişim tespiti ve teknik araçlarla izleme tedbirlerine önleyici amaçlarla başvurulması düzenlenmekte, bu amaçlarla toplanan delillerin başka amaçlarla kullanılamayacağı açıkça belirtilmektedir. Önleyici tedbirlerde temel amaç, gelecekte gerçekleşme ihtimali olan bir suçu engellemek, suç tehlikesinin kaynağına müdahale etmektir. Bu amaç kapsamında alınan tedbirler idare hukukunun konusudur. Ancak suçun işlenmesi ile birlikte adli merciler yetki kazanacak, kişi hak ve özgürlüklerine yönelik müdahaleler CMK usulüne uygun şekilde gerçekleştirilecektir[767]. İdare hukuku ile ceza hukukunu ayıran bu çizgi aşılmamalı, önleyici amaçla toplanan deliller muhakeme sürecinde kullanılmamalıdır. Aksi halde ceza muhakemesi usulünün etrafından dolaşılmasına izin verilmiş olacaktır. Bu husus

---

[765] Doktrinde çoğunluk görüşü de Anayasa ve kanunun lafzının nispi değerlendirme sistemine izin vermediği yönündedir, Öztürk/Tezcan/Erdem/Gezer/Saygılar Kırıt/Alan Akcan/ Tütüncü Erden/Altınok Villemin, s. 400, Centel/Zafer, s.862, Akyürek, s. 70-71.

[766] Birtek, s. 298.

[767] Kızılırmak, Baran, **Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği**, İstanbul Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul 2018, s. 50.

kişisel verilerin işlenmesinde amaca uygunluk ilkesi ile de paralellik göstermektedir. Nitekim Kişisel Verilerin Koruması Kanunu 4. maddede açıkça verilerin ancak belirli, açık ve meşru amaçlar için, bu amaçla bağlantılı ve sınırlı olacak şekilde işlenebileceği belirtilmektedir. Bu nedenle, önleyici amaçla uygulanan tedbirler sonucu elde edilen delillerin, adli amaçlar da dâhil diğer amaçlar için kullanılması ve değerlendirilmesi hem PVSK hem KVKK gereği mümkün değildir.

Hukuka aykırı deliller açısından önem taşıyan diğer bir husus özel kişiler tarafından hukuka aykırı şekilde toplanan verilerin değerlendirilip değerlendirilemeyeceğidir. Anayasa Mahkemesi, özel kişiler tarafından toplanan hukuka aykırı delillerin de değerlendirilemeyeceğinin altını çizmiştir. "Aksi halde resmi makamların delil toplamak için yasadışı mafya benzeri oluşumlara dayanması"nın yolu açılacak, bu yol bir kez açılacak olursa, delil yasakları anlamını yitirecek, hukukun dolanılması mümkün kılınmış olacaktır[768]. Hukuka aykırı delil değerlendirme yasağının amacının geniş anlamda hukuk devletini tesis olduğu dikkate alındığında, özel kişilere yönelik bir istisnanın gözetilmesi kuşkusuz ki bu amaçla çelişecektir. Nitekim Anayasa m. 38 ve CMK m.217 hükümleri uyarınca, hukuka aykırılığın kim tarafından gerçekleştirildiğinin önemi bulunmamaktadır. Herkes bu hükümlerin muhatabıdır[769]. Bununla birlikte Yargıtay kararlarında, işlenmekte olan bir suçla ilgili olarak, daha sonra kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkânının olmadığı ani gelişen durumlarda, mağdurların CMK usulüne uygun olmayan şekilde kayda aldıkları sanıkla yaptıkları konuşmalar ve sanığa ilişkin görüntüler hükme esas alınabilmektedir. Buna gerekçe olarak aksi takdirde kanıtların kaybolması ve bir daha elde edilmesinin mümkün olmaması gösterilmektedir[770]. Bununla birlikte Yargıtay, faili kışkırtarak, tuzağa düşürerek, iradesini sakatlayarak, önceden planlanmış şekilde elde edilen kanıtların hukuka aykırı kabul edilmesi gerektiğini ve bu tür delillerin değerlendirilmesinin CMK m. 217'ye aykırılık teşkil ettiğini kabul etmekte ve bu kayıtların delil olarak kullanılmasının yargılamanın hakkaniyetini zedelediğinin altını çizmektedir[771].

---

[768] AYM E:1999/2, K:2001/2, T:22.6.2001'den aktaran Akyürek, s. 78.
[769] Birtek, s.319.
[770] Yargıtay 4. CD, E. 2017/1889, K. 2020/20924, T. 22.12.2020, CGK, 21.06.2011, E:2010/5-182, K:2011/131, https://lib.kazanci.com.tr/, Erişim Tarihi: 10.09.2021.
[771] Örneğin katılanın, sanığın kendisine hakaret ettiğini iddia ettiği olaydan bir gün sonra sanıkla buluşma ayarlayıp aralarındaki konuşmayı gizlice kaydetmesi, konuşmayı yönlendirerek sanığın yeniden hakaret içerikli sözler söylemesine neden olması karşısında Yargıtay, durumun ani gelişmemesi ve sırf delil oluşturmak maksadıyla sanığın yönlendirilmiş olması nedeniyle, elde edilen

Yargıtay kimi zaman kamu görevlilerinin CMK mevzuatında öngörülen usulün dışına çıktığı hallerde de nispi hukuka aykırılık anlayışına dayanan kararlar vermektedir. Hukuka aykırılığın şekle mi yoksa esasa mı ilişkin olduğu noktasından hareket eden Yargıtay, kimi kararlarında ise sanığın hakları teorisinden yola çıkarak sanığın ihlal edilen bir hakkı olup olmadığını incelemektedir. Örneğin usulüne göre alınmış bir arama kararı bulunan olayda, CMK m. 119/4 uyarınca aramada hazır bulunması kişilerin bulunmamasını değerlendiren Yargıtay, sanığın kararın infazı sırasında yapılan işlemlere ve herhangi bir hakkının ihlal edildiğine yönelik bir itirazı olmadığı, sırf arama sırasında şekle ilişkin bir koşulun ihlal edilmesine dayanılarak aramanın hukuka aykırı sayılamayacağı ve bu yolla ele geçirilen delillerin de "hukuka aykırı olarak elde edilmiş delil" sayılmaması gerektiğine karar vermiştir[772]. Bununla birlikte Yargıtay, hâkim kararının bulunmaması ve gecikmesinde sakınca bulunmadığı halde savcı veya kolluk amiri tarafından karar alınması halinde, toplanan delilleri hukuka aykırı kabul etmektedir[773]. Yine ilgili koruma tedbirleri için aranan makul veya kuvvetli şüphe oluşmadan toplanan deliller bakımından Yargıtay'ın genel olarak mutlak hukuka aykırılık doktrinini uyguladığı görülmektedir[774].

Uygulamada "sanık hakları ihlal edilmediği hallerde hukuka aykırı şekilde elde edilen delillerin kullanılabilmesi" gerektiği ifade edilmekte, "basit" hukuka aykırılıklara dayanılarak delillerin dışlanmasının yargılamanın işleyişini engellediği ileri sürülmektedir. Yargıtay'ın sanık hakları ile suçun topluma verdiği zararı karşılaştırdığı, sanığın topluma verdiği zarar daha fazla ise hukuka aykırı olarak elde

---

ses kaydını hukuka aykırı delil olarak kabul etmiştir, bkz. Yargıtay CGK, E. 2018/18-39, K. 2020/485, T. 1.12.2020, Erişim Tarihi: 10.09.2021. Yine başka bir kararda Yargıtay, hırsızlık suçuna ilişkin kanıt elde etmek amacıyla sanığın eve çağrılarak ikrar içeren ifadelerinin kayıt altına alınması karşısında, bu kaydın hukuka aykırı kabul edilmesi ve hükme esas alınmaması gerektiğini belirtmiştir, bkz. Yargıtay, 13. CD, E. 2014/10489, K. 2014/25006, T. 10.9.2014, https://lib.kazanci.com.tr/, Erişim Tarihi: 10.09.2021.

[772] Yargıtay CGK, E: 2011/8-278, K: 2012/96, T.13.3.2012, https://lib.kazanci.com.tr/, Erişim Tarihi: 10.09.2021, YCGK, E: 2007/7-147, K: 2007/159, 26.6.2007, aktaran, Gödekli, s. 1863.

[773] Yargıtay CGK, E. 2016/20-805, K. 2019/480, T. 18.6.2019, Yargıtay 8. CD, E. 2016/2625, K. 2017/744, T. 26.1.2017, Yargıtay 20. CD, E. 2015/14678, K. 2016/809, T. 16.2.2016, https://lib.kazanci.com.tr/, Erişim Tarihi: 10.09.2021.

[774] Örneğin Yargıtay verdiği bir kararda "somut olayda katılan vekilinin şikâyet dilekçesinde sanığın korsan kitap sattığına dair delil ve emareden bahsedilmediği gibi, genel, soyut nitelikte iddialara yer verilmiştir" diyerek makul şüphe oluşmaksızın yapılan arama sonucu elde edilen delilleri hukuka aykırı kabul etmiştir, bkz. Yargıtay 7. CD, E. 2013/5178, K. 2013/23749, T. 27.11.2013. Sanığın "çeşitli suçlardan kaydı bulunduğu" iddiasının makul şüphe oluşturmadığı ve bu yolla elde edilen delilin hükme esas alınamayacağına ilişkin bkz. Yargıtay 2.CD, E: 2012/29290, K: 2013/27219, T. 20.11.2013, https://lib.kazanci.com.tr/, Erişim Tarihi: 10.09.2021.

edilen delillin kullanılabileceğini belirttiği görülmektedir[775]. Oysa nispi hukuka aykırılık yorumu mevcut düzenlemelere aykırıdır. Nitekim Anayasa ve CMK hükümleri, sanık hakları teorisini veya hakların dengelenerek ağır suçlar açısından belirli hukuka aykırılıkların göz ardı edilmesine izin vermemekte, hukuk kurallarına bir bütün olarak saygıyı ön plana çıkarmaktadır[776]. Mevcut düzenlemeler ışığında bu anlayışı değiştiren ve esneten yorumlar, yargının yasama yetkisine müdahalesi anlamına gelecektir. Bunun yanı sıra "çıkarların dengelenmesi" görüşü hukuk güvenliğini, temel hak ve özgürlükleri tehdit etmektedir. "Kamu düzeni" gibi kavramların karşısında bireysel hak veya çıkarların değerlendirilmesi, bir denge kurulmasından ziyade "bir hakkın ya da çıkarın feda edilmesi"ne yol açacaktır. Örneğin devleti güvenliği ile ilgili suçlar veya kişilere yönelik cinsel saldırı, kasten öldürme gibi suçlar söz konusu olduğunda bu suçlarla korunan hukuki menfaat, şüpheli/sanığın ihlal edilen hakkından üstün tutulacağından, uygulamada ceza muhakemesi usullerine ve genel olarak hukuka aykırı tüm eylemler, neredeyse otomatik şekilde kabul edilebilir hale gelecektir. Bu durum özellikle "ulusal güvenlik" gibi amaçlar karşısında hukuka aykırılıkların yargılamada göz ardı edileceği bir sistemin kapılarını aralamaktadır[777].

Yargıtay'ın ayrıca hüküm kurulurken hukuka aykırı delile dayanılmamış olması, başka bir deyişle hükümle hukuka aykırı delil arası nedensellik bağı bulunmaması veya hukuka aykırı delil olmasaydı da mahkûmiyet için yeterli delillerin bulunması gibi gerekçelerle hukuka aykırı delillere tolerans gösterildiği görülmektedir[778]. Bununla birlikte söz konusu uygulama CMK m.289 hükmüyle çelişmektedir. 289/1-i maddesi, hükümde hukuka aykırı yöntemlerle elde edilen delile dayanılmasını yasaklamış, diğer delillerin hüküm kurmak için yeterli olması veya hukuka aykırı delilin nedensel olarak hükme katkısı gibi unsurlara yer vermemiştir. Dolayısıyla hukuka uygun elde edilmiş diğer delillerle de aynı sonuca varılabilecek olması sonucu değiştirmeyecek, hukuka aykırı delilin hükme esas alınması mutlak

[775] Yargıtay CGK, E: 2005/10-15, K: 2005/29, 15.3.2005, Yargıtay 7.CD, E: 2013/5127, K: 2013/17549, T.3.7.2013, aktaran Gödekli, s.1865.
[776] Birtek, s. 315.
[777] Akyürek, Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu, s.75.
[778] Yargıtay CGK, E. 2007/7-147, K. 2007/159, T. 26.6.2007, Yargıtay CGK, 29.11.2005, E. 2005/7-144, K. 2005/150, aktaran Birtek, s.314.

bozma sebebi olarak kabul edilecektir[779]. Bu nedenle, söz konusu kararlar, CMK m. 289'a da aykırılık teşkil etmektedir.

Son olarak delillerin uzak etkisinin ele alınması gerekmektedir. Mutlak değerlendirme yasağı çerçevesinde yapılmış düzenlemelerin, hukuka aykırı yollar ile doğrudan elde edilen delilleri kapsadığı hususunda hiç şüphe bulunmamaktadır. Bununla birlikte doktrinde, hukuka aykırı delillerden türetilen veya bunlar aracılığıyla elde edilen diğer delillerin hükme esas alınıp alınamayacağı tartışmalıdır. Anglo-Sakson hukuk sisteminde "zehirli ağacın meyvesi de zehirli olur" şeklinde ifade edilen bu kuram, Türkiye'de ve pek çok ülke mevzuatında yazılı şekilde düzenlenmemiştir. Bununla birlikte bu kuramın kabulü veya reddi ceza muhakemesi doktrin ve uygulaması açısından oldukça önemli bir etkiye sahiptir. Bu kurama göre, hukuka aykırı delilden yola çıkarak elde edilen diğer deliller (zehirli ağacın meyveleri) de hükme esas alınamamalıdır.

Doktrinde Anayasa m. 38, CMK m. 217/2 ve CMK m. 206/2(a) birlikte değerlendirilerek, bu hükümlerin dolaylı delil ve doğrudan delil ayrımı yapılmaksızın tüm hukuka aykırı deliller için uygulanacağı belirtilmektedir[780]. Nitekim hukuka aykırı bir zemin üzerine hukuka uygun bir bina inşa edilemez. Yasa koyucunun amacının hukuk devletine ve dürüst işlem ilkesine saygı olduğu bir sistemde, hukuka aykırı delillerin uzak etkisinin kabul edilmemesi, bu kuralların etrafından dolanılmasına yol açacaktır.

Bununla birlikte uygulamada, Yargıtay kararlarında delillerin uzak etkisinden açıkça bahsetmekten kaçınıldığı görülmektedir. Örneğin istihbari çalışmalar sonunda edinilen bilgiye dayanılarak, hâkim kararı olmaksızın ve aramanın diğer şartlarına uyulmaksızın sanığın evde bulunmadığı esnada, "eşinin muvafakati ile" arama yapılması üzerine sanığın evinde hint kenevirlerinin bulunduğu olayda, sanık aramanın ardından teslim olmuş ve ikrarda bulunmuştur. Yargıtay, arama sonucu ikrarda bulunan sanığın ikrarını hukuka aykırı delillerin bulunması üzerine suçun itiraf

[779] Centel/Zafer, s. 860, 861.
[780] Öztürk/Tezcan/Erdem/Gezer/Saygılar Kırıt/Alan Akcan/ Tütüncü Erden/Altınok Villemin, s. 422, Birtek, s. 339, Ünver/Hakeri, s.1594. Hukuka aykırı delillerin uzak etkisini, suç oluşturan eylemlerle elde edilen deliller bakımdan sınırlı şekilde kabul eden görüş için bkz. Yenisey/Nuhoğlu, s. 576, Dülger, **Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağaçların Meyvesi Öğretisi)**, s.109.

edilmesi olarak görmemiş, başka bir deyişle zehirli ağacın meyvesi doktrinini uygulamamıştır. Hükümde arama sonuçlarını hukuka aykırı delil olarak kabul eden Yargıtay, hükmün arama sonucu elde edilen delillere değil, sanığın "özgür ve iradi" ikrarına dayandığını belirterek mahkûmiyet kararını onamıştır. Yalnızca karşı oy gerekçesinde, sanığın ikrarının, evinde hint keneviri bulunduğuna dair arama zabıtlarının önüne konulmasının ardından gerçekleştirdiği, köşeye sıkıştığını hisseden sanığın itirafının hukuka aykırı şekilde elde edilmiş delillerin sonucu olduğu vurgulanmış, hukuka aykırı arama ile elde edilen delile dayanan ikrarın da hukuka aykırı delil olduğu ve "zehirli ağacın meyvesi" olarak yargılamada kullanılamayacağı belirtilmiştir[781]. Başka bir kararda, ihbar üzerine kolluk görevlilerince sanığın üst araması yapılan olayda, söz konusu arama için kolluk görevlileri herhangi bir talimat almadığı gibi, arama sonucu savcıya dahi bildirilmemiş, bu arama üzerine sanığın evinde esrar bulundurduğu ikrarı üzerine sanık ile birlikte evine giden kolluk görevlileri, sanığın evinde esrar bulmuştur. Bu olayda ilk aramanın hukuka aykırılığından yola çıkarak elde edilen diğer delillerin de yargılamada kullanılamayacağı görüşü yine karşı görüş olarak azınlıkta kalmıştır[782]. Bununla birlikte Yargıtay Ceza Genel Kurulu 2009 tarihli kararında hukuka aykırı usullerle elde edilen delillerin yanı sıra bu deliller aracılığıyla edinilen ikrarın özgür irade ürünü sayılamayacağını kabul etmiş, hukuka aykırı delillerin dolaylı etkisini açıkça kabul etmiştir[783]. Yine Yargıtay'ın verdiği yakın tarihli bir kararda genel ve soyut iddialara dayanılarak yapılan aramanın hâkim kararına dayansa dahi hukuka aykırı kabul edileceği, bu arama sonucu elde edilen bandrolsüz kitaplar kadar, bu kitapların incelenmesine dayanan ve dolaylı delil olan bilirkişi raporunun da hukuka aykırı delil kabul edilmesi gerektiğini belirtmiştir[784]. Dolayısıyla hukuka aykırı delillerin uzak etkisine ilişkin yeknesak bir uygulamanın olmadığını söylemek mümkündür.

---

[781] Yargıtay CGK, E. 2005/7-144, K. 2005/150, T. 29.11.2005, https://lib.kazanci.com.tr/, Erişim Tarihi: 11.09.2021.

[782] Yargıtay 10. CD, E. 2020/21403, K. 2021/2205, T. 16.2.2021. Benzer şekilde hukuka aykırı delillerin uzak etkisinin çoğunluk tarafından kabul edilmediği ancak muhalefet görüşünde belirtildiği kararlar için, bkz Yargıtay 19. CD, E. 2015/12122, K. 2015/6823, T. 9.11.2015; Yargıtay 19. CD E. 2015/8078, K. 2015/6366
T. 2.11.2015, https://lib.kazanci.com.tr/, Erişim Tarihi: 11.09.2021.

[783]Yargıtay CGK, E. 2009/7-160, K. 2009/264, T. 17.11.2009, https://lib.kazanci.com.tr/, Erişim Tarihi: 11.09.2021.

[784]Yargıtay 7. CD, E. 2013/5178, K. 2013/23749, T. 27.11.2013, https://lib.kazanci.com.tr/, Erişim Tarihi: 11.09.2021.

Sonuç olarak yerel mevzuat açısından hukuka aykırı deliller düzenlenirken, karşılaştırmalı hukukta olduğu gibi sanık hakları, hakların dengelenmesi, iyi niyet teorisi gibi teorilere dayanılmamış, hukuk devleti ilkesine saygı esas alınmıştır. Bu anlayışla düzenlenmiş olan Anayasa m. 38, CMK m. 206/ 2 (a), 227/2, 289/1 (i) hükümlerinde hukuka aykırı olarak ele geçirilen her türlü veri ve bulgunun, ceza muhakemesinde delil niteliğini haiz olamayacağı, ikame edilemeyeceği ve hükme esas alınamayacağı düzenlenmiştir. Kanunda hukuka aykırı delillerin değerlendirilmesini ve bu delillere dayanılarak elde edilen diğer delillerin hükme esas alınmasını mümkün kılan herhangi bir açıklık bulunmamaktadır. Mutlak değerlendirme yasağı gereği, hukuka aykırılık ya bulunmakta ya da bulunmamaktadır. Dolayısıyla hukuk düzeninin öngördüğü herhangi bir hukuk kuralının ihlali halinde, artık bu delillerin ve bu delillerden yola çıkarak elde edilen "zehirli meyvelerin" hükme esas alınmaması gerekir. Bu bağlamda uygulamanın mevcut kanun hükümlerinin dışına taşarak, kimi zaman karşılaştırmalı hukuktaki teori ve ilkelere dayandığı görülmektedir. Ancak bu ilke ve kuralların ülkemizde uygulanması, mevcut düzenlemeler açısından ihlal teşkil edecek niteliktedir. Bu nedenle mevzuatta yeni bir düzenleme yapılmadığı takdirde kanun koyucunun iradesinin dışına taşılmaması ve mutlak değerlendirme yasağının yeknesak şekilde uygulanması gerekir.

c) AİHM Kararlarında Hukuka Aykırı Delil ve Delillerin Uzak Etkisi

AİHM, hukuka aykırı delillerin ceza muhakemesinde kullanılmasını AİHS m. 6'da düzenlenen adil yargılanma hakkı kapsamında ele almaktadır. İlgili maddede hukuka aykırı delillerin hükme esas alınamayacağına ilişkin açık bir düzenleme bulunmamaktadır. Nitekim Sözleşmeye taraf devletlerin hukuka aykırı delillerin değerlendirilmesi hususunda farklı düzenlemelere sahip olduğu ve farklı yaklaşımlar sergiledikleri görülmektedir. Bu nedenle AİHM, stratejik bir yaklaşımla hangi delillerin hukuka aykırı kabul edilmesi gerektiğini takdir etmeyi taraf devletlerin iç hukukuna bırakmaktadır. Bu nedenle Mahkeme, nispi değerlendirme yasağı veya mutlak değerlendirme yasağından birini tercih etmemekte, taraf devletleri bu sistemlerden birini benimsemeye zorlamayarak bunu devletlerin takdir yetkisi kapsamında görmektedir. Bununla birlikte Mahkeme, yargılama sürecini bir bütün

olarak değerlendirerek, hukuka aykırı delillerin adil yargılanma ilkesini zedeleyip zedelemediğini incelemektedir[785].

Örneğin Schenk/İsviçre kararında Mahkeme, hukuka aykırı şekilde yapılan telefon görüşmesi kaydına ilişkin yaptığı değerlendirmede, hangi delillerin iç hukukta hükme esas alınıp alınamayacağını değerlendirme yetkisi olmadığını, bir delilin iç hukukta öngörülen usule aykırı şekilde toplanmış olmasının otomatik olarak AİHS m. 6'yı ihlal etmeyeceğini belirtmiştir. Bununla birlikte Mahkeme, sanığa bu tür delillere karşı savunma ve delilleri çürütme hakkı tanınıp tanınmadığı, hüküm verilirken salt hukuka aykırı şekilde elde edilmiş delillere dayanılıp dayanılmadığını AİHS m. 6 kapsamında inceleme yetkisi bulunduğunu belirtmiştir. Mahkeme, mevcut davada, sanığın aleyhine delil olarak kullanılan ses kaydına erişim, kaydın sağlamlığı ve güvenilirliğini sorgulama ve kaydın hâkim kararı olmaksızın yapılmasına karşı çıkma hakkının bulunması ve mahkûmiyet hükmünde ses kayıtları dışında pek çok delilin hükme esas alınmış olması nedeniyle, bir bütün olarak davada adil yargılanma hakkının ihlal edilmediğine karar vermiştir[786]. Benzer bir şekilde Khan/Birleşik Devletler kararında da Mahkeme, kolluk tarafından ses kaydı alma yetkisinin, iç hukukta açıkça düzenlenmediğini, bununla birlikte bu şekilde elde edilen delilin ilk ve ikinci derece mahkemeleri önünde her aşamada mahkemeler tarafından irdelendiğini, başvurucunun bu delile mahkeme önünde karşı çıkma hakkını kullanabildiğini belirtmiştir. Dolayısıyla söz konusu delilin toplanma şeklinin özel hayatın gizliliğini ihlal etmekle birlikte adil yargılanma hakkını ihlal etmediğine karar vermiştir[787].

Dolayısıyla, AİHM içtihatlarında özel hayatın gizliliğini ihlal eden usuller söz konusu olduğunda, örneğin arama ve dinlemeye ilişkin açık düzenlemeler bulunmadığı, bu düzenlemelere aykırı usullerle müdahale gerçekleştiği veya orantısız şekilde müdahalelerde bulunulduğu hallerde AİHS kapsamında özel hayatın gizliliğini düzenleyen m. 8 kapsamında inceleme yapmaktadır. Böyle durumlarda Mahkeme m. 8'in ihlal edildiğini kabul etmekle birlikte, bu şekilde elde edilen delillerin ceza muhakemesinde kullanılması doğrudan adil yargılanma hakkının ihlali olarak kabul etmemektedir. Mahkeme, hukuka aykırı şekilde elde edilmiş olsa dahi toplanan

[785] Gödekli, s. 1871.
[786] AİHM, Schenk/ İsviçre, Başvuru No: 10862/84, 12.07. 1988, https://hudoc.echr.coe.int/, para. 46-49, Erişim Tarihi: 25.09.2021.
[787] AİHM, Khan/Birleşik Krallık, Başvuru No: 35394/97, 12 Mayıs 2000, aktaran Gödekli, s. 1872.

delillerin sağlamlığı, güvenilirliğinin tartışmaya açılabilmesi, bu delillere karşı savunma hakkının kısıtlanmaması, bu delillerin tek başına hükme esas alınmaması gibi tüm unsurları bir arada değerlendirerek, yargılamanın bütün olarak adil olup olmadığını ele almaktadır[788].

Mahkeme, susma hakkının hatırlatılmaması veya sanığın müdafiden yararlandırılmaması gibi durumlarda ise özel hayatın gizliliğini ihlal tespitinden daha sert bir tavır sergilemektedir. Bu tür usul ilkelerinin ihlali halinde sanık ifadesine dayanılamayacağını, kişinin kendisini suçlamama hakkı ve susma hakkının da adil yargılanma hakkının temeli olduğunu belirtmektedir[789]. Dolayısıyla ifade ve sorgu yöntemlerine aykırılık bulunması halinde, bu delillerin yönlendirdiği bir yargılama, tartışmasız şekilde adil yargılanma ilkesini ihlal edecektir.

AİHM, AİHS m. 3 kapsamında düzenlenen işkence, insanlık dışı veya aşağılayıcı muamele yasağının ihlali halinde yine doğrudan adil yargılanma hakkının ihlal edildiğine karar vermektedir. İfade ve sorgu yasaklarını ihlal eden yöntemlerle elde edilen delillerin kullanılmasının bu yöntemleri meşrulaştıracağı, bunun şiddetin hukuki değerlendirme kisvesi altında şiddetin kabul edilmesi anlamına geleceğini belirtmektedir[790]. AİHM kararlarında, AİHS m.3'ün demokratik hukuk devletlerinin en temel ilkesi olduğunu, bu ilkenin olağanüstü hallerde dahi askıya alınamayacağını ve bu ilkenin ihlalinin işlenen suçun ağırlığı, devlet güvenliği ve bütünlüğünün tesisi gibi amaçlarla meşrulaştırılamayacağını vurgulamaktadır. AİHS m.3'ü ihlal eden bu tür yöntemlere başvurulmasının susma hakkı, kendini suçlamama hakkı gibi AİHS m. 6 kapsamında düzenlenen temel hak ve ilkeleri de doğrudan ihlal edeceğini belirtmektedir[791]. Bununla birlikte oldukça eleştirilen Gäfgen/Almanya kararında bir çocuğu kaçıran ve karşılığında fidye talep eden başvurucu, kolluğun takibi ile yakalanmış, çocuğun yerini söylemesi için kolluk tarafından tehdit edilmesinin ardından cesedin yerini tarif etmiştir. Ceset üzerinde yapılan DNA incelemesi

---

[788] Quattrocolo, s. 79.

[789] Bu yönde kararlar için, Allan/Birleşik Krallık, Başvuru No: 48539/99, T. 5.11.2002, Aleksandr Zaichenko/ Rusya, Başvuru No:39660/02, T.18.02 2010, Salduz/Türkiye, Başvuru No:36391/02, 27.11. 2008, aktaran Mcbride, Jeremy, "The Case Law of the European Court of Human Rights on Evidentiary Standards in Criminal Proceedings", https://rm.coe.int/council-of-europe-georgia-european-court-of-human-rights-case-study-ev/16807823c3, s.24, dipnot 105-106, Erişim Tarihi: 25.09.2021.

[790] AİHM, Harutyunyan/ Ermenistan kararı, Başvuru No:36549/03, T. 28.06.2007, para 63. https://hudoc.echr.coe.int/, Erişim Tarihi: 25.09.2021.

[791] AİHM, Jalloh/Almanya, Başvuru no: 54810/00, 11/07/2006, para 99-100, https://hudoc.echr.coe.int/, Erişim Tarihi: 25.09.2021.

başvuranın DNA'sı ile örtüşmüş ve söz konusu DNA yargılamada kullanılmıştır. Başvuran ise suçu bir sonraki ifadesinde itiraf etmiştir. AİHM, ilk ifadenin hükme esas alınmamasını yeterli bulmuş, olaydaki diğer deliller açısından zor kullanma veya tehdit gibi yöntemlerin kullanılmasının söz konusu olmadığını belirterek adil yargılanma hakkının ihlal edilmediğini kabul etmiştir[792]. Ancak tehdit altında verilen bir ifadeden türetilen delillerin kabul edilmiş olması, karşı görüş yazılarında belirtildiği gibi işkence ve kötü muamele yasağına ilişkin mutlak bir koruma kalkanını kaldırmakta, bu ilkenin etrafından dolaşılmasını mümkün kılmaktadır.

Sonuç olarak Avrupa İnsan Hakları Mahkemesi'nin görevi üye devletin yaptıkları uygulamaların Avrupa İnsan Hakları Sözleşmesi ve Ek Protokolleri'nde korunan temel hak ve özgürlükleri ihlal edip etmediğini belirlemekle sınırlıdır. Bu bağlamda, AİHM, Sözleşme kapsamında tanımlanan haklar çerçevesinde yerel mahkemelere göre daha dar ve özel bir değerlendirme yapmaktadır. Mahkeme, hukuka aykırı delilin hükme esas alınmaması gerektiğine ilişkin bir hüküm vermekten kaçınmakta, genel olarak bütün soruşturma ve kovuşturma sürecinin Sözleşme'nin 6. maddesi çerçevesindeki adil yargılanma hakkına uygun olarak yürütülüp yürütülmediği ile ilgilenmektedir. Bununla birlikte Mahkeme'nin mutlak değerlendirme yasağını benimsemesinin önünde herhangi bir hukuksal engel bulunmamaktadır[793]. Buna rağmen AİHS m. 3'ün ihlal edildiği durumlar haricinde Mahkeme hukuka aykırı delillerin hükme esas alınamaması hakkında yol gösterici kararlar vermekten kaçınmaktadır. Aksine özel hayatın gizliliğini ihlal suretiyle elde edilen delillerin belli güvenceler altında kullanılabileceğini belirtmekte, hatta Gäfgen/Almanya kararıyla ifade ve sorgu yasaklarıyla elde edilen delillerden türetilen yeni delillerin kullanılabilmesinin önünü açmaktadır. Mahkemenin adil yargılanma ilkesi kapsamında hukuka aykırı delillerin muhakemede kullanılmasına ilişkin çizdiği asgari standartlara uyulması zorunludur. Bununla birlikte AİHM'nin bir üst derece mahkemesi olmaması sebebiyle daha çekingen şekilde ele aldığı bu standartların üzerine çıkılarak insan haklarını daha güçlü şekilde koruyan hükümlerin öngörülmesine herhangi bir engel bulunmamaktadır[794]. Bu nedenle, Türk mevzuatında

---

[792] AİHM/ Gäfgen/Germany, Başvuru No: 22978/05, T. 01.06.2010, para 178-188, https://hudoc.echr.coe.int/, Erişim Tarihi: 25.09.2021.
[793] Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", s 76.
[794] Bu yönde Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", s. 77.

mutlak delil yasağının benimsenmesi, her somut olayda farklı içtihatlarla karşı karşıya kalınmasına engel olmuş, kimi durumlarda insan onuruna ilişkin temel hakların bile etrafında dolaşılmasına izin veren düzenlemelerden daha fazla koruma sağlamıştır. Türkiye özelinde tek eksik, uygulamanın bu konuda yeknesak bir tavır sergilemesidir.

Bugün, profilleme teknolojilerinin ceza muhakemesinde kullanılması halinde, bunların hükme esas alınıp alınamayacağına ilişkin öngörülür bir uygulamanın sağlanması adına, yukarıda hukuka aykırı delilere ilişkin yürütülen tüm bu tartışmalar, profilleme teknolojileri özelinde değerlendirilmelidir. Bu nedenle, bir sonraki başlıkta profilleme teknolojileri ile elde edilen delillerin hukuka uygunluğu detaylı şekilde ele alınacaktır.

2. Profilleme Teknolojilerinin Hukuka Aykırı Delil Kapsamında Değerlendirilmesi

a) Karşılaştırmalı Hukukta Hukuka Aykırı Delil Olarak Profilleme Teknolojileri ve İlgili İçtihatlar

Karşılaştırmalı hukukta, özellikle Kıta Avrupa'sında nispi hukuka aykırılık sisteminin benimsenmesi, profillemenin hukuka aykırı niteliği değerlendirilirken farklı sonuçlara varılmasını mümkün kılmaktadır. Nitekim nispi hukuka aykırılık teorisi, kimi zaman işlenen suçun ağırlığı, kimi zaman ise değerler arası karşılaştırma sebebiyle bazı delillerin hukuka aykırı şekilde toplansa dahi hükme esas alınmasına göz yummaktadır. Bu durum, bazı davalarda profilleme teknolojilerinin kullanımının hukuka aykırı olduğu tespit edilse dahi bu teknolojiler eliyle varılan sonuçların kullanılmasını mümkün kılabilecektir. Yine bu hususta AİHM kararları tartışılırken altı çizildiği üzere, AİHM sistematiğinde özel hayatın gizliliğini ihlal eden tüm hallerde, bu şekilde elde edilen delillerin ceza muhakemesinden dışlanması zorunlu tutulmamaktadır. AİHM bu tür davalarda AİHS m. 8'in ihlal edildiğine hükmetmekle birlikte, sanığın bu tür delillere karşı savunma hakkını etkin şekilde kullanabilmesi ve başka delillerin de varılan hükmü desteklemesi üzerine adil yargılanma hakkının ihlal edilmediğine hükmetmektedir. Ancak AİHM özellikle susma hakkı ve müdafiden yararlanma hakkı gibi temel hakların kullanılmadığı hallerde doğrudan adil

yargılanma hakkının ihlal edildiğine hükmetmektedir[795]. Henüz AİHM önüne doğrudan profilleme ile ilgili bir dava gitmemiş, dolayısıyla profilleme teknolojilerinin savunma hakkını ve adil yargılanma hakkını ihlal edip etmediğine dair henüz bir AİHM içtihadı bulunmamaktadır. Ancak bu teknolojilerin çalışma usulünün savunma tarafından anlaşılamaması ve dolayısıyla vardıkları sonuca karşı gerçek bir görüş ileri sürülememesi, yine sanığın susma hakkının etrafından dolaşarak hakkındaki tüm verileri sınırsızca analiz etmeleri, ayrıca vardıkları sonucun doğruluğunun ve sağlamlığının bilimsel olarak tartışmalı olması, AİHM'nin adil yargılama kapsamında vurguladığı temel ilkeler ile uyuşmamaktadır.

Karşılaştırmalı hukukta risk analizi yapan profilleme teknolojilerinin delil niteliğine ilişkin yerel mahkemelerin birbirinden ayrışan kararlar verdiği görülmektedir. Hollanda'da La Hague Bölge Mahkemesi'nin SyRI profilleme sistemi hakkında yaptığı değerlendirme önemli bir örnektir. Sistem Risk Analizi (System Risk Indication) olarak ifade edilen SyRI, tüm vatandaşların finansal verilerini, sosyal yardım geçmişlerini, eğitim ve topluma uyum sağlamaya ilişkin verilerini toplamakta ve kişileri vergi kaçakçılığı ve diğer kaçakçılık suçlarını işleme risklerine göre puanlandırmaktadır. Yüksek puan alan kişiler, vergi otoriteleri, kolluk görevlileri, göçmen büroları tarafından daha detaylı soruşturulmaya tabi tutulabilmektedir. Mahkeme idare tarafından sevk edilen bu profilleme sisteminin hukukiliğini değerlendirirken, yukarıda tartışılan veri toplamada belirli amaç, amaçla sınırlı ve asgari veri toplama ilkesi gibi kişisel verileri koruma mevzuatındaki ilkeleri, bunun yanı sıra profilleme modelinin savunma hakkını mümkün kılacak şekilde şeffaf olup olmadığını, dolayısıyla adil yargılanma ilkesini esas almıştır. Mahkeme, bu tür profilleme teknolojilerinin kullanılabilmesi için öncelikle belirlilik ve öngörülürlük unsurlarını karşılayan bir kanuni düzenleme yapılması gerektiğini vurgulamıştır. Hollanda'da SyRI'ye ilişkin düzenleme bulunmakla birlikte, bu düzenlemenin verilerin toplanma amacı, sınırı ve özel hayatın gizliliğine ve kişisel verilerin korunmasına ilişkin güvenceler barındırmaması nedeniyle kanunilik unsurunu karşılamadığını belirtmiştir ve bunun yanı sıra özel hayatın gizliliği açısından orantısız bir müdahale oluşturduğunu tespit etmiştir. Bunun yanı sıra profillemeye konu modelin halkla paylaşılmadığı, hangi veri türlerinin kullanıldığı belirtilse de bu verilerin hangi parametrelere göre değerlendirildiğinin belirsiz olduğunun altı

[795] Bu yönde kararlar için, bkz dipnot 789.

çizilmiştir. Bu durum, profilleme sonucu kişilere açıklansa dahi kişilerin bu teknolojiye karşı etkin şekilde savunma yapmalarını imkânsız hale getirmektedir. Mahkemeye göre, profillemeye ilişkin yapılacak düzenleme, hangi verilerin kaçakçılık yapıldığı veya yapılacağı hususunda yüksek risk grubunu tespit etmede kullanılacağını da belirlemelidir. Tüm bu nedenlerle SyRI profilleme teknolojisinin kullanımı hukuka aykırı kabul edilmiştir. İlgili karar, profilleme teknolojilerini düzenleyen normların ne şekilde yapılması gerektiğine ışık tutması ve SyRI gibi risk analizi yapan profilleme teknolojilerine yönelik emsal karar olması nedeniyle çok önemlidir[796].

Amerika Birleşik Devletlerinde, sıklıkla başvurulan COMPAS profilleme teknolojisi ise State/Loomis davasına konu olmuştur[797]. İlgili davada sanık, hükme COMPAS ile varılan sonuçların esas alınmasına itiraz etmiştir. Sanık hakkında COMPAS ile yeniden suç işleme riskinin yüksek olduğu puanı verilmiş, sanık verilen hükümde bu değerlendirmeye dayanılmasının adil yargılanma hakkını ihlal ettiğini belirtmiştir. Gerekçe olarak, COMPAS'ın dayandığı modelin açıklanmaması, açıklanmayan bu modelin doğru sonuçlara vardığının da test edilememesi gösterilmiş, sanık, savunma hakkını kullanamadığını belirtmiştir. Bunun yanı sıra ilgili davada, COMPAS raporlarının, belirli gruplara ilişkin verilere dayanmasının ceza sorumluluğunun şahsiliğini ihlal ettiği ve bireyselleştirilmiş hükme varılmasını engellediği ileri sürülmüştür. Mahkemenin kararında, COMPAS'ın ticari sır olarak korunduğu ve hâkimlerle paylaşılmadığını belirtmiş, böyle durumlarda hâkim tarafından anlaşılamayan profilleme teknolojilerinin tek başına hükme esas alınmaması gerektiği vurgulanmıştır. Mahkeme, COMPAS kullanımının adil yargılanma hakkı ve kararın bireyselleştirilmesi üzerindeki potansiyel olumsuz etkilerinin üzerinde durmakla birlikte, COMPAS'ın kullanımını tamamen yasaklamamıştır. Aksine hâkimlerin, bu uygulamaların vardığı sonuçları diğer delillerle birlikte ele alabileceğini, varacağı hükmü bu sonuçlarla destekleyebileceğini belirtmiştir[798]. Bununla birlikte Mahkeme, COMPAS risk analiz değerlendirmelerinin bir kişiye yönelik hapis cezası verilip verilmeyeceğini veya verilecek cezanın ağırlığını

[796]ECLI:NL:RBDHA:2020:865, davaya ilişkin detaylar için bkz. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865, Erişim Tarihi: 20.10.2021, para 6.63 vd.

[797] Dava için bkz. 881 N.W.2d 749 (2016) 2016 WI 68, https://www.courts.ca.gov/documents/BTB24-2L-3.pdf, Erişim Tarihi: 20.10.2021.

[798] Loomis/State, https://www.courts.ca.gov/documents/BTB24-2L-3.pdf, Erişim Tarihi: 20.10.2021. para. 92

tespit etmeye elverişli olmadığını, yalnızca diğer delilleri desteklemek için kullanılabileceğini belirtmiştir[799]. Dolayısıyla bu davada COMPAS teknolojilerinin kullanımının hukuka aykırı delil olup olmadığı tespit edilmemiş, bunun yanı sıra diğer delillerle desteklendiği takdirde COMPAS'a başvurulmasının adil yargılanma hakkını ihlal etmeyeceği belirtilmiştir. Bununla birlikte, hâkimlerin COMPAS'ın çalışma şeklinin kendileriyle paylaşılmamasını, bu durumun delilin doğruluğu, sağlamlığı ve müşterekliğini incelemeye engel teşkil ettiğini değerlendirmemeleri büyük bir eksikliktir. Dolayısıyla hâkimler COMPAS'ın ne şekilde veri topladığı, dayandığı modelin eşitlik ilkesine uygun, doğru, bilimsel sonuçlara varıp varmadığı hususunu ele almamışlardır[800]. Amerikan sisteminde, hâkimlerin "objektif" olduğu iddiası ile uygulamada bir nevi kullanmak zorunda bırakıldıkları COMPAS'ın genel olarak hukuka uygunluğunu değerlendirmekten kaçındıklarını, diğer delillerin söz konusu olduğu olayda, bu delillere dayanarak adil yargılanma ilkesinin ihlal edilmediğine hükmettiklerini söylemek mümkündür[801].

Malenchik/State of Indiana davasında ise LSI-R profilleme uygulaması değerlendirilmiştir. Kişisinin suç geçmişi, eğitim ve iş durumu, finansal durumu, aile ilişkileri, birlikte yaşadığı kişiler, duygusal ve kişisel sorunları, genel hal ve tavırları gibi değişkenlere dayalı bu uygulamanın verdiği puanlamanın hükme esas alınmasına itiraz edilmiştir. Sanık bu delilin hukuka aykırı delil olduğu iddiasında bulunmamıştır. Daha ziyade, bu teknolojilerin dayandığı, kişinin geçmişinden yola çıkarak, bugün ve gelecekte yapacağı hareketlerin öngörülebileceği varsayımına karşı çıkmış, bu varsayımın bireylerin iradesini tanımadığını, bireylerin hareketlerini yönlendirme ve geçmişten ders alarak düzeltme ihtimalini yok saydığını belirtmiştir[802]. Mahkeme bu iddiayı reddederek uygulamanın bilimsel ve sistematik incelemelere dayandığını,

---

[799] Ibid, para. 104.

[800] Grup verilerine dayanan COMPAS'ın belli sosyo ekonomik grupları ve azınlık gruplarını daha yüksek oranda risk grubu olarak gösterdiği, dolayısıyla doğru sonuçlara varıp varmadığı iddiasının aynı zamanda ayrımcılık yasağını ilgilendirdiği ve Mahkeme tarafından bu hususlara ilişkin yeterli değerlendirme yapılmamasının yerinde olmadığı üzerine bkz. "Criminal Law Sentencing Guidelines, Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing: State v. Loomis, 881 N.W.2d 749 (Wis. 2016)", Harvard Law Review, Cilt: 130, 2017, ss.1530-1537,https://harvardlawreview.org/wp-content/uploads/2017/03/1530-1537_online.pdf, Erişim Tarihi: 20.10.2021, s.1534, 1535.

[801] COMPAS uygulamasının adil yargılanma hakkını ihlal etmediği üzerine benzer yönde bir karar için bkz. People v. Younglove, No. 341901, 2019 WL 846117, at *1 (Mich. Ct. App. Feb. 21, 2019), aktaran John Villasenor/Virginia Foggo, "Artificial Intelligence, Due Process, and Criminal Sentencing", **Michigan State Law Review**, Sayı:2, 2020, ss.295-354, s.338.

[802] Indiana Court of Appeals, No. 79A02-0902-CR-133, 09.06.2010, https://www.courts.ca.gov/documents/malenchik-decision.pdf, Erişim Tarihi: 22.10.2021, s. 2.

uygulama sonucu varılan sonuçların istatistiksel ve klinik olarak doğru olduğunu ve destekleyici delil olarak kullanılabileceğini belirtmiştir. Mahkeme bu davada State/Loomis davasına benzer şekilde ilgili profilleme teknolojilerinin veri işleme usulünün hukuka uygunluğunu değerlendirmemiş, yine bu delillerde bulunması gereken müştereklik ve hukuka uygunluk niteliklerini ele almamıştır. Bununla birlikte ilgili davada LSI-R veya SASSI gibi risk değerlendirme teknolojileri açısından amaç sınırı öngörülmüş, bu teknolojilerin kişiye daha ağır ya da hafif ceza vermek için kullanılamayacağı vurgulanmıştır. İlgili teknolojilerin, ancak ceza tespit edildikten sonra, ne tür bir rehabilitasyon rejimi uygulanacağını tespit etmek için kullanılması gerektiği vurgulanmıştır[803].

Yine LSI-R uygulamasının ele alındığı Rhodes/State[804] davasında ise Malenchik davasının tam tersi yönünde karar alınmıştır. Bu davada İndiana Temyiz Mahkemesi, LSI-R ve standart şekilde kişileri puanlayan diğer uygulamaların mahkemelerin kişiye özel, bireyselleştirilmiş hüküm verme yetkisini aşındırdığı vurgulanmış, hatta daha da ileri gidilerek hâkimlerin bu tür teknolojileri hükme esas almasının takdir yetkisinin kötüye kullanılması anlamına geleceği belirtilmiştir[805].

Cardwell v. State kararında ise Yüksek Mahkeme sanıklara ilişkin risk değerlendiren profilleme teknolojileri hakkında önemli tespitlerde bulunmuştur. Mahkemeye göre, özünde sayılardan ibaret olan bu tür sistemlere dayanarak hüküm kurma, yargılama yetkisini mekanik bir sürece indirgeyecektir ki bu durum ceza muhakemesindeki sorunları azaltmak bir yana daha da fazla soruna yol açacak bir yaklaşımdır. Bu teknolojiler hükme esas alındığı takdirde, hâkimlerin kendi kendine düşünemeyen, bilinçsizce işleyen bu formüllerin adaletsiz sonuçlarına müdahale etmesi mümkün olamayacaktır. Bu noktada üst derece mahkemelerinin ödevi, failin karakterine göre mekanik şekilde hüküm verilmesine engel olmak, yani bu uygulamaların aldatıcı ışığında verilen hükümleri bozmaktadır[806].

---

[803] Ibid, s. 14.

[804] Rhodes v. State, 896 N.E.2d 1193 (Ind. Ct. App. 2008), https://www.casemine.com/judgement/us/591468dfadd7b049342ccffc, Erişim Tarihi: 22.10.2021.

[805] Karardan aktaran Villasenor/Foggo, s. 338.

[806] Cardwell/ State, 896 NE2d 1193 (Ind Ct App 2008), https://www.casemine.com/judgement/us/5914b244add7b0493475ec9c#p1224, Erişim Tarihi: 21.10.2021.

Amerika özelinde kişisel verilerin korunmasına ilişkin GDPR veya 2016/680 sayılı Direktif benzeri tüm eyaletlerde geçerli olan bir düzenleme bulunmaktadır. Bu nedenle Amerikan mahkemelerince verilen kararlarda, genellikle bu teknolojilerin hukuka aykırı veri işleme boyutu üzerinde durulmamış, daha ziyade profilleme ile varılan sonuçların bilimselliği ve pragmatik açıdan hâkimlere destek olma ihtimali üzerinde durulmuştur. Hollanda'da verilen SyRI kararı ise profilleme teknolojilerinin kişisel verilerin korunması ve özel hayatın gizliliğini ihlal eden boyutunu vurgulamış, dolayısıyla SyRI'nin kullanımının özel hayatın gizliliği hakkı çerçevesinde hukuka aykırı olduğunu açıkça tespit etmiştir. Bununla birlikte bu kararlarda profilleme teknolojileri ile varılan sonuçların ceza muhakemesinde yeri ve delil değerine ilişkin genel bir tespit yapıldığından bahsetmek mümkün değildir. Bu kararların hiçbirinde, profilleme teknolojilerine ceza muhakemesi sistematiği içerisinde yaklaşılmamış, bu uygulamaların koruma tedbiri mi güvenlik tedbiri mi olduğu, bu uygulamalar sonucu ulaşılan sonuçların doğrudan tanık ifadesi, bilimsel delil veya bilirkişi görüşü çerçevesinde mi ele alınması gerektiği açıklanmamıştır. Profilleme teknolojileri, sui generis bir uygulama olarak ele alınsa dahi ceza muhakemesinde ne şekilde kategorize edileceğinin, sevk edilme amacının ve sınırlarının çizilmesi gerekir. Ancak bu noktada en temel sorun, profilleme teknolojilerinin geçmişte olan fiilin aydınlatılması ve maddi gerçeğin bulunmasına değil, failin tehlikeliliğine yoğunlaşmasıdır. Oysa risk kavramı, hümanist ceza muhakemesine yabancı bir kavramdır ve sanığın fiilinden yola çıkan ceza muhakemesinin değerler dizisine yabancıdır. Bu noktada en doğru olan, risk tespitine yönelmiş profilleme teknolojilerine ceza muhakemesinde bir yer açmamaktır. Bunun yerine bu teknolojiler ile varılan sonuçların, henüz bilimsellik, müştereklik ve hukuka uygunluk unsurlarını taşımaktan uzak olduğu göz önüne alınmalı ve bunların hükme esas alınamayacağını açıkça vurgulayan düzenlemeler yapılmalıdır.

b) Türk Mevzuatı Kapsamında Hukuka Aykırı Delil Olarak Profilleme Teknolojileri

Hukuka aykırı delillerin düzenlenmesinde, Türk mevzuatında hukuk devleti ilkesine saygı esas alınmış ve yalnızca CMK mevzuatına değil, tüm kanunlara, Anayasa'ya, uluslararası sözleşmelere ve hukukun temel ilkelerine aykırı şekilde elde edilen deliller, hukuka aykırı delil olarak kabul edilmiştir. CMK m. 206/2 (a) ve m. 217/2 ile bu delillere ilişkin mutlak bir değerlendirme yasağı öngörülerek, bu delillerin

hükme esas alınamayacağı, dolayısıyla ilgili delilin olayın ispatında kullanılamayacağı kabul edilmiştir[807]. Yine CMK m. 289/1-i ile hükümde hukuka yöntemlerle elde edilen delile dayanılması mutlak bozma sebebi olarak düzenlenmiştir.

Bu nedenle profilleme aracılığıyla elde edilen delillerin hukuka aykırı olup olmadığı incelenirken, salt ceza muhakemesi hükümlerine uygun olmaları değil kişisel verilerin korunması mevzuatına ve uluslararası sözleşmelere uygunluğu da ele alınmalıdır. Bu bağlamda delillerin hukuka uygunluğu incelemesi, kişisel verilerin korunması ve ceza muhakemesi mevzuatları arasında bağ kurmayı gerektirir. Dolayısıyla, profillemeye konu verilerin kişisel verileri koruma hükümleri ve ceza muhakemesindeki koruma tedbirlerine aykırı şekilde toplanması, işlenmesi ve analiz edilmesi halinde varılan sonuçların ceza muhakemesinde değerlendirilmesi mümkün değildir.

Ceza muhakemesinde kullanılan COMPAS, Static 99-R, Hart, Systeem Risico Indicatie, LSI-R gibi pek çok profilleme teknolojisinin işleme şekli tez kapsamında sıklıkla üzerinde durulduğu üzere geleceğe yönelik risk analizine dayanmaktadır. Bu analiz yapılırken kişilerin nüfus bilgileri, alkol ve uyuşturucu bağımlılıkları, adli sicilleri, günlük alışkanlıkları, sosyal çevreleri gibi pek çok farklı veri grubu ele alınmaktadır. Bu verilerin işlenmesinin hukuka uygunluğu değerlendirilirken, öncelikle kişisel veri olarak kabul edilip edilemeyecekleri, kişisel veri olarak değerlendirildikleri takdirde işleme süreçlerinin Kişisel Verileri Koruma mevzuatına uygunluklarının tespiti önem taşımaktadır. Profilleme teknolojilerine hangi rejimin uygulanacağının tesisi için, bunların kişisel veri işleyip işlemediği kadar, kim tarafından ve ne amaçla sevk edildikleri de önem taşımaktadır.

KVKK mevzuatı, kural olarak kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi koruma altına almaktadır. Profilleme teknolojilerinin belli bir kişinin adresi, nüfus kaydı, eğitim bilgileri, uzak geçmişi[808], internet hareketlerini[809] toplaması ve analiz etmesi halinde, kişisel verilere dayandığı hususunda bir şüphe

[807] Centel/Zafer, s. 859, 860, Birtek s. 298.
[808] Kişinin uzak geçmişinin işlenmesine ilişkin bkz. AİHM, Rotaru/Romanya, Başvuru no. 28341/95, paras 43, 44, T. 04.05.2000, https://hudoc.echr.coe.int, Erişim Tarihi: 10.10.2021.
[809] İnternet hareketlerinin denetimine ilişkin değerlendirme için bkz. AİHM, Copland/Birleşik Krallık, Başvuru no:62617/00, T.03.04.2007, para 41-43, https://hudoc.echr.coe.int, Erişim Tarihi: 10.10.2021.

bulunmamaktadır. Bununla birlikte kişinin kimliği henüz belirli olmadan, kimi zaman ilk bakışta anonim gözüken milyonlarca veri üzerinden yapılan grup profillemesinin söz konusu olduğu durumlarda, profillemeye sunulan ham verilerin kişisel verilerin korunması kapsamında kalmadığı ileri sürülebilir. Bu hususta AİHM kararlarında GDPR hükümleri ve gerekçelerini dikkate alınmaktadır. GDPR 26. gerekçesi belirlenebilirlik açısından, olayın tüm şartları, güncel teknolojik gelişmeler, kişiyi belirlemek için yapılacak masraf ve harcanacak zamanın dikkate alınması gerektiği vurgulanmaktadır[810]. Özellikle kolluğun farklı veri sorumlularından veri toplamasını engelleyen bir hüküm yoksa makul çaba ile farklı kaynaklardan birleştirilen veriler eliyle kişi belirlenebilecektir[811]. Türkiye özelinde 5651sayılı Kanun[812] çerçevesinde internet erişim, içerik ve yer sağlayıcılarının kişisel veri saklama yükümlülükleri öngörülmüş ve bu verilerin kolluk ile paylaşılmasını engelleyici herhangi bir hükme yer verilmemiştir. Yine PVSK m. 15 kapsamında kolluğun bilgi alma hakkı, herhangi bir sınır öngörülmeksizin düzenlenmiştir[813]. Dolayısıyla kolluğun soruşturma ve kovuşturma sürecinde profillemenin ilk aşaması olan veri toplama aşamasında dahi pek çok veri sorumlusuna erişimi ve farklı verileri birleştirerek kişileri "belirleyebilir" nitelikte verileri elde etmesi mümkündür. Bu nedenle muhakeme sürecinde profillemeye konu verilerin henüz süreç başında dahi kişisel veri olduğu kabul edilmelidir.

Profilleme teknolojilerinin kişisel veri işlediği tespit edildikten sonra, veri işlemenin hukukiliğini tespit için, önce bu verilerin kim tarafından ve ne amaçla işlendiği belirlenmelidir. Nitekim bir önceki bölümde "KVKK Kapsamı Dışında Bırakılan veya Sınırlandırma Rejimi Öngörülen Haller" başlığı altında tartışıldığı üzere belli makamlar tarafından ve belli amaçlarla toplanan kişisel veriler, KVKK kapsamı dışında bırakılmıştır. KVKK m. 28/1 (ç) hükmü uyarınca kişisel verilerin görev ve yetkili kamu kurum ve kuruluşlarınca önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi halinde KVKK mevzuatı uygulanmayacaktır. Bu

[810] Bu yönde bkz. Benedik/Slovenya, Başvuru no: 62357/14, T. 24.04.2018,Etişim Tarihi: 10.10.2021, para 55 vd.
[811] Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland,19.10. 2016, ECLI:EU:C:2016:779, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582, Erişim Tarihi: 10.10.2021.
[812] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun no:5651, Resmî Gazete Tarih: 23.05.2007, Sayı: 26530,
[813] Bununla birlikte ilgili maddenin, suç işlenmesinin ardından şüphelenilen kişi hakkında bilgi almak üzere kullanılamayacağının altı çizilmelidir. Bu durumda artık genel bilgi toplama değil, CMK m.147 kapsamında ifade alma söz konusu olacak, ilgili hükümde öngörülen usulün izlenmesi gerekecektir.

durumda suç işlenmeden önce verilerin toplanması sırasında KVKK rejimi uygulanmamaktadır. Ancak kolluğun suç işlenmeden önce topladığı verilere ilişkin PVSK ek madde 7 büyük önem taşımaktadır. Bu maddenin yedinci fıkrası uyarınca önleyici alanda toplanan verilerin ceza muhakemesinde kullanılması yasaklanmıştır. Dolayısıyla, profilleme teknolojileri sevk edilirken bu hüküm dikkate alınarak önleyici alanda toplanan kişisel veriler, ceza muhakemesi alanında kullanılmamalıdır. Bu durumda kolluğun önleyici amaçla toplandığı verileri kullanarak profilleme yapması halinde, KVKK hükümleri uygulama alanı bulmasa dahi varılan sonuçların soruşturma veya kovuşturma sırasında kullanılması halinde PVSK ek madde 7 uyarınca hukuka aykırı delil söz konusu olacaktır.

KVKK m. 28/1 uyarınca tamamen kanun kapsamı dışında bırakılan diğer bir istisna hali, (d) bendinde öngörülen kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi halidir. Bu bent, Anayasa m. 9 uyarınca yargı mercii kabul edilen mahkemelerin ve ayrıca infaz kurumlarının topladığı kişisel veriler açısından KVVK hükümlerinin uygulanmayacağını öngörmektedir. Ancak yargılama mercii olmayan kolluk ve cumhuriyet savcılarının adli amaçla kişisel veri toplaması bu fıkra kapsamda öngörülmemiştir. Dolayısıyla savcılık ve kolluk mercileri açısından KVKK m. 28 dikkate alınmalıdır. KVKK m. 28/2 (a) bendi gereğince, suç soruşturması için kişisel verilerin toplanması halinde ilgililerin verilerine ilişkin bilgi talep etme, verilerinin işlenme amacını öğrenme, verilerin silinmesini talep etme ve profillemeye ilişkin haklarını barındıran m. 11 uygulama alanı bulmayacaktır. Ancak bu fıkra kolluk ve savcılığın adli amaçla topladığı verileri tamamen KVKK dışında bırakmamış, yalnızca belli haklara ilişkin sınırlandırmayı mümkün kılmıştır. Bu durumda soruşturma aşamasında kolluk ve savcılık nezdinde toplanan tüm kişisel verilerin, KVKK bünyesindeki diğer hükümler ve temel ilkeler ile uyum göstermesi zorunluluğu devam etmektedir.

Bunun yanı sıra, profillemeye temel olan çoğu verinin internet servis sağlayıcıları, özel şirketler, sağlık kuruluşları gibi soruşturma ve kovuşturmada yetkili olmayan veri sorumluları tarafından toplandığı düşünüldüğünde, bu süreçte kişisel verileri kolluk ve soruşturma makamlarıyla paylaşan diğer kişilerin KVKK hükümlerine uygun davranıp davranmadığı da mutlaka dikkate alınmalıdır.

Profilleme teknolojilerinin kişisel veri işlediği, kolluk ve savcılık tarafından adli amaçlarla işlenen verilerin de KVKK kapsamına girdiğinin tespit edilmesinin ardından, KVKK kapsamında ilgili düzenlemelere uygunluk değerlendirilmelidir. Profilleme teknolojilerinin özellikle KVKK m. 4 ile öngörülen amacın meşruluğu, belirliliği ve amaçla sınırlılık ilkelerine uygun şekilde sevk edilip edilmedikleri tartışmalıdır. KVKK m. 4 gereği veri işleme, belirli, açık ve meşru amaçlara dayanmalı, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü şekilde yapılmalıdır. Belirli, açık ve meşru amaçlar için işlenme ilkesi gereği profilleme teknolojileri henüz sevk edilmeden önce kişisel verilerin ne amaçla işleneceğinin belirli olmalı ve bu amaç, verisi işlenen kişi tarafından anlaşılabilecek şekilde açık olmalıdır. Oysa profilleme teknolojileri, çoğunlukla kişilerden farklı amaçla toplanan verileri değerlendirmektedir. Örneğin vergi kaçakçılığı suçlarını tespit için Hollanda'da kullanılan SyRI profilleme sistemi ile kişilerin iş, eğitim verileri, taşınır ve taşınmaz mallarına dair bilgiler, borç bilgileri farklı veri sorumlularından toplanarak profillenmek üzere kullanılmıştır[814]. SyRI örneği gibi pek çok profilleme sisteminde kişilerin verilerini paylaştığı sırada öngöremedikleri bir amaç için verileri paylaşılmaktadır. Şirketlerin farklı kollardan aldıkları verileri failin tehlikeliliğini tespit etmek üzere kollukla paylaşması amaca uygunluk ilkesine ve dolayısıyla hukuka aykırı olacaktır.

Profilleme sırasında veri işleme, önceden belirlenmiş ve ilgili kişi tarafından öngörülebilir bir amaca dayanmasının yanı sıra veri işlemenin meşru bir zemine sahip olması gerekir. Çoğu durumda profillemek üzere bu verileri işleme, kanunilik, sözleşme ifası için gerekli olma gibi rıza meşru bir zemine dayanmamaktadır. Bunun yanı sıra Ceza Muhakemesi sürecinde profilleme için yalnızca kolluk tarafından adli amaçla toplanan verilerin kullanıldığı ihtimalde, taraflar arasındaki güç dengesizliği nedeniyle rıza meşru sebebine dayanılamayacaktır[815]. Soruşturma mercileri ile kişiler arası bir sözleşme ifası da söz konusu değildir. Hak ve özgürlüklere müdahale içeren bu uygulamaların ceza muhakemesinde kullanılabilmesi ve meşru bir amaçla veri işlendiğinin kabul edilebilmesi için, bu tür bir veri işleme mutlaka kanunla

[814] The Public Interest Litigation Project, "Profiling and SyRi", https://pilpnjcm.nl/en/dossiers/profiling-and-syri/, Erişim Tarihi: 11.10.2021.

[815] Rızaya ilişkin detaylı bilgi için bkz. Kişisel Verileri Koruma Kurumu, Açık Rıza, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf, Erişim Tarihi: 12.10.2021, s.7

öngörülmelidir. Nitekim Anayasa Mahkemesi, incelediği bir kararda Telekomünikasyon Başkanlığı'nın "ilgili işletmecilerden trafik bilgisi temin etme" yetkisini incelemiştir. AYM, bu yetkinin, temin edilecek bilgilerin konu, amaç ve kapsamını açıkça öngören bir kanun ile sınırlanmadığını, bu durumun belirlilik ilkesi ve dolayısıyla kişisel verilerin korunmasını düzenleyen Anayasa'nın 20. maddesini ihlal ettiği sonucuna varmıştır[816]. Dolayısıyla idari ve adli kurumların veri toplama yetkisi, ancak veri toplamanın amaç, neden, kapsam ve sınırlarını açıkça öngören yasal düzenlemelere dayanırsa meşru kabul edilebilir. Profilleme teknolojilerinin ceza muhakemesinde sevk edilmesine ilişkin kanunda bir düzenleme bulunmaması, bu teknolojilerin ceza muhakemesinde kullanılmasını daha en baştan hukuka aykırı kılmaktadır.

Yine m.4 gereğince işlenen veri, amaçla bağlantılı, sınırlı ve ölçülü olmalıdır. Dolayısıyla veriler meşru amaçla toplansa dahi, bu amaçları gerçekleştirilebilmek için gerekli ve zorunlu olmayan kişisel veriler işlenirse bu ilke çiğnenmiş olacaktır. Veri işleme, sadece en başta belirtilen amacın gerçekleştirilmesi için mutlaka gerekli verilerle sınırlı olmalıdır[817]. Bununla birlikte, profilleme teknolojilerine başvuran büyük şirketler, veri toplama amaçlarını çok geniş tutmakta, çok farklı veri gruplarını bu geniş amaçlar çerçevesinde toplamaktadır. Bu bağlamda örneğin ABD'de sıklıkla başvurulan COMPAS algoritması, şiddet içeren suçların işlenme olasılığı olan bölge ve risk gruplarını belirlemek, kişi hakkında verilecek hükme esas alınmak, kişinin tekrar suç işleyip işlemeyeceğini belirlemek, hükümlülerin infaz rejimini tespit etmek gibi suçu önleme, tespit ve infaz gibi fazla amaçlarla veri toplamaktadır[818]. Bu genişlikte ve birbirinden bağımsız nitelikte amaçlarla veri toplamak kuşkusuz ki öncelikle belirli amaç ilkesini ihlal etmektedir. Bunun yanı sıra COMPAS tarafından toplanan kişinin eğitim seviyesi, aile yapısı, iş durumu, okulda başarısı, özel hayatı, boş zamanlarını nasıl geçirdiği[819] gibi verilerin suç işlendiğini ve yeniden işleneceğini

[816]Anayasa Mahkemesi, E. 2014/149, K.2014/151, T.02.10.2014, https://www.resmigazete.gov.tr/eskiler/2015/01/20150101-16.pdf, benzer yönde Anayasa Mahkemesi,E.2006/167, K.2008/86, T. 20.3.2008, https://www.resmigazete.gov.tr/eskiler/2008/06/20080625-8.htm, Erişim Tarihi: 12.01.2021.

[817] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler, Erişim Tarihi: 11.10.2021, s.8-10.

[818] Yong, Ed, "A Popular Algorithm Is No Better at Predicting Crimes Than Random People", 17 Ocak 2018, The Atlantic, https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/, Erişim Tarihi: 11.10.2021.

[819] COMPAS tarafından toplanan veri kalemleri için bkz. Chelioudakis, s. 89.

tespit gibi amaçlar için gerekli ve ölçülü olduğunu kabul etmek mümkün değildir. Dolayısıyla suçu önleme, tespit ve infaz gibi farklı alanlara ilişkin amaçları birleştiren ve kişilerin suç ile ilişkilendirilemeyecek tüm verilerini toplayan bu tür profilleme modellerinin kullanımı kişisel verilerin korunması mevzuatı kapsamındaki amaca uygunluk, asgari veri işleme ilkesi ve ölçülülük ilkelerine aykırıdır.

CMK hükümlerine uygunluk değerlendirildiğinde, konut dokunulmazlığı, seyahat özgürlüğü, kişi güvenliği, özel hayatın gizliliği de dâhil pek çok hakka müdahale içeren koruma tedbirleri çeşitli güvenceler içerecek şekilde PVSK, CMK ve diğer kanunlar çerçevesinde düzenlenmiştir[820]. CMK m.161 ve 164'te yer alan soruşturma ve kovuşturmaya dair genel yetkiler, temel hakları korumak açısından yetersiz olup, bu haklara müdahale içeren tüm tedbirlere ilişkin ayrı ve özel düzenleme yapılması yoluna gidilmiştir[821]. Bununla birlikte günümüzde farklı kaynaklardan beslenen ve kişiler hakkında konut arama, bilgisayarda arama, fizik kimlik tespiti, iletişimin denetlenmesi gibi pek çok farklı tedbir ile erişilebilecek delillerden çok daha fazla bilgi ve veriyi ele veren profilleme teknolojilerinin kullanımına ilişkin herhangi özel bir düzenleme bulunmamaktadır. Kaldı ki koruma tedbirleri kapsamında tartışıldığı üzere, profilleme teknolojileri CMK kapsamında düzenlenen tedbirlerden çok daha farklı amaçlara yönelmekte ve farklı şekilde çalışmaktadır. Profilleme teknolojileri, fiil üzerine ortaya çıkan, olay ve olgularla desteklenen şüpheye dayanmamakta, geleceğe dönük tahmin niteliğindeki umma ve varsayımlardan yola çıkmaktadır. Geçmiş veriler arası bağ kurularak istatistiki genellemelerle gruplar oluşturan profilleme teknolojileri, bu grubun profiline uyan kişileri analiz etmektedir. Dolayısıyla kişilerin suç teşkil eden hareketi ile ilişili bir müdahale söz konusu değildir[822]. Oysa ceza muhakemesinde kişilerin haklarını sınırlayan tedbirler, gözleme dayalı kanıtlardan yola çıkmalı, failin iç dünyası ile değil, fiiline yoğunlaşmalıdır. Ayrıca profilleme teknolojileri hâkim veya gecikmesinde sakınca bulunulan hallerde savcı denetimine tabi tutulmamıştır. Dolayısıyla profilleme teknolojileri ceza muhakemesinde düzenlenen diğer koruma tedbirleri ile uyuşmamakta, bu tedbirlerin etrafından dolanılarak, suç şüphesi, hâkim güvencesi olmadan ve herhangi bir sınıra

[820] Öztürk/Eker Kazancı/ Soyer Güleç, s.29.
[821] Ünver/Hakeri, s.687.
[822] İlgili davalar sırasıyla United States v. Cortez, 449 U.S. 411, 418 (1981), United States v. Momodu, 909 F. Supp. 1571, 1575 (N.D. Ga. 1995) United States v. Sokolow, 490 U.S. 1 (1989), rev'g 831 F.2d 1413 (9th Cir. 1987), aktaran Raymond, s. 107, 108, dipnot 38, 39.

tabii olmaksızın CMK amacı ve sistematiğine aykırı şekilde veri toplanmasına yol açmaktadır.

Dolayısıyla profilleme teknolojileri ile tespit edilen, ancak suçun konusu fiille ilişkisi bulunmayan bilgiler, şüphe tespitinde, temel hak ve özgürlükleri sınırlayan kararların ve hükümlerin verilmesinde dikkate alınmamalıdır[823]. Nitekim ceza muhakemesinde önemli olan şüpheli ile suç teşkil eden hareket arasındaki bağın kurulmasıdır. Bu amaca hizmet etmeyen veriler, yalnızca belli grupların hedef alınarak, neden-sonuç ilişkisi kurmaksızın olasılıklar üzerinden çeşitli suçlarla ilişkilendirildiği[824] ve ceza hukukunun ön yargılara dayanılarak bir silah olarak doğrultulduğu bir düzenin doğmasına yol açacaktır. Bu durum aynı zamanda temel Anayasal ilkelerden m. 10'da ve TCK m.3'te öngörülen kanun ve adalet önünde eşitlik ilkesine aykırılık teşkil edecektir.

Son olarak CMK kapsamında öngörülen ifade usulü ile profilleme arasındaki ilişki üzerinde özellikle durulmalıdır. İfade ve sorgu, soruşturma ve kovuşturmaya yön veren en önemli ceza muhakemesi işlemlerindendir. İnsan hak ve özgürlüklerinin korunması bakımından ifade ve sorgu işlemleri, şüpheliyi yanıltma, korkutma, kötü muameleye maruz bırakma ihtimalleri barındırdığından ayrıca hassasiyet arz etmektedir. Bu nedenlerle Ceza Muhakemesi Kanunu kapsamında ifade alma ve sorgu usulleri CMK m. 147 ve 148 ile çok sıkı kurallara bağlanmış ve bu kuralların ihlal edilmesi durumunda ifade veya sorgunun hukuka aykırı kabul edileceği ayrıca ve açıkça koruma altına alınmıştır. Kanun koyucu, öngördüğü bu usullerle şüpheliden delile gitme yolunu zorlaştırmayı istemiştir[825]. Bununla birlikte doktrinde, ifade ve sorgu usulü ile profilleme arasındaki ilişki üzerinde durulmadığı görülmektedir.

CMK m. 147 gereği kişinin ifadesinin alınabilmesi için, hakkında soruşturma başlatılmış olması, cumhuriyet savcısının bilgisi talimatı gerekir. Şüpheli veya sanık beyanı, ancak neyle suçlandığının kendisine anlatılması, müdafi hakkının bulunduğunun açıklanması ve susma hakkının bulunduğunun belirtilmesinin ardından alınabilir. CMK m.148 şüpheli ve sanığın beyanının özgür iradesine dayanması

---

[823] Ferguson, "Big Data and Predictive Reasonable Suspicion", s. 388.
[824] Ibid, s.403.
[825] Mehmet Arıcan, "Ceza Muhakemesinde İfade Alma ve Sorgu", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:17, Sayı:1, 2009, ss. 43-66.

gerektiğini vurgulamakta, bunu engelleyici kötü davranma, işkence, ilâç verme, yorma, aldatma, cebir veya tehditte bulunma ve diğer bazı araçları kullanmayı yasaklamaktadır. Oysa profilleme teknolojileri kişiler hakkında henüz soruşturma açılmadan, süreç herhangi bir savcı denetimine tabi olmadan ve suç ithamı bildirilmeden veri toplanması ve bu verilerin analiz edilerek adli yaptırımların uygulanmasına yol açmaktadır. Örneğin Google'ın akıllı ev ürünleri olarak tanıttığı Nest araçlarının ev içinde termostat, radyo, televizyon, fırın gibi pek çok farklı eşyalardan topladığı verilerin analiz edilmesi ile kişilerin evi terk edip etmedikleri, eve döndükleri saati, eve kendileri dışında birinin girip girmediği gibi pek çok bilgiye erişilebilmektedir[826]. Bu bilgilerin ceza muhakemesinde kullanılması halinde, CMK m. 147 kapsamında bir soruşturma konusu olduklarını bilmeden, neyle suçlandıkları konusunda aydınlatılmamış kişilerin, kendilerini en güvende hissettikleri ev ortamında istemsiz olarak paylaştıkları verilerin karşılarına çıkartılması söz konusu olacaktır. Bu durumda CMK m. 147 usulü kadar kişilerin susma hakkı ve kendileri aleyhine delil veya beyanda bulunmaya zorlanamayacakları ilkesi de çiğnenmektedir. Yine kişilerin ileride bir soruşturmada kullanılacağını öngörmedikleri özel hayatlarında eğlence, ticaret, turistik amaçlı yaptıkları etkinliklerin, ziyaret ettikleri yerlerin, görüştükleri kişilerin, sosyal medya hesaplarındaki paylaşımların ve internette bıraktıkları izlerin tümünün profilleme kapsamında analiz edilerek, varılan sonuçların ceza muhakemesinde kullanılmasını aldatma ile beyan alma şeklinde yorumlamak mümkündür. Bu bağlamda bir adım ileri gidilerek bu şekilde sevk edilen profilleme teknolojilerinin, CMK m. 148'de yasaklanan usuller kapsamında değerlendirilmesi gerekir. Dolayısıyla geleceğe yönelik risklerden yola çıkarak kişinin geçmiş verilerini işleyen profilleme sonuçlarının şüpheli veya sanık beyanı yerine geçecek şekilde değerlendirilmesi ya da sanık aleyhine delil olarak kullanılması hukuka aykırı kabul edilmelidir.

Sonuç olarak, profilleme teknolojileri değerlendirilirken, bu teknolojilerin daha ilk aşama olan veri toplama aşamasında kişisel verileri koruma mevzuatına uygunlukları ele alınmalıdır. Bu aşamada, verilerin toplanma amacı hukuki zemine dayanmalı, amaca uygunluk, asgari veri işlenmesi, doğru veri işlenmesi ilkelerine

[826] Gokira Dorai/Shiva Houshmand/İbrahim Baggili, "I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out", **ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security**, Ağustos 2018, https://dl.acm.org/doi/10.1145/3230833.3232814, Erişim Tarihi: 20.10.2021.

sirayet edilmelidir. Günümüzde bu ilk aşamada dahi kişisel verileri koruyan hükümlere aykırı şekilde veri toplandığı görülmektedir. Bu aşamadaki hukuka aykırılık, profilleme ile varılan sonuçları da "zehirli ağacın meyvesi" haline getirecektir. Bunun yanı sıra profilleme teknolojilerinin, herhangi bir hukuki zemine dayanmaması, şüphe derecesi ve hâkim denetimi olmaksızın hak ve hürriyetlere müdahale içermeleri, geleneksel koruma tedbiri rejimine aykırılık teşkil etmektedir. Profilleme teknolojilerini kimlik sorma, arama, el koyma, fiziksel kimlik tespiti gibi geleneksel koruma tedbirleri kapsamında ele almak, bu tedbirlere ilişkin hükümleri kıyasen uygulamak mümkün değildir. Nitekim profilleme, farklı amaçlara yönelmiş yeni ve özgün bir araç olup bu tedbirler içerisinde eritilemeyecektir. Dolayısıyla bu teknolojilerin hukuki bir zemini olmaksızın kullanılması ceza muhakemesi ilke ve kurallarına da aykırılık teşkil etmektedir. Hukuka aykırılık, tüm hukuk normlarına, anayasal haklara, uluslararası sözleşmelere ve hukukun evrensel ilkelerine aykırılığı içerir. Profilleme teknolojileri, eşitlik ilkesi ve dolayısıyla ayrımcılık yasağını, masumiyet karinesi ve susma hakkını da ihlal etmekte, dolayısıyla anayasal koruma altında olan, uluslararası insan hakları sözleşmelerinin temelini oluşturan ilkeleri de çiğnemektedir. Tüm bu sebeplerle bu teknolojilerle varılan sonuçları CMK m. 206 kapsamında hukuka uygun delil kabul etmek, yine CMK m. 217 ve m. 289 kapsamında hükme esas almak mümkün değildir.

SONUÇ

Tez kapsamında yapay zekâ teknolojilerinin, profilleme amaçlı sevk edilmesi ile toplum düzenine yönelik "risk" teşkil eden gruplarının tespit edilmesi, ardından bu tespitlerin ceza muhakemesi alanında kullanılması irdelenmiştir. Öncelikle bu teknolojilerin nasıl işlediği ele alınmıştır. Bu tür profilleme teknolojilerini besleyen veriler arasında kişinin yaşı, ailevi durumu, toplumla bağı, iş durumu, eğitimi, ilgili ülkenin vatandaşı olup olmadığı, sabıka kaydı, işlediği suçun ağırlığı, alkol veya uyuşturucu bağımlısı olup olmadığı, ev sahibi olup olmadığı, "iki yıldan uzun ilişki yaşayıp yaşamadığı", akıl sağlığı, okulda "uyumlu" olup olmadığı gibi pek çok veri yer almaktadır[827]. Kimi risk analizi yapan profilleme teknolojileri ise tehlikeli mahalleleri tespit etmek üzere kullanılmakta, bunlar bir bölgede daha önce hangi tip suçların işlendiği, suç işlenme sıklığı, bölgenin ekonomik, sosyal yapısı, mevsim, günün saati, bölgede bar, ATM bulunup bulunmadığı gibi unsurlara dayanmaktadır[828]. Bu teknolojilerin çalışma şeklini ikiye ayırmak mümkündür. Bunların bir bölümü kendilerine sınırsız şekilde sunulan veri üzerinden, suçlu kişilere ait temel özellikleri otomatik ve istatistiksel olarak belirlemekte ve ardından bu özelliklere yakın nitelikler gösteren kişileri "yüksek risk taşıyan kişiler" olarak gruplamaktadır. Bu çalışma modelinde, kendi kendine öğrenen makine öğrenmesi metotları kullanıldığı takdirde, hangi verilerin öncelikli olarak dikkate alındığı, aralarında nasıl bir bağlantı kurulduğu ve sonuca nasıl varıldığını tespit etmek mümkün olmamaktadır. İkinci çalışma şekli, kural temelli olup, bu modelde hangi veri gruplarının kullanılacağı ve sonuca varış için gerekli adımlar sürecin başından belirlenmiş, yazılıma sadece sonuçları optimize etmesi için ufak bir pay bırakılmıştır. Ceza muhakemesinde, bu tür "karar ağacı" şeklinde işleyen, her karara ilişkin kuralın açık olduğu ve dolayısıyla kolaylıkla takip edilebilen modellere[829] başvurulmadığı tespit edilmiştir.

Failin tüm geçmiş izleri, ait olduğu grupları ve yaşam şeklini ortaya koyan verilere dayanan ve "kara kutu" şeklinde işleyen modellerin tercih edildiği profilleme teknolojilerinin ceza muhakemesinde kullanılışı, ceza muhakemesinin amacı ve

[827] Farklı profilleme teknolojileri ve bu teknolojilerde esas alınan veriler için bkz. Hamilton, Risk-Needs Assessment, s. 286-291.
[828] O'Neil, s.85 vd.
[829] Rudin, "Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead".

usulüne yönelik büyük dönüşümün izlerini taşımaktadır. Bu dönüşümü, salt teknolojik bir sıçrayış olarak tanımlamak mümkün değildir. Ceza hukuku toplumda risk yönetiminde araçsallaştırılan bir silah haline gelmiştir. Bu teknolojiler, kişisel verilere hiçbir ceza muhakemesi aracının taşımadığı şiddette müdahaleyi mümkün kılmıştır. Profilleme eliyle aslında kendine ait mülkiyeti bulunmayan, iyi okullara gitme şansı yakalayamamış, avantajsız bir aileye doğmuş, iş bulamamış, belirli mahallelerde ikamet etmiş, sonuç olarak belirli sosyo-ekonomik sınıfa, dolaylı olarak belirli etnik kökene veya göçmen gruplara dâhil kimseler, diğerlerinden ayrıştırılarak, risk olarak değerlendirilmektedir. Yine cinsiyet, yaş, akıl sağlığı gibi kişinin değiştirmesi mümkün olmayan faktörler de bu değerlendirme kapsamında dikkate alınmaktadır. Bu durum, kişinin davranışlarından değil, aksine kontrolünde olmayan, kimi sosyal kimi ise doğuştan gelen niteliklerden ötürü sorumlu tutulması anlamına gelmektedir. Oysa ceza muhakemesi hukuku, failin kişiliği ile değil kusurlu iradesini ortaya koyan fiili ile ilgilenir. Maddi gerçeği açığa çıkarmayı, fiil ile fail arasındaki bağı göstermeyi amaçlar, sonuç olarak fiil ile verilen zararı ödetmeyi, gelecek suçlardan caydırmayı ve uzun vadede faili topluma yeniden kazandırmayı sağlar. Profilleme teknolojileri ise bu sürece ve amaçlara yabancıdır. Sorunlu mahalleleri diğerlerinden daha çok kontrol etmeye, "toplumun kalanından farklı", "antisosyal" kişilerin bizatihi varlıklarından ötürü taşıdıkları riskleri belirlemeye yöneliktir. Nihai amacı fiilden yola çıkan kefaret veya topluma kazandırma değil, risklere karşı toplumu savunmaktır. Bu durum "doğuştan, değiştirilemez" suçlu algısına dayanan pozitivizmin yeniden hortlamasıdır. Nitekim profilleme teknolojileri de kişilerin özgür iradesi olduğunu reddetmekte, belli karakter, milli, sınıfsal, kültürel özellikleri taşıyan kimselerin kaçınılmaz şekilde suç işleyeceği iddiasına dayanmaktadır[830]. Böylelikle otomatik şekilde tayin edilen gruplar üzerinden kolektif ve kusursuz bir sorumluluk doğmakta, tehlike kavramından da soyut bir risk, henüz gerçekleşmeden, cezai sonuçları bugünden doğmaktadır. Bu nedenle profilleme teknolojileri, geçmişte işlenmiş bir suçu aydınlatan ve insan onuruna saygıyı merkezine alarak maddi gerçeği arayan ceza muhakemesi ilkeleri ile kaçınılmaz şekilde farklılaşmaktadır.

Ceza muhakemesinin temel ilkeleri ve usulü ile tezat oluşturan bu tespitlerin yapılmasının ardından, tez kapsamında ele alınan sorulardan ilki, profilleme teknolojilerine ilişkin ilk düzenleme girişimi olan kişisel verileri koruma normlarının,

[830] Erman, "Ceza Hukukunun Dönüşümü", s. 459.

ceza muhakemesi sürecinde kullanılıp kullanılamayacağı ve bunların yeterli bir koruma teşkil edip etmediğidir. Bu bağlamda profillemenin çoğunlukla özel kişiler tarafından toplanan verilerin işlendiği veya bu verilere erişildiği ilk aşamada, AB kapsamında GDPR, Türkiye'de ise KVKK hükümleri mutlaka dikkate alınmalıdır. Ancak kolluğun veya adli mercilerin, ceza muhakemesi sırasında adli amaçla veri işlediği durumlarda, AB kapsamında 2016/680 sayılı Direktif geçerli olacak ve Türkiye özelinde KVKK m. 28'deki sınırlandırmalar devreye girecektir. KVKK m.28 ile yargılama ve infaz makamlarının veri işlemesini Kanun kapsamı bırakıldığı görülmektedir. Bununla birlikte, yargılama makamı olmayan kolluğun ve savcılığın adli amaçlı veri işlemesi sırasında KVKK hükümlerine uyulmasının zorunlu tutulduğu, yalnızca m. 28/2'de öngörülen belirli hakların sınırlanabileceğine dikkat çekilmelidir. İlgili mevzuatlar incelendiğinde, pek çok ülkede ceza muhakemesinde sevk edilen profilleme teknolojilerinin, bu mevzuatlarda yer alan meşru, belirli amaca dayanma ve bu amaçlar için gerekli ölçüde veri işlenmesi ilkesine aykırı şekilde veri işlendiği tespit edilmiştir. Nitekim ilkin ticari, eğitim amaçlı, sağlığa ilişkin veya diğer amaçlarla işlenen pek çok veri, ardından profilleme sonucu suçu önleme veya tespit amacıyla kullanılmaktadır. Kişilerin özel ve ailevi yaşantısına, ekonomik durumuna, arkadaş çevresi ve psikolojik durumuna dair pek çok veri grubunun toplum düzenine yönelik tehlikeliliği tespit için elverişli ve gerekli olduğunu, dolayısıyla asgari veri toplama ilkesi ve ölçülülük ilkesine riayet ettiğini söylemek mümkün değildir.

Genel ilkelerin yanı sıra tez kapsamında GDPR m. 22 ve Direktif m. 11 kapsamında kişi aleyhine hukuki veya benzer biçimde ciddi sonuçlar doğuran kararların salt otomatik işleme faaliyetine dayalı şekilde alınamayacağını düzenleyen hükümler ele alınmıştır. Bu hükümlerin muadili KVKK kapsamında m. 11/1 (g)'dir. Pek çok ülkede kolluk görevlileri tarafından sadece profilleme teknolojilerinin gösterdiği risk derecesine göre otomatik olarak durdurma veya yakalama işlemi yapılmaktadır. Bunun yanı sıra, profilleme teknolojilerinin çalışma modelinin hâkim ile paylaşılmadığı veya teknik sebeplerle açıklanamadığı hallerde, otomatik süreçte insan müdahalesi ve kontrolü söz konusu olmayacaktır. Bu nedenle ilgili hükümler, profilleme modellerinin çalışma şeklinin açıklanabilir olmasını, yargı mercileri ile paylaşılmasını ve gerçek bir değerlendirmeden geçmesini gerektirdikleri için önemlidir[831]. Bunun yanı sıra AB mevzuatında profilleme sürecinde ilgili kişinin

[831] Häuselmann, s.14.

görüşünü ifade etme ve karara karşı çıkma yönündeki hakları (GDPR m.22/3), yine hakkında otomatik bir karar verildiğini öğrenme, başvurulan otomatik sistemin işleme mantığını, sürecin önemi ve öngörülen sonuçları hakkında "anlamlı" bilgiler edinme hakları (GDPR m.13/2 (f), 14/2 (g), 15/1 (h)) bulunmaktadır. Dolayısıyla öngörülen otomatik risk puanı nedeniyle ceza muhakemesinde bir tedbir veya yaptırıma maruz kalan kişi, hakkında nasıl bu karara varıldığını teknik değil, ortalama kişinin anlayabileceği şekilde öğrenebilmelidir. Nitekim kullanılan profilleme teknolojisinin tüm detaylarıyla teknik şekilde açıklanması, kişinin süreci kavraması ve itiraz edebilmesini engelleyecek, ayrıca yazılıma ilişkin ticari sır, fikri mülkiyet haklarının ileri sürülmesine yol açacaktır. Bununla birlikte GDPR kapsamında ayrıntılarıyla öngörülen bu şeffaflık hakları gerek Kolluk Direktifi gerekse KVKK kapsamında açıkça öngörülmemiştir. Aksine, adli amaçlı veri işlenirken, bu hakları soruşturmanın amacını tehlikeye düşürmemek gibi gerekçelerle sınırlamak mümkündür. Ancak adli amaçla veri işleme sırasında yapılan sınırlandırmalar ve bunlara ilişkin güvenceler AB Kolluk Direktifi bünyesinde detaylı şekilde ele alınmış ve bu sınırlandırmalara karşı kişiye özel başvuru yolları öngörülmüştür. Kişi, örneğin soruşturmanın amacına ulaşabilmesi için sınırlandırmaların nedenini öğrenemediyse, Kişisel Verileri Koruma Kurullarına başvurabilecektir. Böylece kolluk ve savcı tarafından alınan kararlar, şüpheli ile paylaşılmasa dahi başka bir merci tarafından incelenebilmektedir. Oysa Türkiye'de KVKK bünyesinde Direktif'in içerdiği düzenlemelere benzer hükümler öngörülmemiştir. Adli amaçla kişisel veri işlenmesine ilişkin kural ve güvenceler, acilen 2016/680 sayılı Direktif örnek alınarak ayrı bir kişisel verilerin korunması mevzuatı ile öngörülmelidir. Bununla birlikte, mevcut düzenlemeler ışığında dahi, adli amaçla profilleme teknolojileri sevk edilirken, kişisel verilere ilişkin hakların tamamen askıya alınması mümkün değildir. Demokratik toplumda gereklilik ve ölçülülük uyarınca, örneğin soruşturmanın amacını tehlikeye sokan durumun ortadan kalkması ile kişilerin salt otomatik sistemler vasıtasıyla aleyhine analiz yapılmasına itiraz etme, bilgi edinme ve verilerine erişebilme gibi haklarını derhal kullanabilmesi gerekir.

Kişisel Verileri Koruma mevzuatları hem Avrupa hem Türkiye'de profillemeye karşı önemli güvenceler öngörmektedir. Dolayısıyla tezin yoğunlaştığı ilk sorunun cevabı, kişisel verileri koruma mevzuatında öngörülen bu hakların, ceza muhakemesinde profilleme teknolojileri ile veri işlenmesi sırasında

kullanılabileceğidir. Bununla birlikte, ilgili kanunlarda bireysel olarak öngörülen haklar, kişiyi etkileyen sonuçlar doğduğunda devreye girmekte ve bireysel sonuçları ortadan kaldırmayı mümkün kılmaktadır. Ancak profilleme teknolojilerinin ceza muhakemesinde kullanımı için, genel geçer düzenleyici işlemlerle, yani kanunla, bu teknolojilerin amaç ve sınırlarının çizilmesi gerekir. Bu düzenlemeler yapılmadan önce, tez kapsamında profilleme teknolojilerinin ceza muhakemesindeki hukuki niteliği tespit edilmeye çalışılmıştır. Bu bağlamda, bu teknolojilerin koruma tedbiri mi yoksa güvenlik tedbiri mi olduğu ve vardıkları sonuçların delil niteliği masaya yatırılmıştır.

Öncelikle risk analizi yapan profilleme uygulamalarının bir koruma tedbiri sayılıp sayılamayacağı ele alınmıştır. Koruma tedbirlerinin amacı, ceza muhakemesinin ilerlemesini sağlamak ve muhakeme sonucu verilen kararın uygulanabilmesini mümkün kılmaktır. Bu nedenle koruma tedbirleri, delillere ulaşılmasını, delillerin güvence altına alınmasını ve failin kaçmasına engel olunmasını sağlar. Profilleme teknolojileri ise suç teşkil eden fiil ile fail arası bağ kuran delilleri tespit etmeye yönelik sevk edilmemektedir. Nihai amaçları ilgili davanın görülmesi ve suça ilişkin maddi gerçeğin ortaya çıkması değil, risk teşkil eden, yeniden suç işlemesi mümkün görülen kişilerin belirlenmesi ve toplumdan uzaklaştırılmasıdır. Koruma tedbirleri ancak gecikmesinde sakınca bulunulan hallerde uygulanır. Profilleme teknolojileri ise çoğunlukla acil, somut bir tehlike doğmadan, uzun vadeli, soyut bir riski engellemek için kullanılırlar. Koruma tedbirlerinin maddi gerçeğe ulaşılmak için sadece bir araçtır ki bu unsur aynı zamanda tedbirlerin geçici olarak uygulanmalarını gerektirir. Geçicilik, aynı zamanda koruma tedbirlerini kalıcı yaptırımlardan ayırmaktadır[832]. Oysa profilleme teknolojileri yapılan yargılamada araç olma ve geçici olma unsurlarını taşımamaktadır. Bu teknolojilerin yaptıkları gruplamalar ve verdikleri risk puanları, kişiler hakkında neredeyse ömür boyu damgalanma etkisi doğurmaktadır. Kimi zaman bu sonuçlar, bir kişi cezasını infaz ettikten sonra da devam etmekte, bankalar, sigorta şirketleri, özel kurumlar, işverenlerle paylaşılan bu puanlar kişinin sürekli karşısına çıkarak toplumdan tecritine yol açmaktadır. Profilleme teknolojilerinin en vahim etkilerinden biri, delilden faile ulaşmayı sağlayan ve ceza muhakemesinde pek çok tedbirin keyfi şekilde uygulanmasını engelleyen şüphe kavramı üzerindeki dönüştürücü etkileridir. Koruma tedbirleri, genellikle tarafsız bir

[832] Özbek/Doğan/Bacaksız, s.223, Yenisey/Nuhoğlu, s. 324.

gözlemciyi, ilgili kimsenin bir suç işlediği konusunda ikna edecek, objektif nitelikte, somut olay ve olgulardan çıkan şüpheye dayanır. Fiilden yola çıkan bu olgu ve delillerin, ilgili tedbir uygulanmadan önce elde edilmesi gerekir. Profilleme teknolojileri ise henüz bir şüphe doğmadan, hatta suç yoluna girmeden kişilere adeta sorgu ışığı tutmaktadır[833]. Failin kişisel özelliklerinden yola çıkan risk kavramı, fiilden yola çıkan objektif gözlemlere dayalı şüphe kavramını aşındırmaktadır[834]. Tüm bu nedenlerle profilleme teknolojileri, koruma tedbirlerinin amaç, sonuç ve unsurlarıyla uyuşmamakta, sui generis bir nitelik göstermektedir.

Risk analizi yapan bu uygulamaların, pozitivist ekolün ceza hukukuna mirası olan güvenlik tedbirleri ile benzeştiği düşünülebilir. Nitekim güvenlik tedbirleri de failin tehlikeliliğine dayanır, gelecekte yeniden suç işlenmesi ihtimaline karşı toplumu koruma amacı güder. Bununla birlikte TCK m. 3, suç işleyen kişi hakkında işlenen fiilin ağırlığı ile orantılı şekilde güvenlik tedbirine hükmolunacağının altını çizmektedir[835]. Dolayısıyla güvenlik tedbiri açısından failin tehlikeliliği önem arz etse de bu tehlikelilik yalnız kişinin sosyal özellikleri, geçmişi, aile yapısı ve eğitim düzeyi ile değil evleviyetle suç teşkil eden bir fiiliyle dışa vurulmuş olmalıdır. Hangi fiiller için güvenlik tedbiri uygulanabileceği ise elbette kanunda açıkça öngörülmelidir. Profilleme teknolojileri ise bu unsurların hiçbirini karşılamamaktadır. Bu teknolojiler çoğunlukla suç tespit edilmeden önce, hatta bazen kişinin suç teşkil eden hiçbir hareketi bulunmasa dahi uygulanmaktadır. Dolayısıyla çoğu halde kişinin tehlikeliliği bir fiil ile vücut bulmuş ve bu fiil mahkeme kararıyla tespit edilmiş değildir. Yine hangi unsurların hangi oranda kişilerin tehlikeli bulunmasına yol açtığı açık ve öngörülebilir şekilde düzenlenmemiştir. Güvenlik tedbirleri toplumu korumak amacı içerisinde, aynı zamanda faili topluma kazandırmaya çalışır, bu nedenle failin ve fiilin niteliklerine göre, bireyselleştirilmiş tedbirler uygulanır. Oysa profilleme teknolojileri kişinin uyuşturucu bağımlılığı, akıl sağlığı, suça eğilimi gibi pek çok farklı faktörü bir arada değerlendirmektedir. Bu durum profillenen grupla benzer özellik gösterdiği iddia edilen tüm kişilere tek tip muamele gösterilmesi anlamına gelmektedir. Bu nedenle profilleme teknolojileri, güvenlik tedbirlerinin amaç, unsul ve sonuçlarından ayrışmaktadır.

---

[833] Ferguson, "Big Data and Predictive Reasonable Suspicion", s.329.
[834] Ibid, s.330
[835] Artuk/Yılmaz, s.29.

Son olarak profilleme ile ulaşılan sonuçların delil niteliği üzerinde durulmalıdır. Tez kapsamında değerlendirilen yabancı içtihatlarda, mahkemelerin kimi zaman profilleme teknolojilerini hukuka aykırı kabul ettikleri, kimi zaman ise hükme esas aldıkları görülmektedir. Ancak bunların bir belge delili mi, belirti delili mi yoksa bilirkişi görüşü olarak mı ele alınması gerektiği vurgulanmamış, yine bu sonuçların hukuka uygun delil olup olmadığı detaylı şekilde değerlendirilmemiştir. Öncelikle profilleme sonuçlarının delil olarak değerlendirilebilmesi için akılcı olma, sağlam olma, davaya konu olayın bütününü ya da bir parçasını temsil etme, müşterek (kolektif) olma ve hukuka uygun elde edilmiş olması unsurlarını karşılaması gerekir. Tez kapsamında yapılan değerlendirmede, profilleme teknolojilerinin henüz bilimsel ve sağlam kabul edilmesi için gerekli kıstasları karşılayacak nitelikte olmadıkları belirlenmiştir. Bunun yanı sıra dava konusu fiil ile ilişkili olmamaları, delil için aranan "somut olayı temsil etme" niteliğini taşımadıklarını göstermektedir. Son olarak profilleme modelleri, görülen davalarda çoğu durumda hâkimlerle dahi paylaşılmamıştır. Elbette bu durum, duruşma sırasında savunma ve iddianın da katıldığı, kolektif bir tartışmayı imkânsız kılmış, bu nedenle delillerde bulunması gereken müştereklik unsurunun da karşılanmadığı tespit edilmiştir. Özel olarak profilleme teknolojileri tanık beyanları ile karşılaştırılmış, somut olaya ilişkin beş duyuları ile edindikleri bilgileri aktaran tanıklardan farklı oldukları, daha ziyade kişilik tanıkları ile benzeştikleri görülmüştür. Ancak CMK sisteminde sanığın kişiliği, ahlaki değerleri, yaşam tarzına ilişkin sübjektif kanaat içeren bu tür bir tanıklık, maddi olayın ispatında kullanılamayacaktır[836]. Bilirkişi görüşü açısından, ulusal ve uluslararası standartlar ve içtihatlar ışığında, bilirkişinin tarafsızlığı ve alanında uzman olmasının yanı sıra, sunduğu görüşte hangi bilimsel metodu uyguladığının, bu metodun ilgili alanda genel kabul gören, sınanmış ve sonuçları test edilmiş bir metot olup olmadığının da dikkate alınması gerektiği açıklanmıştır. Başvurulan görüşün bilimselliği kadar, olay ile ilgisi ve olaya doğru şekilde uygulanıp uygulanmadığı da mutlaka değerlendirilmelidir. Bu bağlamda, algoritmalar tarafından belirlenen risk grupları ve sanığın bu gruplarla ilişkilendirilerek tehlikeli kişi olduğu sonucu, olasılıklara dayalı, spekülatif niteliktedir. Profilleme teknolojilerinde uygulanan modeller, istatistiksel çıkarımlar yapılmakta, ancak bu modellerin bilim insanlarının çoğunluğu tarafından kabul görmüş teorilere dayandıkları söylemek mümkün değildir.

[836] Birtek, s. 156, 157.

Yalnızca tahmine dayalı suçlu profilleme, sanığa karşı önyargı yaratmakta ve sanık hakkında verilecek hükmü yönlendirmektedir. Bu teknolojiler, ceza yargılamasını, maddi gerçeği açığa çıkarma amacından saptırarak, bir kişinin "kötü bir karaktere sahip olduğunu" kanıtlamaya yöneltmektedir. Oysa bir kişinin uyumsuz, asosyal, tehlikeli olması ile onun ilgili suçun faili olması arasında büyük fark vardır[837]. Dolayısıyla profilleme teknolojilerinin vardığı risk puanlarının bilimselliği kadar, maddi olayı aydınlatmaya elverişliliği de tartışmalıdır. Bu nedenle bunların muhakemenin işleyişine teknik ve güvenilir yardım sunan bilirkişi görüşü olarak kabul edilmeleri mümkün değildir.

Görüldüğü üzere tez kapsamında ikincil olarak irdelenen soru açısından, profilleme teknolojilerine karşı, hem kişisel verilerin korunması kanunu hem de ceza muhakemesindeki mevcut düzenlemeler birlikte değerlendirildiğinde bunların yeterli koruma sağlamadığı yanıtı verilmiştir. Nitekim ceza muhakemesi ilkeleri ve düzenlemeleri, bu teknolojiler ile tamamen farklı amaç ve usuller çerçevesinde inşa edilmiştir. Bunun yanı sıra profilleme teknolojileri ile varılan sonuçların delil ve delil araçlarının barındırması gereken nitelikleri içermediği tespit edilmiştir.

Son olarak bunların ceza muhakemesi dışında bırakılması için en önemli değerlendirme olan hukuka uygunlukları incelenmelidir. Bu inceleme kişisel verileri koruma mevzuatını ceza muhakemesine dâhil eden diğer bir kesişim noktasını oluşturur. Nitekim hukuk düzeni bir bütün olduğundan, ceza hâkimleri, profilleme sürecinin hukuka uygunluğunu incelerken, veri işleme sürecinde KVKK hükümlerine uygunluğu da dikkate almak zorundadır. Bu bağlamda, daha önce de belirtildiği üzere profilleme teknolojilerinin, farklı amaçlarla toplanan verileri işlemesi, analiz metotlarının şeffaf bir şekilde paylaşılmaması, bunun yanı sıra esasa ilişkin gerçek bir denetimden geçirilmeyerek aslında salt otomatik yollarla karar almaları, kişisel veriler mevzuatına aykırılık teşkil edecektir. KVKK düzenlemelerine ek olarak, ayrıca PVSK ek m. 7 gereği, önleyici amaçla toplanan verilerin adli amaçla kullanılması mümkün değildir. Tüm bu nedenlerle, ceza muhakemesinde sevk edilen pek çok profilleme teknolojisi ve bunların vardıkları sonuçların CMK m. 206/2 (a), 217/2 ve 289/1 (i)'de yer alan açık düzenlemeler karşısında hukuka aykırı delil teşkil ettiği ve hükme esas alınamayacağını belirtilmelidir.

[837] Munday, Evidence, s. 255.

Tez kapsamında yapılan bu değerlendirmeler, profilleme teknolojilerinin ceza muhakemesinde kullanımına dair ayrı bir düzenlemeye ihtiyaç duyulduğunu göstermektedir. Karşılaştırmalı hukukta incelenen örneklerde, profillemeye ilişkin ceza muhakemesi veya kolluk mevzuatında ayrıca bir düzenlemeye yer verilmediği görülmektedir. Bununla birlikte profillemeye benzeyen, ancak temel hak ve özgürlüklere çok daha az müdahale içeren veri tabanlarında arama ve eşleştirme yapma, yani "veri madenciliği" tedbirine ilişkin çeşitli hükümler Almanya ve Avusturya'da öngörülmüştür. Yalnızca Fransa'da, bir kişinin "davranışının değerlendirilmesini" içeren hiçbir mahkeme kararının, otomatik şekilde kişisel veri işlenmesine dayandırılamayacağı belirtilmiştir. Türkiye'de bu hususta herhangi açık bir düzenleme bulunmamaktadır. Risk analizi yapan profilleme teknolojilerinin, ceza muhakemesi ile örtüşmeyen yapısı karşısında, profilleme teknolojilerini bir tedbir olarak CMK sistemi ile bütünleştirmek mümkün gözükmemektedir. Dolayısıyla bu teknolojilerin ne şekilde uygulanabileceğini öngören bir düzenleme yerine, bunların ceza muhakemesinde kullanımını yasaklayan bir düzenleme yapılması gereklidir. Ancak bu düzenlemenin Fransa'daki düzenlemeden farklı olarak, yalnız davranış değerlendirmesini yasaklayan bir ifade ile değil daha genel bir ifade ile yapılması farklı yorumların önünü kapatacaktır. Bu bağlamda yeknesak bir uygulama için aşağıdaki içerikte bir düzenleme yol gösterici olacaktır:

"Kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişi hakkında varılan sonuçlar, suç ithamı ve ispatında kullanılamaz."

CMK sistematiğinde, hukuka aykırı kabul edilen ve hükme esas alınamayacak tüm uygulamalar kazuistik şekilde sayılmamıştır. Bu sistematiğe riayet etmek adına, yukarıda önerilen yasak hükmüne kişisel verileri koruma mevzuatında yer verilmesi daha yerinde olacaktır. Bu nedenle hızlı ve ara bir çözüm üretmek adına, KVKK bünyesine bu tür bir düzenleme eklenmesi mümkündür. Ancak mevcut KVKK sistematiğinde de profillemeye ilişkin detaylı düzenlemelere veya genel olarak yargılama aşamasına ilişkin yasaklama maddelerine yer verilmediği görülmektedir. Özellikle kolluk ve adli mercilerin faaliyetlerine ilişkin veri işleme süreci, KVKK kapsamında en suskun kalınan alanlardan biridir. Bu nedenle, öncelikle AB bünyesinde yer alan ve tez kapsamında oldukça detaylı irdelenen 2016/680 Direktif

örnek alınarak, kolluk ve adli mercilerin yürüttükleri suçu önleme, tespit ve infaz sürecinde veri işlenmesini düzenleyen detaylı bir kanuna ihtiyaç duyulmaktadır. Profillemeye ilişkin önerilen madde açısından sistematik olarak en uygun mevzuat ceza muhakemesinde veri işlemesini düzenleyen, yeni bir kişisel verilerin korunması kanunu olacaktır.

KAYNAKÇA

Akçalı Gür, Berna, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:25, Sayı:2, Prof. Dr. Ferit Hakan Baykal Armağanı, Aralık 2019, ss. 850-872

Akpek, Ayça Lütfiye, **Tutuklulukta Kuvvetli Suç Şüphesi**, İstanbul Bilgi Üniversitesi, Yüksek Lisans Tezi, İstanbul 2020

Aksoy Retornaz, Eylem, "Beccaria'nın Hapis Cezasına Bakışı Üzerine Bir Değerlendirme", **Türkiye Barolar Birliği Dergisi**, Cilt:112, 2014, ss.93-106

Aksoy Retornaz, Eylem/Güçlütürk, Osman Gazi, "Yapay Zekânın Kişisel Veri Kavramı ve Kişisel Verilerin İşlenmesinde Temel İlkelerle İlişkisi", İçinde**: Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ**, Ed: Aksoy Retornaz, Eylem/Güçlütürk, Osman Gazi, On İki Levha Yayınevi: İstanbul, 2021, ss.275-302

Aksoy, Şemsettin, **Önleme ve Koruma Tedbiri Olarak Arama**, İstanbul Üniversitesi Kamu Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul 2006

Akyürek, Güçlü, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", **Türkiye Barolar Birliği Dergisi**, Sayı:102, ss.61-82, 2012

Akyürek, Güçlü, **Özel Hayatın Gizliliğini İhlal Suçu**, Seçkin Yayıncılık: Ankara, Ocak 2014

Aletras, Nikolaos/Tsarapatsanis, Dimitrios/Preoţiuc-Pietro, Daniel/Lampos, Vasileios, "Predicting Judicial Decisions of the European Court of Human Rights: a Natural Language Processing Perspective", **PeerJ Computer Science**, 2016, https://doi.org/10.7717/peerj-cs.93

Alkan, Nurettin/ Karamanoğlu, Yunus Emre, "Öngörüye Dayalı Kolluk Temelinde Önleyici Kolluk: Rusya Federasyonu'ndan Örnekler", **Güvenlik Bilimleri Dergisi**, Kasım 2020, Cilt:9, Sayı:2, ss. 388-412

Alpsoy, Zeliha, **Önleme Araması**, Adalet Yayınevi: Ankara, Kasım 2019

Arıcan, Mehmet, "Ceza Muhakemesinde İfade Alma ve Sorgu", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:17, Sayı:1, 2009, ss. 43-66.

Arslan Cansever, Belgin, "Bilgi Toplumunda Bir Kavram Kargaşası: Bilgi mi? Enformasyon mu?", **Sosyoloji Dergisi Armağan Sayısı**, 2017, ss. 41-50

Arslan, Çetin, "Dijital Delil ve İletişimin Denetlenmesi", **Ceza Hukuku ve Kriminoloji Dergisi**, Cilt: 3, Sayı: 2, ss. 253-266

Arslan, Kahan Onur, "İnsan Onuru Kavramı ve Koruma Tedbirleri Bağlamında Temel Bir İlke Olarak İnsan Onurunun Korunması", **Türkiye Barolar Birliği Dergisi**, Eylül Ekim 2015, Sayı:120, ss.155-172

Artuk, Mehmet Emin, "Güvenlik Tedbirleri", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:12, Sayı:1-2, 2008, ss.461-492

Artuk, Mehmet Emin/ Yılmaz, Erkam, "Teorik Açıdan Güvenlik Tedbirleri", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:2, Güz 2020, ss.7-43

Ashworth, Andrew/Zedner, Lucia, **Preventive Justice**, Oxford University Press: Oxford, Nisan 2015

Aşıkoğlu, Şehriban İpek, "Veri Sorumlularının Aydınlatma Yükümlülüğü", **Kişisel Verileri Koruma Dergisi**, Cilt:1, Sayı: 2, 2019, ss. 41-65

Atakan, Arda, "Kamu Düzeni Kavramı", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:13, Sayı:1-2, 2007, ss. 59-166

Atalay, Muhammet, "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt: 9, Sayı: 22, 2017, s.155-172

Atlı, Turan, "Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 2, Sayı: 1, 2019, ss.4-22

Aydın, Devrim, **Ceza Muhakemesinde Deliller**, Yetkin Yayınevi: Ankara, 2014

Aydın, Fatih, **Suçlu Profilleme**, Adalet Yayınevi: Ankara, Mayıs 2011

Ayyüce Kızrak, Merve/Bolat, Bülent, "Derin Öğrenme ile Kalabalık Analizi Üzerine Detaylı Bir Araştırma", **Bilişim Teknolojileri Dergisi**, Cilt: 11, Sayı: 3, Temmuz 2018, ss.263-286

Ballestrem, Johannes Graf/Bär, Ulrike/Gausling, Tina/Hack, Sebastian/ von Oelffen, Sabine, **Künstliche Intelligenz Rechtsgrundlagen und Strategien in der Praxis**, Springer Gabler Yayınları, 2020, https://doi.org/10.1007/978-3-658-30506-2

Başlar, Yusuf, **Ceza Yargılamasında Elektronik Delil**, Sakarya Üniversitesi Siyaset ve Kamu Yönetimi Anabilim Dalı, Doktora Tezi, Sakarya, Mayıs, 2015

Battelle, John, **How Google and its Rivals Rewrote the Rules of Businesses and Transformed Our Culture**, Nicholas Brealey Publishing: London, 2005

Bayraktar, Çiler Damla, "Ceza Muhakemesi Hukukunda Bir Koruma Tedbiri Olarak Otomatik Veri Taraması (Rasterfahndung): İnsan Hakları Bağlamında Bir Analiz", **Ceza Hukuku Dergisi**, Cilt: 13, Sayı:38, Aralık 2018, ss. 25-64

Berk, Richard, **Machine Learning Risk Assessments in Criminal Justice Settings**, Springer Nature Yayınevi, https://doi.org/10.1007/978-3-030-02272-3, 2019

Bernstein, David E., "Frye, Frye, Again: The Past, Present, and Future of the General Acceptance Test", **Jurimetrics**, Cilt:41, Sayı: 3, Bahar 2001, ss. 385-408

Birtek, Fatih, **Avrupa İnsan Hakları Mahkemesi, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat**, Adalet Yayınevi: Ankara, Kasım 2017

Boden, Margaret A, **AI: Its Nature and Future**, Oxford: Oxford University Press, Temmuz 2016

Borgesius, Frederik Zuiderveen, "The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition", **European Data Protection Law Review**, Cilt:3, Sayı:1, 2017, ss. 130-137

Bosco, Francesca/Creemers, Niklas/Ferraris, Valeria/ Guagnin, Daniel/ Koops, Bert-Jaap, "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities", İçinde **Reforming European Data Protection Law**, Ed. Gutwirth, Serge/Leenes, Ronald/de Hert, Paul, Springer Science: Dordrecht, 2015, s.3-33

Böhm, Maria Laura, "Endanger Law: War on Risks in German Criminal Law", İçinde **The Law in the Information and Risk Society**, Ed: Duttge, Gunnar/Lee, Sang Won, Universitätsverlag Göttingen, 2011, ss.145-164.

Börekçi, Eşref Barış,"Yeni Düzenlemeler Işığında Önleme Aramaları", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 17, Özel Sayı, 2020, ss.89-113

Bratus, Sergey/Lembree, Ashlyn/Shubina, Anna, "Software on the Witness Stand: What Should It Take for Us to Trust It?" İçinde: **Trust and Trustworthy Computing**, Ed. Acquisti, Alessandro/Smith, Sean W/Sadeghi, Ahmad Reza, Springer: Berlin, 2010, ss.396-416

Breyer, Jonas, "Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-GVO", **Datenschutz und Datensicherheit**, Cilt:42, Sayı:5, 2018, ss.311-317

Brinkhoff, Sven, "Big Data Data Mining by the Dutch Police: Criteria for a Future Method of Investigation", **European Journal for Security Research**, Cilt:2, 2017, ss. 57–69

Brkan, Maja, "Do Algorithms Rule the World? Algorithmic Decision-making in the Framework of the GDPR and Beyond", **International Journal of Law and Information Technology**, Cilt:27, Sayı:2, 2019, ss.91-121

Broussard, Meredith, **Artificial Unintelligence: How Computers Misunderstand the World**, MIT Press: Cambridge, Mayıs 2018

Buğdaycı, Ali Can, **Önleyici Kolluk Faaliyeti Esnasında Elde Edilen Bilgiler ve Bunların Ceza Muhakemesindeki Delil Değeri**, Ankara Yıldırım Beyazıt Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Ankara, Nisan 2019

Busch, Andreas/Breindl, Yana/Jakobi, Tobias, **Netzpolitik: Ein einführender Überblick**, Springer: Weisbaden, 2019

Butterworth, Michael, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework", **Computer, Law and Security Review**, Cilt: 34, 2018, ss. 257–268

Buxmann, Peter/Schmidt Holger, **Künstliche Intelligenz mit Algorithmen zum Wirtschaftlichen Erfolg**, Springer Yayınları, 2019, https://doi.org/10.1007/978-3-662-57568-0.

Carlson, Greta/ McKinney, Jonathan/Slezak Elizabeth/Wilmot, Esther, "General Data Protection Regulation and California Consumer Privacy Act: Background", **Journal of International Economic Law**, Cilt:24, Sayı: 1, 2020, ss. 62-69

Cartuyvels Yves, "Profilage et Datamining dans le Monde de la Pénalité: Vers Une Sortie Du Droit?",https://dial.uclouvain.be/pr/boreal/object/boreal%3A203248/datastream/PDF_01/view ErişimTarihi:29.06.2021

Casey, Eoghan, **Digital Evidence and Computer Crime**, Elsevier Yayınevi: Waltham, 2011

Castelvecchi, David, "Can We Open the Black Box of AI?", **Nature Journal**, Cilt: 538, Ekim 2016, s.20-23

Centel, Nur, "İnsan Hakları Avrupa Mahkemesi Kararları Işığında Tutuklama Hukukuna Eleştirel Yaklaşım", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:17, Sayı:1-2, s.49-93

Chelioudakis, Eleftherios, "Risk Assessment Tools in Criminal Justice: Is There a Need for Such Tools in Europe and Would Their Use Comply with European Data Protection Law?", **Australian National University Journal of Law and Technology**, Cilt: 2, Sayı:1, Eylül 2020, ss.72-96

Cihan, Erol/Yenisey, Feridun, **Ceza Muhakemesi Hukuku**, Beta Yayınevi: İstanbul, 1998

Coeckelbergh, Mark**, AI Ethics**, The MIT Press: Cambridge, Nisan 2020

Daragenli, Vesile Sonay, **Tehlike Suçları**, İstanbul Üniversitesi Kamu Hukuku Bölümü, Yüksek Lisans Tezi, 1998

De Hert, Paul De Hert/Papakonstantinou, Vagelis, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals", **Computer Law and Security Review**, Cilt:28, Sayı: 2, Nisan 2012, ss. 130-142

De Hert, Paul/ Gurtwith, Serge, "Privacy, Data Protection and Law Enforcement: Opacity of the individual and Transparency of Power", İçinde: **Privacy and Criminal Law**, Ed. Claes, Erik/Duff, Antony/Gutwirth, Intersentia: Antwerpen, 2007, ss.61-104

De Vries, Katja,"Identity, Profiling Algorithms and a World of Ambient Intelligence", **Ethics and Information Technology**, 2010, Cilt:12, Ocak 2010, ss.71–85

Deeks, Ashley, "The Judicial Demand for Explainable Artificial Intelligence", **Columbia Law Review**, Cilt:19, Sayı:7, Kasım 2019, ss.1829-1850

Değirmenci, Olgun, "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği", **Terazi Hukuk Dergisi**, Cilt: 9, Sayı:97, Eylül 2014

Demirdal, Balkan M., "Ceza Hakiminin Vicdani Kanaati Üzerine Bir Değerlendirme", **Çankaya Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:5, Sayı:1, Nisan 2020, ss. 1021-1042

Demirkapı, Ertan, "Anglo-Amerikan Hukukunda Bilirkişilik Kurumunda Yeni Eğilimler", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 5, Sayı: 2, 2003, ss. 39-76

Di Nikola, Andrea/Bressan, Serena, **E-Security and the New Horizon of Urban Security, An Information System for Police Forces and Local Administrations**, http://www.esecurity.trento.it/report/eCrime-eSecurity-Guidelines.pdf, Erişim Tarihi: 01.01.2021

Dilberoğlu, Vedat, A., "Cezalar ve Güvenlik Tedbirlerinin Amacı ve Niteliği", **Ankara Üniversitesi Hukuk Fakültesi Dergis**i, Cilt: 65, Sayı: 4, 2016, ss. 1517-1544

Dimitrova, Anna/Brkan, Maja, "Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts Before and After the NSA Affair", **Journal of Common Market Studies**, Cilt: 56, Sayı:4, 2018, ss. 751–767

Dorai, Gokira/Houshmand, Shiva/Baggili, İbrahim, "I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out", **ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security**, Ağustos 2018, https://dl.acm.org/doi/10.1145/3230833.3232814, Erişim Tarihi: 20.10.2021.

Dreyer, Stephan/Schulz, Wolfgang, **The General Data Protection Regulation and Automated Decision-making: Will it Deliver?**, Bertelsmann Stiftung: Gütersloh, Ocak 2019

Dumortier, Franck, "Facebook and Risks of 'De-contextualization' of Information", İçinde: **Data Protection in a Profiled World** Ed: Gutwirth, Serge/Poullet, Yves Poullet, De Hert, Paul, Springer: Dordrecht, Ağustos 2010

Dülger, Volkan, **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayınevi: Ankara, Haziran 2020

Dülger, Volkan, Bilişim, **Kişisel Verilerin Korunması ve İnternet İletişimi Mevzuatı**, Güncellenmiş 7. Baskı, Seçkin Yayınevi: Ankara, 2021

Dülger, Volkan, **Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağaçların Meyvesi Öğretisi),** Seçkin Yayınevi: Ankara, Eylül 2014

Dülger, Volkan/Özkan, Onur, "Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: 'Unutulan' Direktifin Kapsamlı ve Karşılaştırmalı Analizi", **Ceza Hukuku Derneği**, Sayı:42, Nisan 2020, ss.85-149

Edwards, Lilian/Veale, Michael, "Slave To The Algorithm? Why A 'Right To An Explanation' Is Probably Not The Remedy You Are Looking For", **Duke Law and Technology Review**, Cilt: 16, Sayı:1, 2017, ss.18-84, s.25.

Elaine, Angelino/Larus-Stone, Nicholas/Alabi, Daniel/Seltzer, Margo/Cynthia, Rudin, "Learning Certifiably Optimal Rule Lists for Categorical Data", **Journal of Machine Learning Research**, Cilt:18, 2018, ss. 1-78

Erem, Faruk, "Ceza Usulünün Temeli", **Yargıtay Dergisi**, Cilt:10, Sayı:4, Ekim 1984, s.395-399

Erem, Faruk, "Türk Ceza Kanununda Emniyet Tedbirleri", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:1, Sayı:3, 1944, s. 351-378

Erman, Barış,"Ceza Muhakemesi Hukukunda Belirti ve İspat Değeri", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Köksal Bayraktar'a Armağan, Cilt:9, Sayı:1-1, 2010, ss.679-701

Erman, Sahir, "Suçun Önlenmesi ve Suçlular Hakkında Yapılacak Muamele Mevzuunda Birleşmiş Milletler Avrupa Bölgesi İtişari Grubunun Üçüncü Konferansı", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Sayı:1-2, 1958, ss.14-26

Eroğlu, Fulya, **Beden Muayenesi ve Vücuttan Örnek Alma Suretiyle Elde Edilen Dellilerin İspat Değeri**, Yeditepe Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2009

Evik, Vesile Sonay, "Avrupa Birliği Çerçevesinde Kişisel Verilerin Korunması", Tebliğ, Sanal Dünya'da Adalet, **Uluslararası Suç ve Ceza Film Festivali**, 22.11.2019, https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=9uscff-teblig.pdf, Erişim Tarihi: 30.04.2021.

Ferguson, Andrew Gutherie, "Big Data and Predictive Reasonable Suspicion", **University of Pennsylvania Law Review**, Cilt:163, Sayı:2, 2015, ss.327-410

Fisher, Linda. E., "Guilt By Expressive Association: Political Profiling, Surveillance and the Privacy of Groups", **Arizona Law Review**, Cilt:46, Sayı:4, 2004, ss.621-676

Florence, Justin, "Making the No Fly List Fly: Due Process Model for Terrorist Watchlists", **Yale Law Journal**, Cilt:115, Sayı: 8, 2006, ss. 2148-2182

Foucault, Michel, "About the Concept of the 'Dangerous Individual' in 19th Century Legal Psychiatry", **International Journal of Law and Psychiatry**, Cilt: 1, ss. 1-18, 1978

Fremuth, Michael Lysander,"Wächst zusammen, was zusammengehört? Das Trennungsgebot Zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsarchitektur", **Archiv des öffentlichen Rechts**, Cilt: 139, Sayı:1, 2014

Fritsch, Lothar, "Profiling and Location-Based Services (LBS)", içinde **Profiling the European Citizens**, Ed. Hildebrandt, Mireille/Gutwirth, Serge, Springer: Dodrecht, 2008, ss.147-168

G'sell, Florence, "Les Progrès à petits pas de la 'Justice Prédictive' en France", **Europäische Rechtsakademie**, Cilt: 21, 2020, ss.299–310

Gartska, Krzysztof, "Between Security and Data Protection: Searching for a Model of a Legal Big Data Surveillance Scheme within the European Union Data Protection Framework", **HRBDT Occasional Paper Series**, Kasım 2018, https://www.researchgate.net/publication/329339463_Between_Security_and_Data_Protection_Searching_for_a_Model_of_a_Legal_Big_Data_Surveillance_Scheme_within_the_European_Union_Data_Protection_Framework_2018_HRBDT_Occasional_Paper_Series, Erişim Tarihi: 14.03.2021

Gerling, Rainer W./Langer, Cordula/Roßmann, Ray, "Rechtsgrundlagen zur Rasterfahndung: Einführung und Auszüge aus den einschlägigen Gesetzen", **Datenschutz und Daten Sicherheit**, Cilt: 25, Sayı:12, 2001, ss.746-749, s.746.

Geslevich, Nizan Packin/Lev Aretz, Yafit, "Learning Algorithms and Discrimination", İçinde **Research Handbook of Artificial Intelligence and Law,** Ed. Woodrow Barfield/Pagallo, Ugo, Edward Elgar Publishing: Cheltenham, 2018, ss.88-113

Giannelli, Paul C., "The Admissibility of Novel Scientific Evidence: Frye v. United States, a Half-Century Later," **Columbia Law Review**, Cilt: 80, Sayı: 6, Ekim 1980, ss. 1197-1250

Gil González, Elena/ De Hert, Paul, "Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data: An Analysis of GDPR Provisions and Principles", **ERA Forum**, Cilt: 19, 2019

Gless, Sabine, "Truth or Due Process? The Use of Illegally Gathered Evidence in the Criminal Trial", İçinde **German National Reports to the 18th International Congress of Comparative Law**, 2010, ss. 675-709

Gouldirn, Lauryn P., "Defining Flight Risk", **The University of Chicago Law Review**, Cilt:85, Sayı:3, Mayıs 2018, ss. 677-742

Gödekli, Mehmet, "Türk Ceza Muhakemesinde Maddi Gerçeğe Ulaşmanın Ön Koşulu Olarak Hukuka Aykırı Delillerin Değerlendirilmesi Yasağı", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:65, Sayı: 4, 2016, ss.1815-1924

Gökçen, Ahmet/ Çakır, Kerem, "Ceza Muhakemesinde Delil, Delillerin Muhafazası, Toplanması, Değerlendirilmesi ve Delil Yasakları", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Durmuş Tezcan'a Armağan, Cilt:21, Özel Sayı, 2019, ss. 2911-2951

Gözler, Kemal, **İdare Hukuku**, Cilt:2, Ekin Kitabevi: Bursa, 2003

Gutwirth, Serge/Hildebrandt, Mireille, "Some Caveats on Profiling", İçinde: **Data Protection in a Profiled World**, Ed. Gutwirth, Serge/Poullet, Yves Poullet, De Hert, Paul, Springer: Dordrecht, Ağustos 2010, s. 31-41

Hamilton, Melissa, "Judicial Gatekeeping on Scientific Validity with Risk Assessment Tools", **Behavioral Science Law**, Cilt:38, Sayı:3, 2020, ss 226–245

Hamilton, Melissa, "Risk-needs Assessment: Constitutional and Ethical Challenges", **American Criminal Law Review**, Cilt:52, Sayı:2, ss. 231-291

Hamilton, Melissa, "Back to the Future: The influence of Criminal History on Risk Assessments", **Berkeley Journal of Criminal Law**, Cilt:20, Sayı:1, 2015, ss. 75-134

Hänold Stefanie, "Profiling and Automated Decision-Making: Legal Implications and Shortcomings", Robotics, İçinde: **AI and the Future of Law**, Ed. Corrales, Marcelo /Fenwick, Mark/ Nikolaus Forgó, Springer Science: Dordrecht, Kasım 2018, ss.123-154

Han-Wei, Liu/Ching-Fu, Lin/Yu-Jie, Chen, "Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability", **International Journal of Law and Information Technology**, Cilt:27, Sayı: 2, 2019, ss. 122-141

Hassani, Hossein Hassani/Huang, Hu/Silva, Emmanuel/Ghodsi, Mansi, "A Review of Data Mining Applications in Crime", **Statistical Analyses and Data Mining**, Cilt:9, Sayı:3, ss.139-154

Häuselmann, Andreas Nicolas, "Profiling and the GDPR: Harmonised Confusion", **Jusletter**, 12.02.2018, https://jusletter.weblaw.ch/juslissues/2018/924/profiling-in-the-gdp_3b8e8a124f.html__ONCE&login=false, Erişim Tarihi: 11.04.2021

Haydar, Nuran, "Düşman Ceza Hukuku ve Uygulamaları", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Yıl: 2019, Cilt: 16, Sayı: 2, ss. 281-320

Hildebrandt, Mireille, "Defining Profiling: A New Type of Knowledge?", İçinde: **Profiling the European Citizen**, Ed. Hildebrandt, Mireille/Gutwirth, Serge, Springer Science: Dordrecht, Mayıs 2008

Hildebrandt, Mireille, "Profiling: From Data to Knowledge", **Datenschutz und Datensicherheit**, Cilt:30, Sayı:9, 2006, ss. 548-552

Hildebrandt, Mireille, "Who is Profiling Who? Invisible Visibility", İçinde **Reinventing Data Protection**, Ed: Gutwirth Serge/ Poullet Yves/ De Hert Paul/ de Terwangne Cécile/Nouwt, Sjak, Springer: Dodrecht, Haziran 2009, ss.249-252

Hildebrandt, Mireille, **Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology,** Edward Elgar Publishing: Cheltenham, Mart 2015

Hill, Roben K., "What an Algorithm is", **Philosophy and Technology Journal**, Cilt: 29, 2016, ss. 35–59

Iafrate, Fernando, **Artificial Intelligence and Big Data: The Birth of a New Intelligence**, Wiley Publications: London, Mart 2018

Illuminati, Giulio, "Italy: Statutory Nullities and Non-usability", içinde **Exclusionary Rules in Comparative Law**, Ed.Thaman, Stephan C., Springer: Dodrecht, 2013.

Isaac, Michael, "Privatizing Surveillance: The Use of Data Mining in Federal Law Enforcement", **Rutgers Law Review**, Cilt: 58, Sayı: 4, Yaz 2006, ss. 1057-1090

İnankul, Hakan, "Suçun Önlenmesinde Polisin Rolü", **Turkish Studies**, Cilt:11, Sayı:2, 2016, ss.567-582

İnceoğlu, Sibel, **Adil Yargılanma Hakkı: Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-4**, MRK Baskı: Ankara, Nisan 2018

Janus, Eric S./Prentky, Robert A., "Forensic Use of Actuarial Risk Assessment with Sex Offenders: Accuracy, Admissibility and Accountability", **American Criminal Law Review**, Cilt: 40, Sayı: 4, Güz 2003, ss. 1443-1500

Kahraman, Erkut Güçlü, "Yeterli Şüphe Kavramının İddianamenin İadesi Kurumu Bakımından Değerlendirilmesi", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 16, Sayı: 1, 2014, s. 123-150

Kahraman, Recep, "Koruma Tedbirlerinde Orantılılık İlkesi", **İstanbul Hukuk Mecmuası**, Cilt:79, Sayı: 1, 2021, ss. 273-299

Kama Işık, Sezen, **Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış**, On İki Levha Yayıncılık: İstanbul, Ocak 2020

Kangal, Zeynel, **Yapay Zekâ ve Ceza Hukuku**, On İki Levha Yayıncılık: İstanbul, Mayıs 2021

Karabulut, Ferhat/Karapazarlıoğlu, Ersin/Tosun, Hamza, "Ceza Muhakemesinde Delil Kavramı ve Kovuşturma Sürecinde Hâkimlerin Delil Algısı", **Türkiye Barolar Birliği Dergisi**, Sayı:120, 2015, ss. 385-422

Karakehya, Hakan/ Arabacı, Murat, "Cumhuriyet Savcısının Hukuki Statüsü, Muhakemedeki Taraf Pozisyonu ve İspat Yükünün Bulunması Üzerine", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:65, Sayı: 4, 2016, ss. 2059-2081

Karasulu, Bahadır, "Büyük Veri Çağında Bilişim Sistemleri için Zeki Teknikler Destekli Karar Vermenin Rolü: İnceleme ve Analiz", İçinde **Akıllı Teknoloji ve Akıllı Yönetim**, Ed. Tecim, Vahap/Tarhan, Çiğdem/ Aydın, Can, Gülermant Matbaacılık: İzmir, Eylül 2016, ss.1-11

Kaya, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXIX, Sayı: 1-2, 2011, ss. 317-334, 2011

Kayaduman, Abdurrahman Cihad/ Polat, Harun Hilmi, "Veri Temelli Enformasyon Tanımı", **Akademik Sosyal Araştırmalar Dergisi**, Cilt: 6, Sayı: 79, Ekim 2018, s. 326-336.

Kehl, Danielle/ Priscilla, Guo/ Kessler, Samuel, **Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing**, Responsive Communities Initiative, Berkman Klein Center for Internet and Society, Harvard Law School, 2017, https://dash.harvard.edu/handle/1/33746041, Erişim Tarihi: 03.01.2020

Kelly, Matthew/Bielby, Jared, **Information Cultures in The Digital Age: A Festschrift in Honor of Rafael Capullo**, Springer: Wiesbaden, 2016

Keskin Kiziroğlu, Serap, "5271 Sayılı Ceza Muhakemesi Kanunu'nda Basit Arama (Adli Arama)", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:58, Sayı:1, 2009, ss.139-168

Keyman, Selâhattin, "Cürmi Fiilin Yapısal Unsuru Olarak Hareket", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, 1988, Cilt: 40, Sayı: 1-4, ss.121-171

Kılıç, Ergin, **Türk Hukukunda Adli ve İdari Aramalar**, İstanbul Üniversitesi Kamu Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, Ankara 2004

Kızılırmak, Baran, "Kişisel Verilerin İşlenmesinde Adli ve Önleyici Amaçla Öngörülen İstisnaların Ulusal ve Uluslararası Hukuka Göre Değerlendirilmesi", **Kadir Has Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:2, Aralık 2019, ss. 225-261

Kızılırmak, Baran, **Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği**, İstanbul Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul 2018

Kirkpatrick, Keith, "It's not Algorithm, It's the Data", **Communications of Association for Computing Machinary**, Cilt:60, Sayı:2, Şubat 2017 pp. 21-23, s. 23.

Knuth, Donald E., **The Art of Computer Programming: Fundamental Algorithms**, Adison Wesley Publications: Massachusettes , Cilt: 1, Ocak 1938

Kocasakal, Ümit, **Ceza Hukukunda İtiyad**, İstanbul Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 1994

Köroğlu, Yavuz, **Yapay Zeka'nın Teorik ve Pratik Sınırları**, Boğaziçi Üniversitesi Yayınevi: İstanbul, 2017

Kuner, Christopher/ Bygrave, A. Lee/ Docksey, Christopher (Eds), **The EU General Data Protection Regulation (GDPR): A Commentary**, Oxford University Press: Oxford, 1. Baskı, 2020

Kunter, Nurullah, "Bugünkü Ceza Hukukunda Emniyet Tedbirlerinin Yeri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt:13, Sayı:4, 1947, ss.1327-1349

Kunter, Nurullah**, Ceza Muhakemesi Hukuku**, Beta Yayınevi: İstanbul, 1998

Küzeci, Elif**, Kişisel Verilerin Korunması**, On İki Levha Yayınevi: İstanbul, Mayıs 2020

Ladwig, Bernd, "Menschenwürde als Grund der Menschenrechte? Eine Kritik an Kant und über Kant hinaus", **Zeitschrift für Politische Theorie**, Cilt:1, 2010, ss.51-69

Latessa, Edward/Smith, Paula/Lemke, Richard/Makarios, Matthew/Lowenkamp, Christopher, **Creation and Validation of the Ohio Risk Assessment System: Final Report,** Temmuz 2009, https://university.pretrial.org/HigherLogic/System/DownloadDocumentFile.ashx?Do cu mentFileKey=f99d46b1-4a98-23d2-48a8-99cbb94387f1, Erişim Tarihi: 01.07.2021

Leese, Matthias, "The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union", **Security Dialogue**, Cilt:45, Sayı:5, 2014, ss. 494–511

Leiser, Mark/Custers, Bart, "The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680", **European Data Protection Law Review**, Cilt: 5, Sayı: 3, 2019, ss 367-378

Ligeti, Katalin/ Giuffrida, Fabio, "Artificial Intelligence and Criminal Justice", http://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal %20Justice_Ligeti.pdf, Erişim Tarihi: 01.01.2021

Liu, Han, **Rule Based Systems for Classification in Machine Learning Context**, University of Portsmouth, Doktora Tezi, Kasım 2015

Lugar, George F, **Artificial Intelligence: Structures and Strategies for Complex Problem Solving**, Addison Wesley Yayınları: Edinburgh, Ocak 2005

Lundschien, Sylvia, "Predictive Policing: Wie Algorithmen bei der Verbrechensbekämpfung Helfen", 14.01.2021, https://www.goethe.de/prj/jad/de/the/ari/22082332.html, Erişim Tarihi: 01.07.2021.

Lynskey, Orla, "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection From Predictive Policing", **International Journal of Law in Context**, Sayı:15, 2019, s.162-176

Lynskey, Orla, **The Foundations of EU Data Protection Law**, Oxford University Press: Oxford, Kasım 2015

Maalsen, Sophia/ Sadowski, Jathan, "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance", **Surveillance and Society**, Cilt:17, Sayı:1/2, 2019, ss.118-124

Margaret Hu, "Big Data Blacklisting", **Florida Law Review**, Cilt: 67, Sayı:5, 2016, ss. 1735-1809

Marks, Amber/Bowling, Ben/Keenan, Colman, "Automatic Justice?: Technology, Crime, and Social Control", İçinde: **The Oxford Handbook of Law, Regulation and Technology**, Ed: Brownsword, Roger/Scorford, Eloise/Yeung, Karen, Oxford Univerity Press: Oxford, 2017

Marquenie, Thomas "The Police and Criminal Justice Authorities Directive: Data protection Standards and Impact on the Legal Framework", **Computer, Law and Security Review**, Cilt: 33, 2017, ss. 324-340

Mayor, Adrienne, **Gods and Robots: Myths, Machines, and Ancient Dreams of Technology**, Princeton University Yayınevi: Princeton, Kasım 2018

Mcbride, Jeremy, "The Case Law of the European Court of Human Rights on Evidentiary Standards in Criminal Proceedings", https://rm.coe.int/council-of-europe-georgia-european-court-of-human-rights-case-study-ev/16807823c3, Erişim Tarihi: 25.09.2021.

McCormack, Bridget Mary, "Scientific Evidence", https://www.judges.org/wp-content/uploads/Chapter3-SBBr.pdf , Erişim Tarihi: 03.08.2021

McKay, Carolyn, "Predicting Risk in Criminal Procedure: Actuarial Tools, Algorithms, AI and Judicial decision-making", **Current Issues in Criminal Justice**, Cilt:32, Sayı:1, ss.22-39

Memiş Kartal, Pınar, "Özel Hayatın Gizliliği Kapsamında Kişisel Verilerin Korunmasının Sınırları", Sanal Dünya'da Adalet, Tebliğ, **9. Uluslararası Suç ve Ceza Film Festivali**, 27.11.2019, https://cdn.istanbul.edu.tr/FileHandler2.ashx?f=9uscff-teblig.pdf, Erişim Tarihi: 10.02.2021

Mendoza, Isac/ Bygrave, Lee A., "The Right Not to be Subject to Automated Decisions Based on Profiling", 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855 Erişim Tarihi: 11.04.2021

Metin, Yüksel, "Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:1, 2017, ss.1-74

Meyer, Caroline B., "Criminal Profiling as Expert Evidence?: An International Case Law Perspective", İçinde **Criminal Profiling: International Theory, Research, and Practice**, Ed. Kocsis, Richard N, Humana Press: New Jersey, ss.207-247

Minsky, Marvin, **Computation: Finite and Infinite Machines**, Prentice Hall: London, Ocak 1967

Munday, Roderick, **Evidence**, Oxford University Press: Oxford, Temmuz 2017

Mutlu, Emre/ Okudan, Mustafa/Aşıcıoğlu, Faruk, "Uyuşturucu Madde İmalatında Kullanılan Öncül Maddeler: On Yıllık Tek Merkez Verileri", **Türkiye Klinikleri Adli Tıp ve Adli Bilimler Dergisi**, Cilt:17, Sayı:1, 2020, ss.25-34

Nišević, Maja, "Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR", **Global Privacy Law Review**, Cilt:1, Sayı: 2, 2020, ss. 104-115

O'Neil, Cathy, **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**, Crown Publishers: New York, Eylül 2016

Ömeroğlu, Ömer, "Ceza Muhakemesinde Şüpheli ve Sanığın Fizik Kimlik Tespiti", **Türkiye Barolar Birliği Dergisi**, Cilt: 27, Sayı: 115, Kasım 2014, ss.61-102

Öntan, Yaprak, **Ceza Muhakemesi Hukukunda Bilirkişilik**, Ankara Üniversitesi Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Ankara, 2011

Özbek, Murat, "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", **1st International Symposium on Digital Forensics and Security (ISDFS'13)**, Mayıs 2013, https://www.bilgisayardedektifi.com/wp-content/uploads/2013/06/MuratOZBEK_Adli_ Bilisimde_Orijinal_Delil_Uzerindeki_hash_ Sorunlari_isdfs_bildiri.pdf

Özbek, Veli Özer, "Ceza Muhakemesinde Hâkimin Vicdani Kanaati", **Hukuk Felsefesi ve Sosyoloji Arkivi,** Cilt:16, 2007, ss.282-287

Özbek, Veli Özer/ Doğan, Koray/ Bacaksız Pınar, **Ceza Hukuku Genel Hükümler**, Seçkin Yayınevi: Ankara, Eylül 2021

Özbek, Veli Özer/ Doğan, Koray/ Bacaksız, Pınar, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, Eylül 2021

Özel, Kadir Can, "Bir Koruma Tedbiri Olarak Arama", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Durmuş TEZCAN'a Armağan, Cilt:21, Özel Sayı, 2019, s. 1217-1266, s.1219, 1230

Özgenç, İzzet, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayınevi: Ankara, Eylül 2021

Öztürk, Bahri/ Eker Kazancı, Behiye/ Soyer Güleç, Sesim, **Ceza Muhakemesi Hukukunda Koruma Tedbirleri**, Seçkin Yayınevi: Ankara, Mart 2021

Öztürk, Bahri/ Erdem, Mustafa Ruhan/ Özbek, Veli Özer, **Uygulamalı Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, 2004

Öztürk, Bahri/ Tezcan, Durmuş/ Erdem, Mustafa Ruhan/ Sırma Gezer, Özge/ Saygılar Kırıt, Yasemin/ Alan Akcan, Esra/ Özaydın, Özdem/ Erden Tütüncü, Efser/ Altınok Villemin, Derya/ Tok, Mehmet Can, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, 2021

Peeters, Rik/Schuilenburg, Marc, "Machine Justice: Governing Security Through the Bureaucracy of Algorithms", **Information Polity**, Cilt:23, Sayı:1, 2018, ss. 267–280

Poullet, Yves, "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?", İçinde: **Data Protection in a Profiled World**, Ed: Gutwirth, Serge/Poullet, Yves Poullet, De Hert, Paul, Springer: Dordrecht, Ağustos 2010, s.3-30

Privacy International, **Stellungnahme an das Bundesverfassungsgericht zum Verfassungsbeschwerdeverfahren 2 BvR 1850/18**, Eylül 2019, https://privacyinternational.org/sites/default/files/2019-09/BVerfG_Statement_PI_Trojans_Sept2019_DE.pdf, Erişim Tarihi: 14.06.2021, s.3.

Purtova, Nadezhda, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law", **Law, Innovation and Technology**, Cilt:10, Sayı: 1, 2018, ss. 40-81

Quattrocolo, Serena, **Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion**, Springer: Cham, Ağustos 2020, s.5.

Raymond, Margaret, "Down on the Corner, Out in the Street: Considering the Character of the Neighborhood in Evaluating Reasonable Suspicion", **Ohio State Law Journal**, Cilt:60, Sayı:1, 1999, ss.99-141

Rettenberger, Martin/Eher, Reinhard, "Die deutsche Übersetzung des Static 99 zur aktuarischen Kriminalprognose verurteilter Sexualstraftäter Monatsschrift für Kriminologie und Strafrechtsreform", **Monatsschrift für Kriminologie und Strafrechtsreform**, Cilt: 89, Sayı: 5, Ekim 2006, ss.352-365

Roth, Andrea L., "Machine Testimony", **Yale Law Journal**, Cilt: 126, Sayı: 1, 2017, ss.1972-2053

Rubinstein, Ira/ Lee, Ronald D./ Schwartz, Paul M.,"Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches", **University of Chicago Law Review**, Cilt:75, Sayı:1, 2008, ss. 261-285

Rudin, Synthia, "Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead", 22.09.2019, https://arxiv.org/abs/1811.10154, s.6, Erişim Tarihi: 29.04.2021.

Russel Stuart J/ Norvig Peter, **Artificial Intelligence: A Modern Approach**, Pearson: Edinburgh, Mayıs 2016

Sajfert, Juraj/ Quintel, Teresa, "Data Protection Directive (EU) 2016/680 For Police And Criminal Justice Authorities", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, 2019, Erişim Tarihi: 29.04.2021,

Say, Cem, **50 Soruda Yapay Zekâ**, 7 Renk Basım Yayınevi: İstanbul, Nisan 2020, İstanbul, s. 34.

Schermer, Bart W., "The Limits of Privacy in Automated Profiling and Data Mining", **Computer, Law and Security Review**, Cilt: 27, Sayı:1, 2011, ss. 45-52

Searle, John R. "Minds, Brains, and Programs", İçinde **Foundations of Cognitive Pscyhology: Core Readings**, Ed: Levitin, Daniel J., MIT Press: Cambridge, Ekim 2002, ss. 95-113

Selbst, Andrew D./ Powles, Julia, "Meaningful Information and the Right to Explanation**", International Data Privacy Law**, 2017, Cilt: 7, Sayı: 4, ss.233-242

Sevdiren, Öznur, "Anayasa Mahkemesi'nin Tutuklama Kararının Maddi Şartları İçtihadına Eleştirel Bir Yaklaşım", **Anayasa Hukuku Dergisi**, Cilt:8, Sayı:16, 2019, ss. 295-358

Sezer, Yasin/İpek, Ali İhsan/Parlak, Engin, **Adli ve Önleme Amaçlı İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme**, Seçkin Yayınevi: Ankara, 1. Baskı, Eylül 2012

Shah, Huma/ Warwick, Kevin, "Imitating Gender as a Measure for Artificial Intelligence: Is It Necessary?" In **Proceedings of the 8th International Conference on Agents and Artificial Intelligence**, Roma, 2016, ss. 126-131, s.130.

Simmons, Ric "Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System", **Michigan State Law Review**, Sayı: 4, 2016, ss. 947-1018

Slobogin, Christopher, "Transaction Surveillance by the Government", **Mississippi Law Journal**, Cilt:75, 2005, ss.139-191

Solove, Daniel J., “Data Mining and the Security-Liberty Debate”, **The University of Chicago Law Review**, Cilt: 75, Sayı:1, 2008, ss. 343-362

Staffler, Lukas/Jany, Oliver, ”Künstliche Intelligenz und Strafrechtspflege: Eine Orientierung”, **Zeitschrift für Internationale Strafrechtsdogmatik**, Sayı:4, 2020, s.164-177

Steinbock, Daniel J., "Data Matching, Data Mining, and Due Process," **Georgia Law Review**, Cilt: 40, Sayı: 1, Güz 2005, ss. 1-84

Stumpf, Juliet P. “Getting to Work: Why Nobody Cares About e-verify (and Why They Should)”, **UC Irvine Law Review**, Cilt:2, Sayı 1, 2012, s 381-414

Sundby, Scott E./Ricca, Lucy B.,“The Majestic and the Mundane: The Two Creation Stories of the Exclusionary Rule”, **Texas Tech Law Review**, Cilt:43, 2010, ss. 391-433

Şahin, Cumhur/ Göktürk, Neslihan, **Ceza Muhakemesi Hukuku II**, Seçkin Yayınevi: Ankara, Şubat 2021

Şahin, İlyas, “Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi”, **Marmara Üniversitesi Hukuk Faültesi Hukuk Araştırmaları Dergisi**, Cilt:20, Sayı:3, 2014, ss.97-144

Şen, Ersan, “Gizli Tanıklık”, **Nevşehir Barosu Dergisi**, Cilt:1, Sayı, 1, Mart 2014, ss. 273-283

Şener, Yavuz Selim, **Fikri Mülkiyet Hukukunda Dijital Veri Tabanlarının Korunması**, İstanbul Kültür Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, 2013

Şentürk, Cadide/ Bayzit, Tuğba, “Gizli Tanık”, **Türkiye Barolar Birliği Dergisi**, Cilt:25, Sayı:101, ss. 103-166

Taneri, Gökhan, “Temel Cezanın Belirlenmesi”, **Ankara Barosu Dergisi**, Cilt:74, Sayı:3, 2016, ss. 127-161

Tatar, Erol, “Gizli Tanık”, **Ankara Barosu Dergisi**, Sayı:4, 2013, ss.285-296

Tayebi, Mohammad A./ Glässer, Uwe, **Social Network Analysis in Predictive Policing: Concepts, Models and Methods**, Springer Yayınevi: Londra, Ekim 2016

Tene Omar/ Polonetsky Jules, “Big Data for All: Privacy and User Control in the Age of Analytics”, **Northwestern Journal of Technology and Intellectual Property**, Cilt: 11, Sayı: 5, 2013, s.258.

Tetik, Erdoğan, “Kimlik Tespitinde Parmak İzi Arşivlerinin Gerekliliği ve Ülkemizdeki Durumun Değerlendirilmesi, https://www.caginpolisi.com.tr/eski_ sitemiz/35/42-43-44-45-46-47.htm, Erişim Tarihi: 30.06.2021.

Thai, Joseph T., "Is Data Mining Ever Search Under Justice Stevens's Fourth Amendment", **Fordham Law Review**, Cilt:74, Sayı:4, 2006, ss.1731-1758

The University of Oxford, **The Law on Policing Peaceful Protests**, September 2020, https://www.law.ox.ac.uk/sites/files/oxlaw/opbp_report_on_the_law_on_policing_peaceful_protests_0.pdf, Erişim Tarihi: 29.06.2021

Tien, Lee, "Privacy, technology and Data mining", **Ohio Northern University Law Review**, Cilt:30, Sayı:3, 2004, ss. 389-416

Topal, Çağatay, "Alan Turing'in Toplumbilimsel Düşünü: Toplumsal Bir Düş Olarak Yapay Zekâ", **Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi**, Cilt:57, Sayı: 2, 2017, ss. 1340-1364,

Torre, Marco, **Il Captatore Informatico: Nuove Tecnologie Investigative e Rispetto delle Regole Processuali**, Guiffre Editore: Milano, Haziran 2017

Turner Iontcheva, Jenia, "Regulating Interrogations and Excluding Confessions in the United States: Balancing Individual Rights and the Search for the Truth", İçinde **Do Exclusionary Rules Ensure a Fair Trial?**, Ed:Gless, Sabine/Richter, Thomas, Springer, 2019, ss. 93-129,

Tümerkan, Somay, "Klasik, Pozitivist Okullarda ve Toplumsal Savunma Hareketinde Ceza Sorumluluğunun Esası", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt:48, Sayı:1-4, İstanbul, 1983, ss.51-71

Türinay, Faruk Yasin, "Ceza Muhakemesi Hukukunda Koruma Tedbirlerinin Sınıflandırılması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:70, Sayı:2, 2021, ss. 475-541

Tyler, Tom R./ Jackson, Jonathan/ Mentovich, Avital, "The Consequences of Being an Objectof Suspicion: Potential Pitfalls of Proactive Police Contact", **Journal of Empirical Legal Studies**, Cilt:12, Sayı: 4, Aralık 2015, ss. 602–636

Ünver, Yener/ Hakeri, Hakan**, Ceza Muhakemesi Hukuku**, Adalet Yayınevi: Ankara, Mayıs 2019

Van der Sloot, Bart, "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'", **Utrecht Journal of International and European Law**, Cilt:31, Sayı:80, 2015, s.25-50

Van Schendel, Sascha, "The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI", İçinde **Regulating New Technologies in Uncertain Times**, Ed. Reins, Leonie, Springer: The Hague, Mart 2019, s.225-240

Vedder, Anton, "KDD: The Challenge to Individualism", **Ethics and Information Technology**, Cilt:1, 1999, ss. 275–281

Villasenor, John/Foggo, Virginia, "Artificial Intelligence, Due Process, and Criminal Sentencing", **Michigan State Law Review**, Sayı:2, 2020, ss.295-354

Wachter, Sandra, "Normative Challenges of Identification in the Internet of Things: Privacy, profiling, Discrimination, and the GDPR", **Computer Law and Security Review**, Cilt:34, 2018, s.436-449

Wachter, Sandra/Mittelstadt, Brendt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law In The Age Of Big Data And AI", **Columbia Business Law Review**, Cilt:2019, Sayı: 2, ss. 494-620

Wachter, Sandra/Mittelstadt, Brendt/Russell, Chris, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", **Harvard Journal of Law and Technology**, Cilt: 31, Sayı: 2, Spring 2018, ss. 841-887

Wang, Chenchen, **Encadrement de la Liberté de la Preuve dans la Procédure Pénale: Étude comparée France-Chine,** Université de Bordeaux, Hukuk Fakültesi Doktora Tezi, Kasım 2019

Warnking, Vera, **Strafprozessuale Beweisverbote in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und ihre Auswirkungen auf das deutsche Recht**, Peter Lang GmbH: Frankfurt am Main, 2009

Westermann, Hannes, **Change of Purpose: The effects of the Purpose Limitation Principle in the General Data Protection Regulation on Big Data Profiling**, Lund Üniversitesi Hukuk Fakültesi, Yüksek Lisans Tezi, 2018, s.46, 47.

Wisser, Leah, "Pandora's Algorithmic Black Box: The Challenges of Using Algorithmic Risk Assessments in Sentencing", **American Criminal Law Review**, Cilt:56, Sayı:4, 2019, ss. 1811-1832

Yenidünya, Caner, "Ceza Muhakemesinde Delillerin Değerlendirilmesi, Delil Yasakları ve Hukuka Aykırı Delillerin Ceza Yargılamasında Vaziyeti", 25.06.2019, https://caneryenidunya.medium.com/ceza-muhakemesinde-delillerin-de%C4%9Ferlendirilmesi-delil-yasaklar%C4%B1-ve-hukuka-ayk%C4%B1r%C4%B1-delillerin-ceza-bff814552eb4, Erişim Tarihi: 10.09.2021.

Yenidünya, Caner, "Ceza Muhakemesinde Koruma Tedbirlerine İlişkin Temel Özellikler", 26.06.2019, https://caneryenidunya.medium.com/ceza-muhakemesinde-koruma-tedbirlerine-i%CC%87li%C5%9Fkin-temel-%C3%B6zellikler-f0f35107b92d, Erişim Tarihi: 01.07.2021.

Yenisey, Feridun, "Anayasa Mahkemesi'ne Bireysel Başvuru Kararlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi: Tutuklama", **Anayasa Yargısı Dergisi**, Cilt: 33, 2016

Yenisey, Feridun/ Nuhoğlu, Ayşe, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi: Ankara, Eylül 2021

Yılmaz, Zehra, **Ceza Muhakemesi Hukukunda Şüphe**, Selçuk Üniversitesi Kamu Hukuku Ana Bilim Dalı, Yüksek Lisans Tezi, Konya 2019

Yokuş Sevük, Handan, "Ceza Muhakemesi Hukukunda Bilirkişilik", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 64, Sayı: 1, 2006, ss. 49 – 107

Yücedağ, Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LXXV, Sayı: 2, 2017, ss. 765-790

Zafer, Hamide, "Emniyet Tedbiri Muhakemesinin Özellikleri", **İstanbul Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:62, Sayı:1-2, ss.263-314

Zarsky, Tal Z., "Incompatible: The GDPR in the Age of Big Data", **Seton Hall Law Review**, Cilt: 47, 2017, ss.995-1020

Završnik, Aleš, "Criminal Justice, Artificial Intelligence Systems, and Human Rights", **ERA Forum**, Cilt:20, 2020, ss. 567-583

Zuiderveen, Frederik Borgesius, **Improving Privacy Protection in the Area of Behavioural Targeting**, Doktora Tezi, Amsterdam Üniversitesi Hukuk Fakültesi, Aralık 2014

Rapor, Görüş, Tavsiye Kararları

Article 29 Data Protection Working Party, **Guidelines on Consent under Regulation 2016/679,** 17/EN WP259, Revised Version 10.04.2018, https://ec.europa.eu/newsroom/article29/items/623051, Erişim Tarihi: 30.04.2021

Article 29 Data Protection Working Party, **Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC**, 844/14/EN WP 217, 09.04.2014, https://www.fia.org/sites/default/files/2019-11/Excerpts%20-%20Opinion%2006-2014%20on%20the%20notion%20of%20legitimate%20interests%20of%20the%20....pdf, Erişim Tarihi:27.04.2021

Article 29 Working Party, **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679,** 17/EN, http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826, 06.02.2018, Erişim Tarihi: 25.02.2021

Article 29 Working Party, **Opinion 03/2013 on Purpose Limitation**, 00569/13/EN WP 203, 02.04.2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, Erişim Tarihi: 22.02.2021

Article 29 Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf, Erişim Tarihi: 16.02.2021

Article 29 Working Party, **Opinion on Some Key Issues of the Law Enforcement Directive**, 17/EN WP 258, 29.11.2017

Comission of European Communities, **Amended Proposal for a Council Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data**, COM(92) 422 final—SYN 287, 15.10.1992, https://aei.pitt.edu/10375/1/10375.pdf, Erişim Tarihi: 11.04.2021,

Council of Europe Committee of Ministers, **Resolution (74) 29 on the Protection of The Privacy of Individuals Vis-A-Vis Electronic Data Banks In The Public Sector**, 20 Eylül 1974, https://rm.coe.int/16804d1c51, Erişim Tarihi: 10.02.2021.

Council of Europe, Committee of Ministers**, Resolution N (73) 22 on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks In The Private Sector**, 26 Eylül 1973, https://rm.coe.int/1680502830, Erişim Tarihi: 10.02.2021.

Council of Europe, **Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, European Treaty Series Sayı: 108, https://rm.coe.int/16800ca434, Erişim Tarihi: 10.02.2021.

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, Erişim Tarihi: 30.12.2020

European Commisson, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-65-F1-EN-MAIN-PART-1.PDF, Erişim Tarihi: 31.12.2020

European Data Protection Board, **Recommendations 01/2021 on the Adequacy Referential under the Law Enforcement Directive**, 02.02.2021, https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf, Erişim Tarihi: 30.04.2021

European Union Agency for Fundamental Rights, **Handbook on European Data Protection Law,** Publications of European Union: Luxembourg, 2014

European Union Agency for Fundemantal Rights, **Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU**, Imprimerie Centrale: Lüksemburg, 2017

Farsam, Salimi, **National Report for Austria**, 19th International AIDP-Congress on Information Society and Penal Law, Eylül 2013,

https://www.combattingcybercrime.org/files/virtual-library/national-laws/preparatory-colloquium-section-iii-national-report-for-austria.pdf, Erişim Tarihi: 12.09.2021

Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf, Nisan 2018, Erişim Tarihi: 01.05.2021

Kişisel Verileri Koruma Kurumu, Açık Rıza, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf, Erişim Tarihi: 01.05.2021

Le Comité des Ministres du Conseil de l'Europe, **La Protection des Personnes à l'Égard du Traitement Automatisé des Données à caractère personnel dans le Cadre du Profilage** Recommandation, CM/Rec(2010)13, 23.11.2010, Editions du Conseil de l'Europe: Strasbourg Cedex, s.43.

Lück, Nico, **Lernende Künstliche Intelligenz in der Rüstungskontrolle**, PRIF Report 4/2019, https://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/prif0419.pdf

ÖZGEÇMİŞ

TEZ ONAY SAYFASI

Üniversite	:T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü	:SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı	:IRMAK ERDOĞAN
Tez Başlığı	:YAPAY ZEKÂ TEKNOLOJİLERİNİN CEZA MUHAKEMESİNDE KİŞİSEL VERİ TOPLANMASINA ETKİLERİ
Savunma Tarihi	: 28 /12/ 2021
Danışman	: PROF. DR. VESİLE SONAY EVİK

JÜRİ ÜYELERİ:

Unvan, Ad-Soyadı İmza

Prof. Dr. Zeynel T. Kangal

Doç. Dr. Güçlü Akyürek

Doç. Dr. Eylem Aksoy Retornaz

Prof. Dr. Pınar Memiş Kartal

Prof. Dr. Vesile Sonay Evik

Prof. Dr. M. Yaman ÖZTEK

Enstitü Müdürü