YAPAY ZEKÂ TEMELLİ TEKNOLOJİLER VE CEZA HUKUKU

Yapay Zekâ Çalışma Grubu

Yıllık Rapor

2021

İSTANBUL BAROSU

•

Bilişim Hukuku Komisyonu

•

Yapay Zekâ Çalışma Grubu

Yapay Zekâ Çağında Hukuk

2021

Danışman
Dr. Barış Erman-*Yeditepe Üniversitesi Hukuk Fakültesi*

•

Editörler
Av. Selin Çetin
Av. Elif Baban
Av. C. Sümeyye Uçar
Av. Kübra İslamoğlu Bayer
Av. Zeynep Öğretmen Kotil
Av. Tarık T. Yazıcılar
Av. Damlanur İpek
Av. Benay Çaylak
Av. Nihan Üçer
Av. Pınar Saruhan
Av. Zeynep Cemre Demirtaş
Av. Mikal İpek
Av. Beyza Nur Gemci
Ayşegül Sivri

Yapay Zekâ Çalışma Grubu, İstanbul Barosu, Bilişim Hukuku Komisyonu bünyesinde 2019 yılında oluşturulmuştur. Çalışma grubunun odak noktası, yapay zekâ ve robotik teknolojilerin hukuki yansımalarıdır. Çalışma grubu, yapay zekâ ve robotik teknolojiler konusunda hukuki görüş bildirmekte ve bu kapsamda İstanbul Barosu'nun diğer merkez ve komisyonlarıyla iş birliği içinde çalışmaktadır. Çalışma grubunun diğer bir amacı ise, bu alanda yaşanan teknik ve hukuki gelişmeleri hukuk kamuoyuna duyurmaktır.

Grup ile ilgili daha fazla bilgi için:
https://www.istanbulbarosu.org.tr/HaberDetay.aspx?ID=15275&Desc=Yapay-Zeka-%C3%87a%C4%9F%C4%B1nda-Hukuk

İçindekiler

Yönetici Özeti 5

Executive Summary 8

Yapay Zekâlı Otonom Varlıkların Dahil Olduğu Suçlarda Önerilen Suç Sorumluluğu Modelleri 11

Yapay Zekâ Temelli Önleyici Hukuk Mekanizmaları- Öngörücü Polislik 29

Yüz Tanıma Teknolojilerinin Temel Hak ve Özgürlükler Üzerindeki Etkileri 47

Derin Sahte (*Deepfake*) Teknoloji Karşısında Türk Ceza Hukuku 60

Ceza Muhakemesinde Yapay Zekâ Temelli Risk Değerlendirme Araçları ve Hukuki Etkileri 77

Yapay Zekâ Kullanan Otonom Silah Sistemleri ve Savaş Suçları 91

Yönetici Özeti

İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zekâ Çalışma Grubu olarak, 2021 yılı raporumuzda yapay zekâya ilişkin gelişmeleri ve kullanımı yaygınlaşan bazı uygulamaları ceza hukuku bakımından ele aldık.

Raporda ilk olarak, Kadir Has Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Arş. Gör., Würzburg Üniversitesi Doktora Öğrencisi Baran Kızılırmak tarafından "Yapay Zekâlı Otonom Varlıkların Dahil Olduğu Suçlarda Önerilen Suç Sorumluluğu Modelleri" başlıklı kısım kaleme alınmıştır. Yapay zekâlı otonom varlıklar çeşitli şekillerde suça dahil olabilir. Alışılagelmiş ceza hukuku sorunlarından farklı olarak, bunların otonom özellik göstermesi ve öngörülmesi güç çıktılar üretmesi ceza sorumluluğunun tespitini güçleştirmektedir. Öğretide mevcut ceza hukuku anlayışının sınırlarının zorlandığı belirtilmekte; bazıları kaynağını haksız fiil sorumluluğundan alan modeller önerilmektedir. Bu çalışma öğretide ileri sürülen başlıca modelleri ana hatlarıyla değerlendirmeyi amaçlamaktadır. Bu doğrultuda, yapay zekâlı otonom varlıklara ayrı bir hukukî kişilik tanınması, kendi ceza sorumluluklarının olabilirliği, dolaylı faillik gibi konuların yanı sıra, bazı özel hukuk sorumluluk modellerinin uyarlanabilirliği üzerinde de durulmaktadır. Nihâyet şu soru gündeme gelmektedir: "Gelecekte ceza sorumluluğu ile haksız fiil sorumluluğu birbirine yaklaşacak mıdır?"

İkinci olarak, Marmara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı Doktor Öğretim Üyesi Zafer İçer tarafından "Yapay Zekâ Temelli Önleyici Hukuk Mekanizmaları- Öngörücü Polislik" başlıklı kısım kaleme alınmıştır. Yapay zekâ sistemleri, bir yandan sağladığı olanaklarla kolluk faaliyetlerinin daha etkin şekilde icra edilmesini kolaylaştırırken öte yandan bu faaliyetlerin temel hak ve hürriyetlere olan etkisine ilişkin birtakım hukuki problemler doğurmaktadır. Bu risk-yarar dengesini irdeleyen bu çalışmada yapay zekâ temelli öngörücü kolluk faaliyetlerinin farklı örnekleri kısaca açıklandıktan sonra bu faaliyetlerin avantajları ve dezavantajları ortaya konulmuş; akabinde öngörücü kolluk faaliyetlerinin haklar bağlamında meydana getirebileceği sorunlar tespit edilmiştir. Tüm bunların nihayetinde, kolluk faaliyetinin tek başına yapay zekâ sistemlerine bırakılmasının hukukun evrensel ilkeleriyle örtüşmeyeceği ve bireylerin temel haklarına müdahalede asli unsurun insan olmaya devam etmesi gerektiği sonucuna varılmıştır.

Üçüncü olarak, İstanbul Barosu İnsan Hakları Merkezi Başkanı Av. Tuğçe Duygu Köksal tarafından "Yüz Tanıma Teknolojilerinin Temel Hak ve Özgürlükler Üzerindeki Etkileri" başlıklı kısım kaleme alınmıştır. Pek çok ülkede suç işlenmesinin önlenmesi, kamu düzeninin korunması gibi sınırlı sayıda olmayan meşru amaçlarla önleyici kolluk faaliyetleri kapsamında kullanılmaya başlanan yüz tanıma sistemleri, pek çok açıdan temel hak ve özgürlüklere müdahale teşkil edebilmektedir. Hiç şüphesiz bu müdahalenin demokratik bir toplumda gerekli olup olmadığını değerlendirmeden ve meşru amaçla orantılı bir kullanımın

söz konusu olup olmadığını saptamadan evvel kanuni dayanağın olup olmadığının belirlenmesi önemlidir. Kanuni bir dayanak bulunması gereği, keyfi kullanıma ilişkin olarak usuli güvenceleri barındıran temel bir yasal düzenleme ile sağlanmalıdır. Bu gereklilik sağlandıktan sonra müdahalenin temel hak ve özgürlükler bakımından etkileri, adil denge kriterleri gözetilerek değerlendirilmektedir. Yüz tanıma sistemlerinin kolluk faaliyetlerinde kullanımı uluslararası alanda da ayrımcılık yasağı ile özel hayat ve aile hayatının korunmasına saygı hakkı kapsamında tartışılmış, bu tartışma pek çok şirketin yüz tanıma sistemlerinin satışını durdurmasına kadar varmıştır. Bu çalışmada dile getirilen endişeler ve Avrupa İnsan Hakları Mahkemesi'nin mevcut içtihadı karşısında yüz tanıma sistemlerinin durumu ele alınmaya çalışılmıştır.

Dördüncü olarak, Fatih Sultan Mehmet Vakıf Üniversitesi, Öğretim Görevlisi Dr. Buket Abanoz Öztürk tarafından "Derin Sahte (Deepfake) Teknoloji Karşısında Türk Ceza Hukuku" başlıklı kısım kaleme alınmıştır. Bu çalışmada, bir kişinin görüntüsünün başka bir kişinin vücuduna yerleştirilerek sahte görsel ve işitsel içerik üretilmesini mümkün kılan derin sahte (*deepfake)* teknolojiden doğan ceza hukuku sorumluluğu değerlendirilmektedir. Her geçen gün gelişmekte olan ve derin öğrenme teknolojisinin kullanımıyla oluşturulan sahte içerikler, insanın duyu organlarıyla kolayca ayırt edemeyeceği kadar gerçekçi gözükmektedir. Bununla birlikte, herkesin erişimine ve kullanımına açık olan mobil uygulama ve araçlarla herhangi bir kişi, kolaylıkla anlık sahte içerik üretebilmektedir. Belirtilen bu özellikleriyle söz konusu teknoloji, temel hak ve özgürlüklere ciddi şekilde müdahale edebilecek bir potansiyele sahiptir ve birçok suçun işlenmesi amacıyla kullanılma riski bulunmaktadır. Gerçek bir kişinin sesi ve görüntüsü manipüle edilerek sahte bir içerik üretildiğinde bu sahte içerik; o kişiyi aşağılamak, küçük düşürmek, tehdit etmek veya dolandırmak için kullanılabileceği gibi derin sahte pornografi sektörü ile cinsel dokunulmazlığın, özel hayatın gizliliğinin ve kişisel verilerin gizliliğinin de ihlali söz konusu olabilir. Derin sahte teknoloji ile oluşturulan profil, haber veya videolar bilgi dezenformasyonu ile kitleleri yönlendirmek veya seçim sonuçlarını manipüle etmek amacıyla da kullanılabilir. Dolayısıyla derin sahte teknoloji karşısında doğru ve güvenilir bilgiye erişim hakkının da tehlike altında olduğu söylenebilir. Ayrıca ceza muhakemesinde önemli bir delil kaynağı olan ses ve görüntü kayıtları, söz konusu teknoloji ile manipüle edildiğinde delillerin karartılması ve adaletin engellenmesi riski de ortaya çıkmaktadır. Çalışmada, derin öğrenme teknolojisinin kullanımıyla oluşturulan sahte içeriklerin beraberinde getireceği tehlike ve zararlar karşısında Türk ceza hukukundaki mevcut düzenlemelerin yeterli olup olmadığı sorusu tartışmaya açılırken, söz konusu teknoloji karşısında yeni suç tipleri oluşturulmasını öneren görüşler de değerlendirilmektedir.

Beşinci olarak, İstanbul Barosu, Bilişim Hukuku Komisyonu- YZ Çalışma Grubu üye ve İstanbul Üniversitesi, Kamu Hukuku Doktora Adayı Av. Ozan Can Özbalçık tarafından "Ceza Muhakemesinde Yapay Zekâ Temelli Risk Değerlendirme Araçları ve Hukuki Etkileri" başlıklı kısım kaleme alınmıştır. Makine öğrenimi ve yapay zekâ alanındaki gelişmeler hızlandıkça bunların ceza adaleti süreçlerinde kullanımı da yaygınlaşmaktadır. Bugün gelinen

noktada yapay zekâ sistemli risk değerlendirme araçları, bir suçun ya da bunun kim tarafından işleneceğinin, sanığın yargılama esnasında kaçma veya yeniden suç işleme olasılığının tahmini gibi birçok amaçla kullanılmaktadır. Bu araçlar, karar alıcıların işlerini kolaylaştırıyor gibi görünse de ceza adaleti sisteminin amaçlarına ve ceza hukukunun çeşitli güvencelerine yönelik tehditler oluşturmaktadır. Bu çalışmada, risk değerlendirme araçlarının ceza muhakemesinin hangi aşamalarında kullanıldığı ve nasıl faydalar sağlayabildiği ortaya konulduktan sonra ayrımcılık, adil yargılanma, kişi özgürlüğü ve hâkimin tarafsızlığı gibi konularda yol açabileceği sorunlara değinilerek çözüm önerileri ele alınmıştır.

Son olarak, Tübingen Eberhard Karls Üniversitesi, Doktora Öğrencisi Ceren ÖZBEK ve İstanbul Bilgi Üniversitesi, Uluslararası Hukuk Anabilim Dalı Araştırma Görevlisi, Galatasaray Üniversitesi, Kamu Hukuku Doktora Adayı Hilâl Nur ŞARBAK tarafından "Yapay Zekâ Kullanan Otonom Silah Sistemleri ve Savaş Suçları" başlıklı kısım kaleme alınmıştır. YZ ile bütünleşik silah sistemleri dünyanın farklı yerlerinde devam eden silahlı çatışmalarda yoğunlukla kullanılmakta ve bu sistemlere ilişkin teknoloji her geçen gün hızla gelişmektedir. Bununla birlikte, YZ kullanan ve otonom silah sistemleri (OSS) olarak adlandırılan sistemlerin askeri kullanımına ilişkin mevcut uluslararası hukuk düzenlemeleri muğlak ve yetersizdir. Bu çalışma, YZ'nin askeri amaçlarla kullanılmasına ilişkin uluslararası hukuk düzenlemelerini savaş suçları bakımından değerlendirmektedir. Bu bağlamda çalışma, üç temel kısımdan oluşmaktadır. Çalışmanın ilk kısmı, YZ ve OSS kavramlarının açıklanmasına ayrılmıştır. Çalışmanın ikinci kısmı, OSS aracılığı ile işlenebilecek savaş suçları kapsamında ortaya çıkabilecek sorumluluk hukuku problemlerine odaklanmaktadır. Çalışmanın üçüncü ve son kısmı ise, uluslararası sorumluluk hukuku kapsamında çıkabilecek sorunlara ilişkin çözüm önerilerini incelemektedir.

Executive Summary

As the Istanbul Bar Association, IT Law Commission-AI Working Group, we argued the developments in artificial intelligence and some applications that have become widespread, in terms of criminal law, in the 2021 report.

In the report, firstly, the section titled “Propounded Criminal Liability Models in Crimes Involving Artificial Intelligence Autonomous Agents” was penned by Baran Kızılırmak who is research assistant at Kadir Has University Law Faculty Department of Criminal and Criminal Procedure Law and University of Würzburg PhD Student. Autonomous agents with artificial intelligence may be involved in crimes in various circumstances. Unlike conventional criminal law disputes, their autonomous character and production of unforeseeable outputs cause determining criminal liability challenging. Some opinions in the doctrine argue that the limits of the current criminal law perception is being pushed. Certain models, some of which derive from tort liability are propounded. This study aims to evaluate the prominent models put forward in the doctrine. Thus, recognition of a separate legal personhood for autonomous agents with AI, the feasibility of having their own criminal liability and perpetration through another model; as well as the adaptability of certain private law liability models are also evaluated. Finally, the following question is posed: “Will criminal liability and tort liability converge in the future?”

Secondly, the section titled “AI Based Predictive Law Mechanism-Predictive Policing” was penned by Dr. Zafer İçer -Marmara University Law Faculty Department of Criminal and Criminal Procedure Law. Artificial intelligence systems simplify the more effective law enforcement implementations with the facilities which it provides, but also cause a number of legal problems related to the impact of these activities on fundamental rights and freedoms. In this study, which examines this risk-benefit balance, different instances of artificial intelligence-based predictive policing were briefly explained. After that, advantages and disadvantages of these types of implementations were presented and then, the problems that predictive policing may cause in the context of rights were identified. Finally, it was concluded that the execution of law enforcement by artificial intelligence systems alone will not comply with the universal principles of law and that the essential element should continue to be human in practices that interfere with the fundamental rights of individuals.

Thirdly, the section titled “The Effects of Face Recognition Technology on Fundamental Rights and Freedoms" was penned by Atty. Tuğçe Duygu Köksal- the head of the Istanbul Bar Association, the Centre of Human Rights. The facial recognition systems have started to be used in preventive law enforcement activities in many countries for non-limiting legitimate purposes such as preventing crime and protecting public order. [The facial recognition] can interfere with fundamental rights and freedoms in many respects. Undoubtedly, it is important

to determine firstly, whether there is a legal basis before assessing whether this interference was necessary in a democratic society and proportional to the legitimate aim. The need for a legal basis must be ensured by a legal regulation that includes procedural safeguards against arbitrary use of facial recognition. When this legality requirement is met, the effects of the intervention in terms of fundamental rights and freedoms should be assessed by taking into consideration the fair balance exercise. The use of facial recognition systems in the law enforcement activities has also been discussed in the international arena in elation with the prohibition of discrimination and the right to respect for private and family life. This debate has reached the point where many companies have stopped selling facial recognition systems. In this study, the facial recognition systems will be discussed in the light of the articulated concerns and the current case law of the European Court of Human Rights.

Fourthly, the section titled "Turkish Criminal Law Against Deepfake Technology" was penned by Dr. Buket Abanoz Öztürk- Lecturer, Fatih Sultan Mehmet Vakıf University. The aim of this study is to evaluate criminal liability arising from deepfake technology, a software that enables the production of fake visual and audio content by placing a person's facial image on another person's body. The developing deepfake technology allows the production of videos that look so realistic that people cannot easily distinguish them with their sense organs. In addition, any person can easily produce instant fake content with mobile applications and tools that are open to everyone's access and use. Deepfake technology has the potential to seriously interfere with fundamental rights and freedoms, and there is a risk of being used to commit many crimes. When fake content is produced with deepfake technology, this fake content; It can be used to humiliate, insult, threaten or defraud a person. Fake news or videos created with deep fake technology can also be used to manipulate audiences or election results with information disinformation. Therefore, deepfake technology is also dangerous for the right of access to accurate and reliable information. In addition, when the camera footage, which is an important evidence tool in criminal procedure, is manipulated with deepfake technology, there is a risk of obscuring the evidence and preventing justice. In the study, the question of whether the current regulations in Turkish criminal law are sufficient in the face of the dangers and damages brought by deep fake technology is open to discussion.

Fifthly, the section titled "Artificial Intelligence Based Risk Assessment Tools in Criminal Procedure and Their Legal Effects" was penned by Atty. Ozan Can Özbalçık- Istanbul Bar Association-IT Law Commission-AI WG, and Istanbul University- Public Law PhD Candidate. As developments in the field of machine learning and artificial intelligence accelerate, the use of such fields in the criminal justice process is also becoming widespread. At the stage reached in today's world, artificial intelligence-based risk assessment tools are used for many purposes such as predicting crime or perpetrator, probability of a defendant's absence or recidivism during trial. Although such tools seem to assist the decision-makers with their critical decisions, they also pose threats to the aims of criminal justice and various safeguards of the criminal law. In this article, it has been put forward which stages of the

criminal procedure the risk assessment tools are used at, and the benefits they might provide, along with suggested solutions by addressing the problems that may arise regarding the issues such as discrimination, fair trial, right to liberty and the impartiality of the judge.

Finally, the section titled “Autonomous Weapon Systems Using Artificial Intelligence and War Crimes” was penned by Ceren Özbek- Tübingen Eberhard Karls University, postgraduate, and Hilâl Nur Şarbak- Istanbul Bilgi University, International Law Department Research Assistant, and Galatasaray University Public Law, PhD Candidate. Military use of Artificial Intelligence (AI) enabled weapon systems are becoming the new paradigm in ongoing armed conflicts all over the world. While AI-enabled weapon systems called "Autonomous Weapon Systems" (AWS) are being developed and proliferated very rapidly for military purposes, existing international law regarding their use in armed conflicts are insufficient and vague. This paper evaluates the international rules regarding the military use of AI in terms of war crimes. In this regard, the paper consists of three main parts. The first part defines the concepts of AI and AWS. The second part focuses on the issue of accountability and responsibility gap under international law if the prohibition of war crimes is violated by AWS. The third and last part examines the proposals addressing the responsibility gap.

Yapay Zekâlı Otonom Varlıkların Dahil Olduğu Suçlarda Önerilen Suç Sorumluluğu Modelleri

Arş. Gör. Baran Kızılırmak

Giriş

Yapay zekâlı otonom varlıkların dahil olduğu suçlarda, sorumluluğun belirlenmesine yönelik öğretide farklı görüş ve modeller ileri sürülmektedir. Bu çalışmada, önerilen modeller ana hatlarıyla değerlendirilmeye çalışılmaktadır.

Yapay zekânın kullanıldığı otonom varlıklar çeşitli biçimlerde suça dahil olabilirler: Kendisini programlayan ve eğiten kişiler tarafından araç olarak kullanılabilir, "hacklenerek" bir suçun işlenmesinde kullanılabilir yahut istenmeyen bir çıktı üreterek, bir suça neden olabilir; yani nedensellik bağının bir noktasında yer alabilirler. Üçüncü olasılık bu varlıkların programlanması ve eğitilmesi aşamalarındaki bir hatadan kaynaklanabileceği gibi, onların dış dünyayla etkileşimde bulunarak *öğrenmeleri* sonucunda veya bu varlıkların otonom özellikleri nedeniyle ortaya çıkabilir.

Çalışmada **yapay zekâ**dan ziyade **otonom varlık** terimini vurgulamayı tercih etmekteyiz. Zira konunun ceza hukuku bakımından tartışılmasının temelinde, bu varlıkların otonomlukları ve önceden tahmin etmesi güç biçimde çıktılar üretmeleri yer almaktadır. Gerçekten, makine öğrenmesinin temelinde makinenin mevcut koşullara uygun olarak kendi çözümlerini üreteceği varsayımı yer alır, onu programlayanların veya kullanıcıların olası tüm çıktıları öngörmeleri mümkün değildir[1]. Deterministik sistemlerin aksine, otonom varlıklara tüm olası durumlar için önceden yemek tarifi verircesine talimat vermek mümkün değildir[2]. Örneğin birçok sensör aracılığıyla veri toplayarak bunları işleyen ve duruma en uygun kararı vererek bunu uygulayan sürücüsüz araçlarda, farklı seviyede otonomluk dereceleri mevcut olup; bu

[1] Sabine Gless / Emily Silverman / Thomas Weigen, "If Robots Cause Harm, Who Is To Blame? Self-Driving Cars and Criminal Liability", New Criminal Law Review, C. 19, S. 3, 2016, s. 414; Susanne Beck, "Intelligent Agents and Criminal Law—Negligence, Diffusion of Liability and Electronic Personhood", Robotics and Autonomous Systems, C. 86, 2016, s. 138; Sebastian Lohsse / Reiner Schulze / Dirk Staudenmayer, "Liability for Artificial Intelligence", Liability for Artificial Intelligence and the Internet of Things: Münster Colloquia on EU Law and the Digital Economy IV, Ed: Sebastian Lohsse / Reiner Schulze / Dirk Staudenmayer, Nomos Verlagsgesellschaft, 2019, s. 12.

[2] Beck, "Intelligent Agents", s. 138.

araçların sevk ve idaresini doğrudan doğruya sürücü (aracın otonomluk seviyesine bağlı olarak) gerçekleştirmemektedir[3].

Özel hukukta kullanılan kimi sorumluluk modelleri, otonom varlıkların dahil olduğu suçlarda sorumluluğun belirlenmesini kolaylaştırmaktadır. Öte yandan ceza sorumluluğunun temelinde bir kimsenin kusurlu olarak, hukuk tarafından korunan bir hak veya menfaati ihlal etmesi yer alır. Özellikle makinenin arkasındaki kişilerin ceza sorumluluğu, kendilerinden beklenen davranışların ve dolayısıyla öngörülebilirliğin kapsamıyla doğrudan ilgilidir. Burada ceza hukuku yanıtı güç kimi sorularla karşılaşmaktadır: Var olan ceza hukuku normları, mevcut ve gelecekteki olası sorunları adil biçimde çözmeye yeter mi? Otonom varlıkların kendi sorumluluğu olabilir mi? Onlara pragmatik amaçlarla hukuki kişilik tanınmalı mıdır? Makinenin arkasındaki kişilerin neleri öngörerek davranmaları hukuken kendilerinden beklenebilir? Suçlayacak kimse yoksa, otonom varlıkların dahil olduğu suçların cezasız kalması olası mıdır?

Bu soruları yanıtlamak ve otonom varlıkların dahil olduğu suçlardaki ceza sorumluluğunu belirlemek amacıyla, temelini özel hukuktan alan kimi yöntemler öğretide önerilmektedir. Bu yöntemlerin ortak noktası gerek teorik bakımdan kapsamı gerekse uygulamada ispatındaki güçlükleri göz önünde bulundurarak kusura dayalı sorumluluğu esnetmeleri veya onu bypass ederek, bir faraziye ile pragmatik çözümler ileri sürmeleridir.

1. Otonom Varlıklara Hukuki Kişilik Tanınması ve Kendi Ceza Sorumlulukları

Yapay zekâlı otonom varlıkların hukuki statüsüne ilişkin tartışmalar, onlara hukuki kişilik tanınmasına ve hatta kendi ceza sorumluluklarına kadar uzanmıştır. Mevcut ve yakın gelecekte doğabilecek sorunlara pragmatik çözümler üretebilmek adına, onlara yapay insan ve kölelik gibi statülerin yanı sıra elektronik kişilik gibi hukuki kişiliklerin tanınması önerilmiştir.

Hukuki kişilik önerilerinin başında gelen elektronik kişilik üzerinde özellikle Avrupa'daki çalışmalarda durulmuştur. Konuya ilişkin ilk önerilerden biri *euRobotics*'in 2012 yılındaki raporunda yer almaktadır[4]. Ardından devam eden tartışmalar sonucunda, Avrupa Parlamentosu tarafından gelişmiş otonom robotlara uzun vadede elektronik kişilik tanınarak verecekleri zararlardan (tazminat bakımından)[5] sorumlu tutulmaları 2017 yılının başında

[3] Eylem Aksoy Retornaz, "Otonom Araçlar ve Ceza Hukuku", Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ, Ed.: E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk, On İki Levha Yayıncılık, 2021, s. 331; Mesut Serdar Çekin, "Otonom Araçlar ve Hukuki Sorumluluk", TAAD, S. 33, 2018, ss. 285-287.

[4] J.P. Günther, E. May, F. Münch, S. Löffler, S. Beck, E. Hilgendorf, "Exploration track: non-human agents and electronic personhood", Suggestion for a green paper on legal issues in robotics, Ed: C. Leroux, R. Labruto, euRobotics, The European Robotics Coordination Action, 2012, ss. 58-64. https://www.researchgate.net/publication/310167745_A_green_paper_on_legal_issues_in_robotics (çevrim içi, E.T.: 20.11.2021 13:00).

[5] Raporda özel hukuk – ceza hukuku sorumluluğu ayrımına değinilmemiş olmakla birlikte, ceza sorumluluğuna ilişkin ayrıca bir belirleme yapılmamış ve ürün sorumluluğu, objektif sorumluluk gibi özel hukuk sorumluluk türlerinin üzerinde durulmuştur. Bkz.: European Parliament, Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), Committee on Legal Affairs, 27.01.2017

önerilmiştir[6]. Bu öneri, her ne kadar gelecekte otonom varlıkların daha sofistike olabileceği varsayımı üzerinden onlara uzun vadede elektronik kişilik tanınmasına yönelik olsa da; geçtiğimiz dört yıl içerisinde bu fikir pek çok uzman tarafından, otonom varlıkların henüz bu aşamada olmadığı gerekçesiyle eleştirilmiş ve elektronik kişilik tartışmaları bir hukuki metin oluşmadan şimdilik rafa kalkmıştır.

Literatürde, önerdiği modeller üzerinde sıklıkla durulan Hallevy'e göre[7], yapay zekâlı otonom varlıklar suçun unsurlarını karşılayacak biçimde suç işleyebilir, suç faili olabilirler[8]. Ceza hukukunun başta insanları konu edinerek ortaya çıktığını; fakat 17. yüzyıldan beri ceza sorumluluğunun artık yalnızca insanlar için olmadığını ifade eden ve Amerikan hukuku eksenli bir yaklaşımda bulunan yazara göre, bu bariyerin tüzel kişiler bakımından aşılmış olması, otonom varlıklar için de aşılabileceğini göstermektedir[9]. Gerçekten, Roma hukukuna dayanan ve gerçek kişilerin aksine tüzel kişilerin suç faili olamayacağını ifade eden *societas delinquere non potest* ilkesi, özellikle Anglo-Sakson hukukunu benimseyen ülkelerde terk edilmektedir[10]. Bu gelişimin bir sonucu olarak günümüzde ve yakın gelecekte otonom varlıkların da bir hukuki kişiliğe sahip olabileceği, suç faili olmasının yanı sıra; kendi ceza sorumluluklarının dahi olabileceği bu şekilde ileri sürülmektedir.

Yapay zekâlı otonom varlıklara hukuki kişilik tanınması durumunda, makinenin arkasındaki kişinin de ceza sorumluluğuna sahip olup olmayacağı ve bunun başkasının fiilinden sorumluluk (**Ing**. *vicarious liability*) olarak değerlendirilip değerlendirilemeyeceği tartışılmaktadır. Hallevy, günümüzdeki anlayışta tüzel kişinin organlarının *ultra vires* olsun veya olmasın, suçun hem maddi hem de manevi unsurunu gerçekleştirebildiğini; dolayısıyla tüzel kişiliğin doğrudan sorumluluğa sahip olduğunu ifade etmekte[11] ve benzer bir durumu yapay zekâya sahip otonom varlıklar bakımından da önermektedir[12]. Bir başka ifadeyle, yazar belli özelliklere sahip yapay zekâlı otonom varlıkların suçun hem maddi hem de manevi unsurunu gerçekleştirebileceğini, bu durumda kendi ceza sorumluluğunun da mevcut olması

---

https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf , s. 7. (çevrim içi, E.T.: 20.11.2021 13:00).

[6] A.e., s.18.
İfade etmek gerekir ki, raporun taslak metninde gelişmiş otonom robotların belirli hak ve yükümlülüklere sahip olması da önerilmekteydi; ancak bu ifade asıl raporda yer bulmamıştır: European Parliament Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), Committee on Legal Affairs, 31.05.2016 https://www.europarl.europa.eu/doceo/document/JURI-PR-582443_EN.pdf?redirect , s. 12. (çevrim içi, E.T.: 20.11.2021 13:00).

[7] Burada belirli bir yazarın görüşlerini detaylandırma nedenimiz, tespit edebildiğimiz kadarıyla, yazarın yapay zekâlı otonom varlıkların suç faili olabileceğini ve ceza sorumluluğu tanınabileceğini net bir şekilde savunarak öğretide ileri sürülen görüşleri etkilemiş olmasıdır.

[8] Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer International Publishing, 2015, s. 131.

[9] Hallevy, a.g.e., ss. 42-43, 103.

[10] Pedro Miguel Freitas / Francisco Andrade / Paulo Novais, "Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible", AI Approaches to the Complexity of Legal Systems, Ed. Pompeu Casanovas vd., Lecture Notes in Computer Science, Heidelberg: Springer, 2014, s. 147.

[11] Hallevy, a.g.e., s. 42.

[12] A.e., s. 130.

gerektiğini ifade etmektedir[13]. Üstelik, bu şekilde işlenen suçlarda otonom varlıkların yalnızca kasıtlı değil; belli koşulların karşılanması hâlinde, insanlarınkine benzer biçimde taksirli de olabileceğini ileri sürmektedir[14].

Kimi yapay zekâlı otonom araçlara hukuki kişilik tanınması, âdeta onun arkasındaki gerçek kişilerin ve hukuki sorumluluklarının bu faraziyede ele alınmasını sağlamaktadır. Üstelik kimi otonom varlıklar fiziksel varlığı haiz olarak insanlarla etkileşime geçebildiğinden bu, şirketlerdeki gibi tam anlamıyla bir faraziye değildir. Bununla birlikte, ifade edildiğinin aksine [15] yapay zekâlı otonom varlıklara hukuki kişilik tanınmasının, onun hatalı çalışmasında kusuru olan gerçek kişilerin (özellikle taksirli) sorumluluğuna engel olmayacağı görüşü Avrupa'da taraftar bulmaktadır[16].

Öğretideki aksi yöndeki görüşlere göre, elektronik kişilik tartışmaları temelini esasen özel hukuktan ve haksız fiil sorumluluğundan almakta ve bir "hukuk oyunu" ile, tazminat talepleri için bir muhatap tayin etmektedir. Bu, özel hukuk için orijinal ve pragmatik bir fikir olsa da ceza hukukunun amacı zararın ödenmesini garanti altına almak olmadığından, uygulama alanı bulamayacaktır[17]. Gerçekten, yapay zekâlı otonom varlıklara kişilik tanınmasına ilişkin tartışmalar, bir ölçüde yapay zekânın insana benzetilme çabasının bir sonucudur. Bununla birlikte, öğrenme, düşünme, karar verme, acı çekme gibi insana has özelliklerin yapay zekâlı otonom varlıklarda bulunup bulunmayacağı bugün bilinemediğinden[18], bu öncüllerden yola çıkan argümanlar tatmin edici değildir.

Günümüzde, makine öğrenmesinin ve yapay zekâlı varlıkların oldukça şaşırtıcı ve insanlar tarafından gerçekleştirilmesi mümkün olmayan işler yaptıklarına tanık olunsa da -makine öğrenmesinin tabiatını da göz önüne alarak- başarısız işler ön plana çıkmadığından, bu hayret duygusunun bir ölçüde yanlılığa dayandığı ve yapay zekânın henüz erken aşamalarında olunduğu unutulmamalıdır. Nitekim, yapay zekâlı otonom varlıkların bir nevi öğrenme ve karar verme kapasitesinden söz edilebilirse de doğru ve yanlışı ayırt etme yetisinin yanı sıra, günlük yaşam tecrübesinden büyük ölçüde yoksunlardır[19]. Bugün için kendi özerk yapılarını,

---

[13] A.e., s. 131.

[14] Hallevy, kendisine gelen bilgiyi işleme, gerekçelendirerek makul bir karar verme gibi pek çok durumda insan ve yapay zekâlı otonom varlıklar arasında benzerlik kurmaktadır. Bu varlıkların taksirli sorumluluğundan söz etmek için en azından gerekli kapasiteye sahip olması gerekir, bunun başında da algılama (Ing. *awareness*) gelir. Fakat algılama aşamasında kusurlu olunması hâlinde de taksirli sorumluluğundan söz edilebilecektir (Yazar *awareness* terimini, *dışarıdan gelen verilerin alınarak bunların genel bir imgesinin beyinde oluşması*nı ifade etmek üzere kullanmaktadır. Bu ifadeyi aynı bağlamda Türkçe'de tam olarak karşılayan bir sözcük bulamasak da buna en yakın ifadenin *algılama* olduğunu düşünerek bu sözcüğü tercih ettik). Bkz.: Hallevy, a.g.e., ss. 124-127, 131.

[15] Hallevy, a.g.e., s. 41.

[16] Beck, "Intelligent Agents", ss. 141-142; Freitas vd., a.g.e., s. 151.

[17] Monika Simmler / Nora Markwalder, "Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence." Criminal Law Forum C:30, S:1, 2019, ss. 19-20.

[18] Zeynel Kangal, Yapay Zekâ ve Ceza Hukuku, On İki Levha Yayıncılık, 2021, ss. 47-48.

[19] Fiziksel akıl yürütme konusunda GPT-3'ün tamamlanması beklenen metin buna örnek gösterilebilir, (kendisine verilen metni GPT-3 italik yazılı kısım ile tamamlamıştır):

geçmişlerini, hak ve borçları olduğunu anlama yeteneklerinin mevcut olduğunu söylemek mümkün değildir[20]. Ahlaki değerlendirme sistemleri olmaksızın, onları kınamak ve cezalandırmak bir anlam ifade etmeyecektir[21]. En azından bugünün ceza hukuku, bu arayışın yanıtını vermemektedir. Elektronik kişiliğinse bu varlıkların ancak bir gün kendi varlığının ve bilincinin farkında olması durumunda tanınabileceği ileri sürülmektedir[22]. Kanımızca en azından günümüzde, otonom varlıkların suçun unsurlarını karşılayabilecek şekilde suç işlemesi mümkün değildir. Onların otonomluklarını göz önünde bulundurarak, üretim anından son kullanıcının tasarrufunda geçirdiği zamana dek tüm süreçte gerçek kişilerin kusurlu davranıp davranmadıklarına odaklanmak gerekmektedir. Gerçekten tıpkı hayvanlarda olduğu gibi, söz konusu otonom varlıklarda da fiil insana atfedilebildiği ölçüde önem taşır. Dolayısıyla otonom varlıkların suçu kendilerinin işlemesinden ve ceza sorumluluklarından bugün için bahsedilmesi mümkün değildir[23]. Bununla birlikte, hızla ilerleyen teknoloji karşısında yirmi yıl sonrasını dahi öngörmek zordur, dolayısıyla bu tartışmaların devam etmesi ceza hukukunun gelişimi için önem arz etmektedir.

2. Dolaylı Faillik

Otonom varlıkların dahil olduğu suçlarda uygulanması önerilen modellerden biri de dolaylı failliktir (**Ing**. *perpetration through / by another*)[24]. Öneriye göre, makinenin arkasındaki gerçek kişinin, otonom varlığı kasıtlı olarak işlemek istediği suçta kullanması durumunda dolaylı faillik kurumuna başvurulabilir.

Otonom varlığın bir suçta kullanılması farklı biçimlerde gerçekleşebilir. Örneğin, sürücüsüz bir aracın hız sınırını aşarak diğer araçlara çarpması amacıyla, yol kenarındaki trafik levhasının insanlar tarafından kolayca anlaşılmayacak; fakat araç tarafından 35 yerine 85 km.

"Küçük bir akşam yemeği partisi veriyorsun. Yemeği salonda sunmak istiyorsun. Fakat akşam yemeği masası kapı aralığından daha geniş. Masayı salona sokmak için *kapıyı ortadan kaldırman gerekiyor. Bir masa testeren var, böylece kapıyı ikiye bölüyorsun ve üst yarısını çıkarıyorsun."* Örnek için: İzlem Gözükeleş, "Yapay zekâ kime hizmet edecek?", Bilim ve Gelecek, S:199, 2020.

[20] Gless vd., a.g.e., s. 416.

[21] A.e., s. 422.

[22] Hasan Aksoy, "Yapay Zekalı Varlıklar ve Ceza Hukuku", International Journal of Economics, Politics, Humanities & Social Sciences, C:4, S:1, 2021, s. 24.

[23] Aksoy Retornaz, a.g.e., s. 339.
Öğretide bir görüş, hareket ve fiil kavramı ayrımı üzerinden, otonom varlıkların "hareketlerinin" ceza hukuku bakımından maddi unsuru karşılayıp karşılamayacağını tartışarak, onlara her halükârda kusur atfedilemeyeceğinden, kendi ceza sorumluluklarının olamayacağını belirtmektedir. Tuba Kelep Pekmez, "Otonom Araçların Kullanımından Doğan Cezaî Sorumluluk: Türk Hukuku Bakımından Genel Bir Değerlendirme", Ceza Hukuku ve Kriminoloji Dergisi, C. 6, S. 2, 2018, ss. 182-185.

[24] Öneriyi ileri süren Halleyv (a.g.e. s. 144 vd.), otonom varlıkları *bir başkası* olarak değerlendirerek *başkasının fiilinden sorumluluğa* da değinmişse de kanımızca açıkladığı hususu Türk hukukundaki dolaylı faillik kurumu karşılamaktadır. Aynı yönde: Sinan Altunç, "Yapay Zekâ ve Ceza Hukuku Sorumluluğu", Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ, Ed.: E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk, On İki Levha Yayıncılık, 2021, ss. 354-355.

olarak algılanacak biçimde değiştirilmesi durumunda[25] onun otonomluğundan da yararlanarak bir suç işlenmesinde kullanılmaktadır[26]. Benzer bir örnek sürücüsüz aracı programlayanların, aracın yayalara çarpması amacıyla, programlama ve eğitim aşamasında yaya yolunda yol vermeye ilişkin hiçbir verinin yüklememesinde karşımıza çıkar. Burada araç, yaya yoluna ilişkin kurallar dışındaki tüm trafik kuralları bilgisi ve eğitimiyle donatılmış olup, onun -somut olayın koşullarına göre muhtemel veya muhakkak bir netice olan- insanlara çarpması istenmekte; diğer bir deyişle bu amaç için kullanılmaktadır. Dikkat edilmelidir ki, her iki örnekteki suçlar da kasıtla işlenmektedir. O hâlde, otonom varlıkların bu şekilde suç işlemekte kullanıldığı hâllerde dolaylı faillik kurumunun uygulanabilirliği üzerinde durulmalıdır.

Bu modelin savunucularına göre, yapay zekâlı otonom varlıklar masum aracı (**Ing**. *innocent agent*)[27] konumunda olup, asıl ceza sorumluluğu onları suç işlemekte kullanan kişilere aittir. Bu varlıklar suçun fiziksel olarak işlenebilmesi için gerekli kapasiteye sahip olsa da algılama yeteneği veya iradesi olmayan türleri ceza hukuku bakımından fail olamazlar; ancak akıl hastalarına veya çocuklara benzetilebilirler. Bu durumda onları araç olarak kullanarak suç işleten kişiler dolaylı fail olarak sorumlu tutulur[28]. Buna verilen örnek, yapay zekâya sahip bir otonom robotun gece kimse yokken fabrikayı yakmasının programlanması yahut sahibinin emirlerini yerine getirmeye programlı yapay zekâlı bir robotun, sahibinin eve zorla girmeye çalışanlara saldırması yönündeki talimatıdır[29]. Yapay zekâlı otonom varlıkların, arkasındaki kişilerin iradesinden bağımsız olarak, kendi öğrendikleri ve tecrübesi nedeniyle bir suç işlemesi hâlinde ise dolaylı failliğin uygulanmayacağı belirtilmektedir[30].

Dolaylı faillikte, masum aracının sorumlu olup olmadığından bağımsız olarak, arka plandaki kişi davranış kendisininmişçesine ve yalnızca kasıtla sorumlu olabilir[31], masum aracınınsa ceza sorumluluğu olmadığı kabul edilir[32]. Bununla birlikte, suç işlemekte kullanılanın kimi zaman *masum* değil, *yarı masum aracı* (**Ing**. *semi-innocent agent*) konumunda olabileceği ve yapay zekâlı otonom varlıkların da bu kapsamda değerlendirilebileceği ileri sürülmektedir[33].

---

[25] Catie Keck, "How a Piece of Tape Tricked a Tesla Into Reading a 35MPH Sign as 85MPH", https://gizmodo.com/how-a-piece-of-tape-tricked-a-tesla-into-reading-a-35mp-1841791417 (çevrim içi, E.T.: 20.11.2021 13:00).

[26] Benzer örnekler için bkz.: Calo vd., "Is Tricking a Robot Hacking?", Berkeley Technology Law Journal, C. 34, S. 3, 2019, s. 910 vd.

[27] Masum aracı terimi için bkz.: Murat Önok, Yapısal Suçlarda Failin Tespiti: Müşterek Suç Girişimi (Joint Criminal Enterprise) ve Örgütsel Hakimiyete Dayalı Dolaylı Faillik Doktrinleri, Seçkin Yayıncılık, 2019, s. 237. Burada *araç olarak kullanılan kişi* yerine *masum aracı* ifadesini benimsememizin nedeni, dolaylı faillik modelini önerenlerin terminolojisine sadık kalmanın yanı sıra, *otonom varlıkların araç olarak kullanılmasının* başka bir hususu ifade etmek üzere kullanılmasıdır.

[28] Hallevy, a.g.e., ss. 109–110; Altunç, a.g.e., ss. 354-355.

[29] Hallevy, a.g.e., ss. 110-111.

[30] Freitas vd., a.g.e., s. 150; Hallevy, a.g.e., s. 111.

[31] Önok, a.g.e., ss. 237-238, 284.

[32] Hallevy, a.g.e., s. 133.

[33] Bunun için yapay zekâlı otonom varlıkların taksirin koşullarını yerine getirebilecek kapasiteye sahip olması gerekmektedir. Bu kapasitenin mevcudiyetine ek olarak, benzer bir durumda makul bir kişinin ilgili veriyi algılayabilecek olması ve yapay zekâlı otonom varlığın somut olayda bu veriyi algılamamış olması gerekir.

Yarı masum aracıya şu örnek gösterilmektedir: Hemşirenin düşmanı olan ve öldürmek istediği hasta ameliyat edilecektir. Hemşire aletlere enfeksiyona neden olacak bir bakteri bulaştırır. Ameliyata başlamadan önce, cerraha kullanılacak aletleri sterilize ettiğini ve bunun kendi sorumluluğu olduğunu söylemesi üzerine cerrah normal şekilde ameliyatı gerçekleştirir. Ameliyattan bir süre sonra hasta enfeksiyondan ölür. Cerrahın hukuki yükümlülüğü kapsamında ameliyattan önce aletlerin sterilize edildiğinden emin olmasının yer aldığı düşünüldüğünde, cerrah bir masum aracı değil; yarı masum aracı konumundadır ve taksirli sorumluluğu mevcuttur[34].

Yapay zekâyı programlayan kişinin onu belirli bir suçu işleyecek şekilde eğittiği durumlarda programcının dolaylı fail olarak sorumlu olabileceğini, bu durumda yapay zekâlı otonom varlığın herhangi bir bilişim sisteminden veya tornavidadan farkı olmayacağı ifade edilmektedir[35]. Kanımızca bu söylem iki açıdan hatalıdır. İlk olarak otonom varlığın belirli bir şekilde, deterministik olarak davranmasının programlanabildiği durumlarda onun otonomluğundan söz etmeye gerek yoktur, burada herhangi bir tartışmaya gerek olmaksızın arkadaki kişinin doğrudan ceza sorumluluğu olmalıdır. Dahası, tornavida gibi bir aletin araç olarak kullanıldığı suçlarda dolaylı faillikten söz etmek mümkün değildir; aksi yaklaşım bu aletlere sınırlı da olsa bir irade ve ceza hukuku anlamında fiil gerçekleştirme kapasitesi tanımak anlamına gelecektir. Kaldı ki, söz konusu aletler otonom olsa dahi, bunların belirli amaçlarla suç işlemekte kullanılması durumunda yine de dolaylı faillikten söz edilemeyeceği kanaatindeyiz.

Bizim anladığımız şekliyle dolaylı faillikten söz edebilmek için arka plandaki kişinin, bir başka kişiyi[36] kendi işlemek istediği suç için araç olarak kullanması gerekir[37]. Burada önemli olan arka plandaki failin bir başkasının fiziksel bedenini değil; davranışlarını araç olarak kullanması, onun davranışları[38] ve iradesi üzerinde hakimiyet kurmasıdır[39]. Cansız nesnelerin araç olarak kullanılmasında dolaylı faillikten söz edilemez[40]. Dolaylı faillik yalnızca kusur

---

Hallevy, a.g.e., s. 133. Ayrıca bu varlıkların taksirli sorumluluğu için bkz. yuk.: §2. Otonom Varlıklara Hukukî Kişilik Tanınması ve Kendi Ceza Sorumlulukları.

[34] Hallevy, a.g.e., s. 132.
Bu örnekte insan öldürme suçunun taksirli şekli düzenlendiğinden taksirle sorumluluk mümkündür. Ancak örneğin mala zarar verme suçunun taksirli şekli düzenlenmediğinden, yarı masum aracının ceza sorumluluğu olmayacaktır. Meral Ekici Şahin, "Dolaylı Failliğin Ortaya Çıkış Biçimleri", BÜHFD, C: 8, S: 107-108, 2013, ss. 76-77.

[35] Hallevy, a.g.e., s. 118.

[36] 5237 sayılı Türk Ceza Kanunu'nun 37. maddesinin 2. fıkrasında dolaylı faillik "[s]uçun işlenmesinde bir başkasını araç olarak kullanan kişi de fail olarak sorumlu tutulur" denilmek suretiyle düzenlenmiştir. 26.09.2004 tarih ve 5237 sayılı Türk Ceza Kanunu, (R.G. no: 25611, 12.10.2004).
Benzer şekilde Alman Ceza Kanunu (StGB) § 25 (1): "Suçu, başkası aracılığıyla ya da kendisi işleyen kimse fail olarak cezalandırılır."

[37] Hasan Sınar, "Türk Ceza Hukukunda Dolaylı Faillik", CHD, S: 15, 2011, s. 59.

[38] Ekici Şahin, a.g.e., ss. 66-67.

[39] Önok, a.g.e., s. 221.
Bu durum, 5237 sayılı Türk Ceza Kanunu'nun 37. maddesinin gerekçesinde de "*arka plandaki kişi, suçun icraî hareketlerini gerçekleştiren şahsın ve hareketinin üzerinde hâkimiyet kurmaktadır*" şeklinde belirtilmektedir.

[40] Ekici Şahin, a.g.e., ss. 66-67.

yeteneği olmayanların araç olarak kullanılmasında değil; aynı zamanda kişiyi zorlayarak fiili üzerinde hakimiyet kurulması, hataya düşürülmesi yahut hatasından yararlanılması gibi durumlarda da söz konusu olur[41]. Bununla birlikte, mutlak kuvvet uygulanarak masum aracının iradesi adeta devre dışı kalmış ve bir nesne konumuna indirgenmişse, burada artık dolaylı faillikten söz edilemez[42]. Bu nedenlerle, otonom varlıkların suç işlemekte kullanılması hâlinde kanımızca, 1- iradeye sahip olmadıkları için, 2- gerçekleştirdikleri "şey" ceza hukuku anlamında fiil olarak kabul edilemeyeceği için, 3- insan olmadıkları için dolaylı faillikten söz etmek mümkün değildir.

Otonom varlıkların iradeye sahip olup olmadığı ve ceza hukuku anlamında bir fiil gerçekleştirip gerçekleştiremeyecekleri bu çalışmanın kapsamını aşmaktadır. Yalnızca şunu belirtmek gerekir ki, (kabul edilen teoriye göre) fiilin klasik anlamdaki bedensel boyutu göz ardı edilse bile hem iradi davranış ölçütü bakımından hem de sosyal uygunluğu bakımından yapay zekâlı otonom varlıkların bugün için gerçekleştirdiği şeyin fiil olduğunu söylemek güçtür[43]. Yine de gelecekte yapay zekâlı varlıkların kapasitelerinin ve otonomluklarının artmasıyla fiil kavramına bakışımızın değişmesi mümkündür.

Son olarak, dolaylı faillikten söz edilebilmesi için günümüzde hem öğreti hem de yasada kabul edilen anlayış "bir başkasının" insan olması gerektiği yönündedir. Bu, neler olduğunu anlayabilecek, başka türlü davranmayı da seçebilecek bir kişi olmalıdır[44]. Bugün için dolaylı faillikten söz edilemeyeceğini belirten, fakat bu kapıyı da tamamen kapamayan bir düşünceye göre; gelecekte yapay zekâlı otonom varlıkların insana benzer şekilde yeterince gelişmiş, sofistike ve girift olmaları; etraflarında neler olduğunu algılayabilme ve buna uygun davranabilme kapasitelerine sahip olmaları durumunda dolaylı faillik tartışmaları bir anlam ifade edecektir[45]. Kanımızca masum aracının insan olma koşulu aranmasa ve hatta otonom varlıkların ceza hukuku anlamında fiil gerçekleştirebileceği kabul edilse bile, bu tartışmanın anlamlı olabilmesi için belli düzeyde iradeye sahip olmaları gerekecektir.

3. Muhtemel Sonuçtan Sorumluluk (*The Natural-Probable-Consequence Liability*)

Bu modeli öneren Hallevy'e göre, yapay zekâlı otonom varlıkların dahil olduğu, işlenmesi amaçlanmasa da gerçekleşen suçların cezasız kalması olasılığı bu model ile bertaraf edilebilir [46]. Buna göre, başlangıçta otonom varlık kullanılarak işlenmesi amaçlanan bir suç vardır; fakat sonuçta, aynı suç planlanandan daha fazla sayıda yahut bu suçtan başka veya daha ağır suç(lar) da işlenmiştir. Modele göre, başlangıçta amaçlanmayan diğer suçların, amaçlanan fiil

[41] Önok, a.g.e., ss. 249-308; Sınar, a.g.e., ss. 62-74.
[42] Önok, a.g.e., ss. 253-254.
[43] Gless vd., a.g.e., s. 419; Dafni, Lima, "Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law." South Carolina Law Review, C:69, 2018, s. 682.
Yapay zekâlı otonom varlıkların ceza hukuku anlamında fiil gerçekleştirip gerçekleştiremeyeceğine ilişkin tartışma için bkz.: Kelep Pekmez, a.g.e., ss. 182-184.
[44] Lima, a.g.e., s. 690.
[45] A.e.
[46] Hallevy, a.g.e., s. 116.

bakımından tabii olası bir suç olup olmadığı değerlendirilerek programlayanın taksirli sorumluluğu ele alınmalıdır[47].

Bu modelin uygulanması için öncelikle diğer suçların, planlanan suçun sonucu olması ve gerçekleşmesinin başlangıçta sübjektif olarak öngörülebilir olması gerekir[48]. Bu durumda, programlayan kişinin hem planlanan hem de planlanmayan suçtan sorumluluğu olacaktır[49]. Bununla birlikte planlanmayan suç, güçlü yapay zekâlı ve gelişkin otonom bir varlığın etkisiyle işlenmişse, programlayanınkine ek olarak onun da ceza sorumluluğu olacaktır[50]. Eğer hiçbir suçun işlenmesi planlanmamışsa; fakat otonom varlık yine de bir suça neden olmuşsa bu model uygulanmayacaktır[51].

Kanımızca bu modele, her ne kadar Amerikan hukukundan yola çıkarak farklı bir isim verilse de özünde neticesi sebebiyle ağırlaşan suçtan ve şeriklerin planlanan suçun dışına çıkmasından farklı bir hususa karşılık gelmemektedir. Bu bağlamda, bir sonraki başlıkta ele alınacak olan makinenin arkasındaki gerçek kişilerin ceza sorumluluğundan farklı bir sonuca da ulaşmamaktadır. Nitekim yazar bu model ile yapay zekâlı otonom varlıkların arkasındaki kişilerin daha dikkatli ve özenli olması amacıyla caydırıcılığın sağlanması gerektiğini ifade etmektedir[52].

4. Makinenin Arkasındaki Kişinin Kasıtlı ve Taksirli Sorumluluğu

Otonomluk içermeyen herhangi bir ürünün dahi öngörülmeyen biçimde zararlı bir sonuca neden olduğu durumlarda sorumluluğunun tespitinin zorluğu karşısında[53], öngörülemez çıktılar üretebilen yapay zekâlı otonom varlıkların dahil olduğu suçlarda gerçek kişilerin ceza sorumluluğunun belirlenmesi birçok açıdan güçtür. Gerçekten, yapay zekâlı otonom varlıkların programlanması, veri setleriyle eğitilmesi, üretilmesi, piyasaya sürülmesi, kullanılması, farklı sensörler ve kaynaklar aracılığıyla elde edilen verilerin işlenerek çıktı üretilmesi, denetimi ve geliştirilmesi aşamalarının her birinde istenmeyen bir sonucun gerçekleşmesine neden olabilecek sayılamayacak kadar çok olasılık vardır. Bunların her birinde yer alan gerçek kişilerin (tasarlayan, programlayan, geliştiren, üreten, satan veya kullananlar) ortaya çıkan suç bakımından kasıtlı yahut taksirli sorumluluklarının belirlenmesi önemlidir.

---

[47] A.e., ss. 115-120.
[48] A.e., s. 115.
[49] Bu modele örnek olarak, iki kişinin anlaşarak banka soymaya gittiği olayda şeriklerden birinin kararlaştırılan suçun dışına çıkarak güvenlik görevlisini öldürmesi verilmektedir. A.e., s. 113.
[50] A.e., s. 119.
[51] A.e.
[52] A.e.
[53] Örneğin Microsoft Word'ün çökmesi sonucu uzun emeklerle yazılmış bir raporun kaybolmasının sorumlusu var mıdır ve nasıl belirlenmelidir? Programlayanlar benzer tüm sonuçlardan sorumlu tutulabilir mi, yoksa buna kişiler / toplum mu katlanmalıdır? Ryan Calo, "Robotics & The Law: Liability For Personal Robots", Stanford Law School The Center for Internet and Society, 26.11.2009, s. 4, https://ftp.documation.com:8443/references/aba10a/PDfs/2_1.pdf , (çevrim içi, E.T.: 20.11.2021 13:00).

Makinenin arkasındaki gerçek kişilerin kasıtlı sorumluluğunun tespiti görece kolaydır. Örneğin yukarıda yer verilen[54], trafik levhasındaki hız limiti değiştirilerek sürücüsüz aracın kaza yapmasının sağlandığı veya yaya yolu kurallarına ilişkin herhangi bir verinin yüklenmediği sürücüsüz aracın dahil olduğu suçlarda bilme ve isteme koşulları gerçekleşmekte; failler kasıtlı olarak suçu işlemektedir. Dikkat edilmelidir ki, öğretide kasıtlı suçlara verilen örneklerin birçoğu esasen deterministik araçların suç işlenmesinde kullanılmasına ilişkin olup, otonomluğu göz ardı etmektedir[55]. Çalışmanın başında vurgulandığı gibi, ceza hukuku bakımından yanıtı güç sorular yaratan bu varlıkların otonomluğu dolayısıyla olası çıktıların öngörülmesinin güçlüğüdür. Nitekim, günlük yaşamda otonom varlıkların arkasındaki gerçek kişilerin sorumluluğu çoğunlukla taksirli olacaktır.

Taksirli sorumluluğun kaynağı tasarımdan kullanıma dek tüm aşamalardaki olgularla bağlantılı olabilir[56]. Makine öğrenmesi günümüzde son derece gelişmiş olarak pek çok alanda kullanılsa ve insanların yapamayacakları karmaşık işleri hayret uyandıracak biçimde gerçekleştirse de; bunun bedeli girdi ve çıktılar arasındaki ilişkilerin yorumlanmasının güçlüğü; diğer bir söyleyişle, yapay zekânın işleyişinde hangi parametrelerin tam olarak nasıl etkide bulunduğunun, hangi nedenlerle belirli çıktıların oluştuğunun çoğunlukla belirlenememesidir[57]. Diğer yandan, bu varlıkların örüntüleri tanıma ve istenen biçimde çalışmasındaki başarısı, aynı zamanda onun karmaşıklığına ve dolayısıyla açıklanmasındaki güçlüğe de bağlıdır. İşte bu nedenle, otonom varlıkların hangi çıktıları vereceğini, nasıl davranacağını her zaman öngörmek mümkün değildir[58]. Otonom varlıkların her davranışının öngörülmesi gerektiğinin ileri sürülmesi makinenin arkasındaki kişiler bakımından *de facto* olarak kusursuz sorumluluğa yol açacaktır.

Taksirin esasında öngörülebilir olan neticenin dikkat ve özen yükümlülüğüne aykırı olarak öngörülmemesi yer almakta olup, taksirli sorumluluk insanları daha dikkatli ve özenli olmaya sevk eder. Makinenin arkasındaki kişilerden beklenen dikkat ve özen yükümlülüğünün sınırı; özellikle öngörebilmelerinin kapsamının ne olduğunun tespiti, konunun özünü oluşturmaktadır. Gerçekten, otonom varlıkların öngörülmesi güç biçimde üretebildiği çıktılar karşısında, hukuk düzeni makinenin arkasındaki kişilerden tam olarak ne beklemektedir? Örneğin, bir robot süpürgenin olağan çalışması sırasında kir zannederek değerli bir eşyaya zarar vermesi[59] yahut yerde yatan kişinin saçını "süpürerek" onu yaralaması[60] durumunda, bu

[54] Bkz.: yuk.: §3. Dolaylı Faillik.
[55] Örneğin, yapay zekâlı bir robotun kimsenin olmadığı sırada fabrikayı yakmasının programlanması. Bkz.: Hallevy, a.g.e., s. 110.
[56] Beck, "Intelligent Agents", ss. 138-139.
[57] Calo vd., a.g.e., s. 899.
[58] Susanne Beck, "Google Cars, Software Agents, Autonomous Weapons Systems New Challenges for Criminal Law?", Robotics, Autonomics, and the Law: Legal Issues Arising from the AUTONOMICS for Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy, Robotik und Recht 14, Ed: Eric Hilgendorf/Uwe Seidel, Nomos Verlagsgesellschaft, 2017, s. 243.
[59] Lima, a.g.e., s. 691.
[60] Justin McCurry, "South Korean woman's hair 'eaten' by robot vacuum cleaner as she slept", The Guardian, 09.02.2015,

neticelerin onu programlayan ve verilerle eğitenler yahut kullananlar tarafından öngörülmesi beklenebilir mi? Bu durumda temel soru, bu kişilerin ilgili neticeyi öngörebilecek ve engelleyebilecek durumda olup olmadığıdır. Öngörmekle birlikte kayıtsız kalınması, neticenin kabullenilmesi hâlinde ise olası kasıtla sorumluluk gündeme gelecektir[61].

Diğer taraftan yapay zekâlı otonom varlığın dahil olduğu bir suç meydana geldiğinde, istenmeyen bu sonuca neyin yol açtığının retrospektif olarak tespiti, makine öğrenmesinin; özellikle derin öğrenmenin doğası gereği çoğunlukla mümkün olmamaktadır. Dolayısıyla iki husus makinenin arkasındaki gerçek kişilerin taksirli sorumluluğunun belirlenmesini zorlaştırmaktadır: 1- Başlangıçta otonom varlığın bu sonuca yol açabilecek şekilde bir çıktı üretip üretmeyeceğinin öngörülmesi 2- Suç meydana geldikten sonra bunun hangi hatadan kaynaklandığının saptanması. Bunlara uygulamadaki ispat sorunları da eklenecektir. Özellikle açık kaynak kodlu yazılımlarda yahut bir ekip / şirket bünyesinde üretilen yapay zekâ sistemlerinde, hatanın tespitinin güçlüğüne birden çok kişinin fiilinin varlığı da eklenecektir. Bu hâllerde kişilerin dikkat ve özen yükümlülüğü ile sorumluluklarının belirlenmesine yönelik olarak, güven ilkesi üzerinde durulmaktadır[62].

En dikkatlice hazırlanan tasarımlarda bile otonom varlıkların kullanımından doğan güvensizlik ve riskler tamamen ortadan kaldırılamamaktadır[63]. Her zaman öngörülmeyen sonuçlar olabileceği gibi, öngörülen sonuçlar öngörülemeyen veya engellenemeyen biçimde de ortaya çıkabilir. Örneğin, literatürde çoğunlukla daha az gelişmiş ve eski bir yapay zekâ olan Microsoft Tay örneği verilirken, günümüzdeki en kapsamlı veri setleriyle eğitilen yapay zekâlarından olan GPT-3'ün çok daha yakın bir zamanda (test sırasında) intihar etmeyi düşündüğünü söyleyen hastaya, kendini öldürmesi gerektiğini yazmasının[64] öngörülebilir yahut engellenebilir olup olmadığı tartışılabilir. Sohbet botlarında sıklıkla karşılaşılan bu tür durumların (ve kimi zaman suçların) engellenmesi için kimi modeller geliştirilse dahi, her zaman bir siyah kuğu olabileceği düşünüldüğünde makinenin arkasındaki kişi ceza hukuku bakımından sorumlu olmalı mıdır? Yoksa izin verilen risk kavramı göz önünde bulundurularak[65], olası zararlı sonuçlar bu varlıkların kullanımının bedeli olarak mı

---

https://www.theguardian.com/world/2015/feb/09/south-korean-womans-hair-eaten-by-robot-vacuum-cleaner-as-she-slept (çevrim içi, E.T.: 20.11.2021 13:00).

[61] Lima, a.g.e., s. 692.

[62] Eric Hilgendorf, "Automated Driving and the Law", Robotics, Autonomics, and the Law: Legal Issues Arising from the AUTONOMICS for Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy, Robotik und Recht 14, Ed.: Eric Hilgendorf/Uwe Seidel, Nomos Verlagsgesellschaft, 2017, s. 182; Beck, "Google Cars", ss. 247-248; Koray Doğan, "Sürücüsüz Araçlar, Robotik Cerrahi, Endüstriyel Robotlar ve Cezai Sorumluluk", DEÜ – HFD, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s. 3232.

[63] Melinda Florina Lohmann, "Liability Issues Concerning Self-Driving Vehicles." European Journal of Risk Regulation (EJRR), C:7, S: 2, 2016, ss. 337-338.

[64] Ryan Daws, "Medical chatbot using OpenAI's GPT-3 told a fake patient to kill themselves", 28.10.2020, https://artificialintelligence-news.com/2020/10/28/medical-chatbot-openai-gpt3-patient-kill-themselves/ (çevrimiçi, E.T.: 20.11.2021 13:00).

[65] Hilgendorf, a.g.e., s. 182.

değerlendirilmelidir? Öngörülebilirlik açısından neyin siyah kuğu neyin öngörülebilir fakat öngörülmemiş sürpriz unsur olduğunun tespiti önemlidir.

Yapay zekâlı otonom varlıkları kullananların, ürünün güvenli olduğunu düşünmesi ve bir hatadan kaynaklı kazalarda üreticiyi sorumlu tutması doğaldır. Öğretide bu tür durumlarda, ürün piyasaya sunulup son kullanıcıya ulaşana kadarki aşamalarda yer alan kişilerin standartları uygulayarak, yazılımı güncelleyerek ve hataları düzelterek sorumluluğunu belli açılardan yerine getirebileceği ileri sürülmektedir[66]. Bir görüşe göre, otonom varlıkların dahil olduğu suçlarda sorumluluk belirlenirken detaylı bir araştırma yapılmalı; üretici, operatör gibi makinenin arkasındaki kişilerin somut olayın koşullarına göre mümkün olan tüm tedbirleri alıp almadığı, belli davranışları gerçekleştirip gerçekleştirmediği saptanmalıdır. Örneğin ürün kapsamlı biçimde test edilerek, piyasaya sunulmadan önce gerekli bilimsel ve teknik standartlara uygunluğu sınanmalı, öngörülebilen risklerin ortadan kaldırılmasında gerekli özen gösterilmeli, ürün piyasaya sunulduktan sonra devamlı takip edilmeli, kullanıcı ve üçüncü kişilere yönelik gerekli uyarılar olası gizli tehlikeleri de kapsayacak biçimde özenle yapılmalı, hatanın tespiti hâlinde bu derhal düzeltilmeli ve gerekiyorsa ürün geri çekilmelidir [67]. Yine de sorumluluktan böyle bir savunmayla kurtulmak mümkün olsa bile, bunun sınırının ne olacağı; özellikle kendisi öğrenerek arzulanmayan biçimde davranabilen otonom sistemler bakımından sorunludur. Ayrıca bu hususların ispatı da son derece güçtür[68]. Bir görüşe göre, tasarımcıların özellikle öğrenebilen yapay zekâlı sistemleri geliştirirken büyük bir özenle hareket etmesi gerekmekle birlikte, zararlı sonuçlardan kaçınma konusunda tüm sorumluluk onlarda değildir; sayılan diğer gerçek kişiler de sorumluluğu paylaşır[69]. Öte yandan, öngörülemez ve doğası gereği tehlike yaratabilecek sistemleri geliştirenlerin, ürün insanlarla etkileşime geçmeden önce kontrollü bir ortamda yeterince test etmeleri ve piyasaya sunulduktan sonra da onun zamanla gelişebildiği ve bunun sonucunda öngörülmeyen çıktılar da üretebileceği konusunda insanları uyarmaları gerekir[70]. Günün sonunda, her bir somut olayda gerekli dikkat ve özenin gösterilip gösterilmediğine mahkemeler karar verecektir[71].

Makinenin arkasındaki kişilerin izin verilen risk kapsamında dikkat ve özen yükümlülüğüne uygun olarak üzerlerine düşeni yaptıklarını ileri sürmeleri için konuya ilişkin davranış kurallarının, standartların, mevcut bilim ve teknoloji alanındaki gelişmelerin göz önüne alınması gerekir. Ancak yapay zekânın ve robotiğin henüz erken aşamalarında olunduğundan gerek standartların oluşturulması gerekse potansiyel risklerin saptanması ve bunlara ilişkin

---

[66] Florina Lohmann, a.g.e., ss. 337-338.

[67] Gless vd., a.g.e., s. 429.
Hallevy'e göre, kişinin taksirli sorumluluktan kurtulmak için tüm makul tedbirleri almasına gerek yoktur; makul bir tedbir almış olması yeterlidir. Bkz.: Hallevy, a.g.e., s. 138.

[68] Lohsse vd., a.g.e., s. 22.

[69] M.J. Wolf, K. W. Miller, F. S. Grodzinsky, "Why We Should Have Seen That Coming - Comments on Microsoft's Tay "Experiment," and Wider Implications", The ORBIT Journal, C:1, S:2, ss. 2-3, https://doi.org/10.29297/orbit.v1i2.49 (çevrimiçi, E.T.: 20.11.2021 13:00)

[70] Wolf vd., s.11.

[71] Hilgendorf, a.g.e., s. 188.

kaçınılması gereken davranışların bilinmesi kolay değildir. Bugün programlayan, üreten ve kullananlara yol gösterebilecek sosyal kuralların eksikliği, kabul edilebilir ve edilemez davranış kuralları arasındaki ayrımı çizmeyi güçleştirmektedir[72].

Otonom varlıkların dahil olduğu suçlarda makinenin arkasındaki kişilerin ceza sorumluluğu olup olmayacağı kimi noktalarda çözümü güç sorunlar yaratsa da mevcut ceza hukukunun bugünün birçok sorununu karşılayabileceği kanaatindeyiz. Gerçekten, birçok durumda eski örneklerden pek de uzaklaşmaya gerek yoktur. Örneğin sürücüsüz araç "hacklenerek" kaza yaptırıldığında, yalnızca sistemi manipüle edenlerin değil; güvenlik sistemini geliştirenlerin de ceza sorumluluğu tartışılabilir. Kazaya neden olabilecek şekilde, saldırılarda kolayca aşılabilecek bir güvenlik sistemi kurulmuşsa[73] kanımızca kaza sonucu gerçekleşen ölüm, yaralanma gibi öngörülebilir neticelerden güvenlik sistemini kuranların -diğer koşulların varlığı hâlinde- taksirli sorumluluğu gündeme gelecektir. Bir başka örnek olarak sürücüsüz aracın, aracın sevk ve idaresinin devralınması için uyarı vermesine karşın, sürücünün bunu yapmaması durumunda, olaydaki koşullar dikkate alınarak, doğrudan veya olası kasıtla sorumluluğu düşünülebilir[74]. Sürücünün aracın sevk ve idaresini devralmakta gerekli dikkat ve özeni göstermemesi durumunda taksirli sorumluluğun da gündeme gelebileceği; fakat ondan bu şekilde sürüşün devralmasının umulmadığı durumlarda bu dikkat ve özeni göstermesinin beklenmediği de ifade edilmektedir[75]. Kanımızca, bir kazanın muhtemel olarak yaklaşmakta olduğunu ve sürücüsüz aracın bunu engelleyemeyeceğini (veya hatalı çalıştığını) fark eden sürücünün[76], ilgili karayolları mevzuatı kendisine böyle bir yükümlülük yüklemese de, bu kazayı engellemek üzere aracın sevk ve idaresini devralması gerekir; aksi durumda taksirle sorumluluğu gündeme gelecektir. Benzer şekilde, yapay zekâlı otonom varlıkların üreticilerinin devlet tarafından konulan (veya sektör tarafından geliştirilen) standartlara uyduğunu ispatlamasının da taksirli sorumluluktan kurtulmak için yeterli olmayacağı kanaatindeyiz; zira taksirde esas alınan davranış kurallarının kaynağı yalnızca bunlardan meydana gelmemektedir.

Bir görüşe göre bugün için yapay zekâlı otonom varlıkların yanlışı doğrudan ayıracak şekilde bir davranışı seçme yeteneğinden söz edilemese de ileride bunu gerçekleştirebileceklerdir. O zaman tıpkı otomobilin lastiği patlayıp kaza yapıldığında olduğu gibi suçlayacak kimse bulunamayabilir. Her şey öngörülebilir ve engellenebilir değildir, günlük yaşamda ceza hukukunu ilgilendirebilecek pek çok durumda aslında suçlayacak kimse yoktur, insanların bu kötü talih ile de yaşaması gerekir[77]. Gerçekten günlük yaşamda her şey öngörülebilir ve

---

[72] Beck, "Google Cars", ss. 240-243.
[73] Hilgendorf, a.g.e., s. 183.
[74] Aksoy Retornaz, a.g.e., s. 340; Aynı yönde bkz.: Kangal, a.g.e., s. 96.
Burada ilgili hukuk normlarının aracın sevk ve idaresine ilişkin sürücüye yükümlülük yüklemesi önemlidir.
[75] Aksoy Retornaz, a.g.e., s. 341.
[76] Örneğin *Microsoft'un* ünlü sohbet botu *Tay* konusunda *Kangal'*a göre, üreticinin gerçek ihmali suçları önleme yükümlülüğünden dolayı, üretici *Tay'in* hakaret ve diğer suçları işlemeye başladığını tespit ettiğinde müdahale etmesi gerekir; aksi durumda ihmali davranışla bu suça iştirak eder. Bkz.: Kangal, a.g.e., s. 98.
[77] Lima, a.g.e., s. 694.

engellenebilir olmayabilir; her zaman bir siyah kuğu olabilir. Ancak günümüzde COVID19 gibi bir pandeminin dahi öncesindeki bilimsel araştırmalarda öngörülebilir olduğu düşünüldüğünde, sorun insanların öngörme ve önlem alma gerekliliğinin ne kadarının hukuken beklenebileceği noktasında düğümlenmektedir. Yapay zekâlı otonom varlıkların dahil olduğu suçlarda makinenin arkasındaki kişilerin ceza sorumluluğu bu soruya verilen yanıta göre belirlenecektir.

5. Özel Hukuktaki Bazı Sorumluluk Modellerinin Uyarlanması

Yapay zekâlı otonom varlıkların dahil olduğu suçlarda, suçtan kaynaklanan sorumluluğun belirlenmesi açıklandığı üzere her zaman kolay olmamaktadır. Teorik olarak yapılan çıkarımlar bir yana, günlük yaşamda işler daha da karmaşıklaşmakta; makinenin arkasındaki kişilere ceza sorumluluğu atfedilip atfedilemeyeceği, kusurlu olup olmadıkları çoğu zaman yanıtlanması güç bir soru olarak kalmaktadır. Öğretide bugünün gelişmişlik düzeyine sahip otonom varlıklar için ceza hukukunun bir ölçüde çözüm üretebildiği; ancak gelecekte bunun da mümkün olmayacağı yaygın olan kanıdır. Ortaya çıkabilecek adaletsiz sonuçları engellemek amacıyla özel hukuktaki ürün sorumluluğu, tehlike sorumluluğu, *respondeat superior,* objektif veya kusursuz sorumluluk modellerinin ceza hukukunda da uygulanması üzerinde durulmaktadır. Bu modellerin ceza hukukuna uyarlanmasının önerilmesinin altında, ceza sorumluluğunun temelinde kusurun yer alması vardır. Nitekim, bu öneriler de kusura dayanan sorumluluğu esnetmekte veya onu bypass etmektedir.

Kusursuz sorumluluğun ve türevlerinin[78] öncelikle yapay zekâlı otonom varlıkların neden olduğu zararlarda özel hukukta kullanılması önerilmektedir[79]. Bununla birlikte, otonomluk seviyesi arttıkça onu kullananların sorumluluğunun azalacağı ve tam otonomluk düzeyine ulaşıldığında bu kişilerin sorumluluğundan söz edilemeyeceği düşünülerek, kusursuz sorumluluk hâlinin geçiş dönemi için uygulanması önerilmektedir[80]. Bir görüşe göre objektif sorumluluk modeli yapay zekâlı otonom varlıkların dahil olduğu suçlarda da kullanılabilir. İlgili gerçek kişinin sorumluluktan kurtulması için, kasıtlı veya taksirliği olmadığının yanı sıra, suçun gerçekleşmesini engellemek için tüm makul tedbirleri almış olduğunu ispatlamalıdır[81]. Buna karşılık mevcut ceza hukukunun otonom varlıkların kullanımını sınırlı olarak karşılayabileceğini belirten aksi görüş, objektif sorumluluğun ceza hukukunda kabul edilemeyeceğini belirtmektedir[82].

Ürün sorumluluğuna ilişkin bir görüş, gelecekte kazaların kullanım hatasından ziyade, ürünün kusurlu olmasından kaynaklanacağını belirterek, sorumluluğun kullanıcıdan üreticiye

[78] Kusursuz sorumluluk hâllerinin konunun özel hukuk boyutuyla incelenmesi için bkz.: Onur Sarı, "Yapay Zekanın Sebep Olduğu Zararlardan Doğan Sorumluluk", TBB Dergisi, S.147, 2020, s. 267 vd.
[79] Semih Yünlü, "Current Developments on Artificial Intelligence and Liability for Robot Caused Damages." Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C:16, S:1, 2019, s. 206; Lohsse vd., s. 15.
[80] Başak Bak, "Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk", Türkiye Adalet Akademisi Dergisi, S: 35, 2018, s. 225.
[81] Hallevy, a.g.e., s. 138.
[82] Beck, "Google Cars", a.g.e., s. 244.

kayacağını ifade etmektedir[83]. Bir başka görüş, bu konuda ceza hukuku bakımından ürün sorumluluğundan türetilen bir modelde, objektif sorumluluğun taksirin koşullarıyla birlikte değerlendirilmesinin düşünülebileceğini ileri sürmektedir[84].

Asıl olarak haksız fiil sorumluluğundan türeyen *respondeat superior,* bir kimsenin kontrolünde olduğu başka bir kimsenin fiilinden sorumluluğuna işaret etmektedir (**Ing**. "*let the master answer"*)[85]. Roma hukukundaki *paterfamilias'*a veya günümüzdeki istihdam edenin sorumluluğuna benzetilen bu model, ABD'de şirketlerin, aracıları tarafından yetkileri dahilinde, şirket adına ve onun menfaatine işlenen suçlardan şirketin sorumluluğunun belirlenmesinde kullanılmaktadır[86]. Objektif sorumluluğu gerektirmeyen suçlarda, şirket yöneticilerinin suçun işlenmemesi için gereken özeni (*due diligence*) gösterdiğini ispatlayarak sorumluluktan kurtulmasının mümkün olduğu belirtilmektedir[87]. Yapay zekâlı otonom varlıkların dahil oldukları suçlarda da bu modelin ceza hukuku bakımından uygulanabilirliği tartışılmaktadır[88]. *Respondeat superior*, robotların köle olarak kullanıldığı bilim kurgu evrenlerini çağrıştırmaktadır. Öğretide yapay zekâlı varlıklara köle statüsünün verilemeyeceği, köleliğin ilkel bir düşünce olduğu ve terk edilmesi gerektiği ifade edilmektedir[89]. Bu düşüncenin üzerinde peşin bir yargıya varmadan durulması ve otonom varlıklara tanınabilecek kölelik benzeri bir statünün niçin sakıncalı olduğunun sorgulanması gerektiği kanaatindeyiz. İnsan onuruna aykırı olduğu için mi? Sömürüye dayandığı yahut insanın içindeki kötüyü açığa çıkardığı için mi? Günümüzde herhangi bir sinir sistemine, hisse ve bilince sahip olmayan yapay zekâlı otonom varlıklar bakımından ancak üçüncü öncül kabul edildiğinde bu argümanın geçerli olabileceği kanaatindeyiz. Zira, kölelik insanlık tarihi kadar eski bir kurum olmakla birlikte, görece yeni bir hak olan mülkiyet halihazırda insanlara eşyalar üzerinde haklar tanımaktadır. Nitekim, insana benzesin veya benzemesin, sınırlı bir otonomiye sahip varlıklar ile kurduğumuz ve muhtemelen gelecek on yılda kuracağımız ilişki de bundan farklı olmayacaktır. *Respondeat superior* ise bu varlıkların neden olacakları zararlardan onun operatörünün sorumlu olmasını ifade etmek üzere ileri sürülen bir öneridir. Kanımızca bu modelin bugün kabul edilmesi mümkün olmamakla birlikte, geleceğe yönelik bazı sorular akla gelmektedir: İleride ceza sorumluluğu ile haksız fiil sorumluluğunun birbirine yaklaşması mümkün müdür? Otonom varlıklar geliştikçe yahut fiziksel varlığı olmayan yazılımların sayısız olacağı düşünülünce onlardan sorumlu bir operatör olması mümkün olacak mıdır?

[83] Florina Lohmann, a.g.e., s. 337.
[84] Lima, a.g.e., s. 693.
[85] Lima, a.g.e., s. 692.
[86] Gless vd., a.g.e., s. 417-418.
[87] Gless vd., a.g.e., s. 418.
[88] Hallevy, a.g.e., s. 106 vd.
[89] Bak, a.g.e., s. 219; Melisa Aydemir, "Yapay Zekalı Robotların Ceza Sorumluluklarının Araştırılması", Suç ve Ceza, S. 4, 2018, s. 47.

Sonuç olarak, yapay zekâlı otonom varlıkların dahil olduğu suçlarda, makinenin arkasındaki kişilerin kusursuz sorumluluğunun kabul edilmesi[90] ortaya çıkabilecek cezasızlık ve adaletsizlik hissini dindirecekse de cezalandırılma korkusu geliştiricileri ve üreticileri caydıracaktır[91]. Bu endişe yalnızca kusursuz sorumluluk türlerinde değil, makinenin arkasındaki kişilerin ceza sorumluluğuna sahip olacağı klasik modelde de mevcut olacaktır; öte yandan taksirli sorumluluğun insanları daha dikkatli ve özenli olmaya sevk ettiği anımsamak gerekir.

Sonuç

Yapay zekâlı otonom varlıkların dahil olduğu suçlarda sorumluluğun belirlenmesi, mevcut ceza hukukunun sınırlarını zorlamaktadır. Öğretide kimi yazarlar mevcut ceza hukuku kurallarının yeterli olduğunu, sorunların birçoğunu karşılayabileceğini belirtirken; kimileri başta yapay zekâlı otonom varlıklara ayrı bir hukuki kişilik tanınması olmak üzere, ceza normlarının da değişmesi gerektiğini, ortaya çıkan ve çıkabilecek sorunların ancak bu şekilde çözülebileceğini ileri sürmektedir.

Kanımızca günümüzde ceza hukukunun çözüm üretemediği ileri sürülen sorunların büyük bölümünü makinenin arkasındaki kişinin taksirli sorumluluğu karşılamaya yetecektir. Ancak yakın gelecekte otonomluk arttıkça ve yapay zekânın açıklanabilirliği azaldıkça, ceza hukuku her duruma yanıt veremez olacaktır. Bunun için öğretide, kaynağını özel hukuktan alan ve kusura dayalı sorumluluğu esneten bazı sorumluluk modellerinin ceza hukukuna da uyarlanabileceği ileri sürülmektedir. Ancak unutulmamalıdır ki, belirli faraziyelerden yola çıkan sorumluluk modellerinde; bir kişinin belirlenerek cezalandırılması, diğerlerinin kusursuz olduğu anlamına gelmez. Dolayısıyla bu faraziye içinde ceza hukuku sorumluluğunun belirli bir kimseye yüklenmesi, diğerlerinin cezasız kalmasına yol açmamalıdır. Nitekim, ceza hukukunda amaç zararın tazmin edileceği bir muhatap belirlemek olmayıp; herkes kusurunca sorumlu olacaktır.

[90] Bir görüşe göre, bugün için en makul olan tehlike sorumluluğu veya ürün sorumluluğu, gelişmiş yapay zekâlar için yeterli olmayacağından, yeni yasal düzenlemelerin yapılması gerekmektedir. Bak, a.g.e., s. 223.
Tehlike sorumluluğunun uygulanabilirliğine ilişkin bkz.: Sarı, a.g.e., ss. 294-299.
[91] Lima, a.g.e., s. 693.

Kaynakça

Aksoy Retornaz, Eylem: "Otonom Araçlar ve Ceza Hukuku", Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ, Ed.: E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk, On İki Levha Yayıncılık, 2021, ss. 331-345.

Aksoy, Hasan: "Yapay Zekalı Varlıklar ve Ceza Hukuku", International Journal of Economics, Politics, Humanities & Social Sciences, C:4, S:1, 2021.

Altunç, Sinan: "Yapay Zekâ ve Ceza Hukuku Sorumluluğu", Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ, Ed.: E. Eylem Aksoy Retornaz, Osman Gazi Güçlütürk, On İki Levha Yayıncılık, 2021, ss.347-371.

Aydemir, Melisa: "Yapay Zekalı Robotların Ceza Sorumluluklarının Araştırılması", Suç ve Ceza, S. 4, 2018, ss. 1-96.

Bak, Başak: "Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk", Türkiye Adalet Akademisi Dergisi, S: 35, 2018, ss. 211-232.

Beck, Susanne: "Google Cars, Software Agents, Autonomous Weapons Systems New Challenges for Criminal Law?", Robotics, Autonomics, and the Law: Legal Issues Arising from the AUTONOMICS for Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy, Robotik und Recht 14, Ed: Eric Hilgendorf/Uwe Seidel, Nomos Verlagsgesellschaft, 2017, ss. 227-251.

Beck, Susanne: "Intelligent Agents and Criminal Law—Negligence, Diffusion of Liability and Electronic Personhood", Robotics and Autonomous Systems, C. 86, 2016, ss. 138-143.

Çekin, Mesut Serdar: "Otonom Araçlar ve Hukuki Sorumluluk", TAAD, S. 33, 2018, ss. 283-345.

Doğan, Koray: "Sürücüsüz Araçlar, Robotik Cerrahi, Endüstriyel Robotlar ve Cezai Sorumluluk", DEÜ – HFD, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s.3219-3251.

Ekici Şahin, Meral: "Dolaylı Failliğin Ortaya Çıkış Biçimleri", BÜHFD, C: 8, S: 107-108, 2013, ss. 61-88.

Evtimov, Ivan / O'Hair, David / Fernandes, Earlence / Calo, Ryan / Kohno, Tadayoshi: "Is Tricking a Robot Hacking?", Berkeley Technology Law Journal, C. 34, S. 3, 2019, ss. 891-918.

Florina Lohmann, Melinda: "Liability Issues Concerning Self-Driving Vehicles." European Journal of Risk Regulation (EJRR), C:7, S: 2, 2016, ss. 335-340.

Freitas, Pedro Miguel / Andrade, Francisco / Novais, Paulo: "Criminal Liability of Autonomous Agents: From the Unthinkable to the Plausible", AI Approaches to the Complexity of Legal Systems, Ed. Pompeu Casanovas vd., Lecture Notes in Computer Science, Heidelberg: Springer, 2014, ss. 145-156.

Gless, Sabine / Silverman, Emily / Weigen, Thomas: "If Robots Cause Harm, Who Is To Blame? Self-Driving Cars and Criminal Liability", New Criminal Law Review, C. 19, S. 3, 2016, ss. 412-436.

Gözükeleş, İzlem: "Yapay zekâ kime hizmet edecek?", Bilim ve Gelecek, S:199, 2020.

Hallevy, Gabriel: Liability for Crimes Involving Artificial Intelligence Systems, Springer International Publishing, 2015.

Hilgendorf, Eric: "Automated Driving and the Law", Robotics, Autonomics, and the Law: Legal Issues Arising from the AUTONOMICS for Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy, Robotik und Recht 14, Ed.: Eric Hilgendorf/Uwe Seidel, Nomos Verlagsgesellschaft, 2017, ss. 171-193.

Kangal, Zeynel: Yapay Zekâ ve Ceza Hukuku, On İki Levha Yayıncılık, 2021.

Kelep Pekmez, Tuba: "Otonom Araçların Kullanımından Doğan Cezaî Sorumluluk: Türk Hukuku Bakımından Genel Bir Değerlendirme", Ceza Hukuku ve Kriminoloji Dergisi, C. 6, S. 2, 2018, ss. 173-195.

Lima, Dafni: "Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law" South Carolina Law Review, C:69, 2018, ss. 677-696.

Lohsse, Sebastian / Schulze, Reiner / Staudenmayer, Dirk: "Liability for Artificial Intelligence", Liability for Artificial Intelligence and the Internet of Things: Münster Colloquia on EU Law and the Digital Economy IV, Ed: Sebastian Lohsse / Reiner Schulze / Dirk Staudenmayer, Nomos, 2019, ss. 11-26.

Önok, Murat: Yapısal Suçlarda Failin Tespiti: Müşterek Suç Girişimi (Joint Criminal Enterprise) ve Örgütsel Hakimiyete Dayalı Dolaylı Faillik Doktrinleri, Seçkin Yayıncılık, 2019.

Sarı, Onur: "Yapay Zekanın Sebep Olduğu Zararlardan Doğan Sorumluluk", TBB Dergisi, S.147, 2020, ss. 251-312.

Sınar, Hasan: "Türk Ceza Hukukunda Dolaylı Faillik", CHD, S: 15, 2011, ss. 59-86.

Simmler, Monika/ Markwalder, Nora: "Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence." Criminal Law Forum V:30, I:1, 2019, p.19-20.

Wolf, M.J. / Miller, K. W. / Grodzinsky, F. S.: "Why We Should Have Seen That Coming-Comments on Microsoft's Tay "Experiment," and Wider Implications", The ORBIT Journal, C:1, S:2, ss. 1-12.

Yünlü, Semih: "Current Developments on Artificial Intelligence and Liability for Robot Caused Damages." Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C:16, S:1, 2019, ss. 189-213.

Çevrim içi Kaynaklar[92]

Calo, Ryan: "Robotics & The Law: Liability For Personal Robots", Stanford Law School The Center for Internet and Society, 26.11.2009, https://ftp.documation.com:8443/references/aba10a/PDfs/2_1.pdf.

Daws, Ryan: "Medical chatbot using OpenAI's GPT-3 told a fake patient to kill themselves", 28.10.2020, https://artificialintelligence-news.com/2020/10/28/medical-chatbot-openai-gpt3-patient-kill-themselves/

European Parliament Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), Committee on Legal Affairs, 31.05.2016 https://www.europarl.europa.eu/doceo/document/JURI-PR-582443_EN.pdf?redirect

European Parliament, Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), Committee on Legal Affairs, 27.01.2017 https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf

Günther, J.P./ May, E./ Münch, F./ Löffler, S./ Beck, S./ Hilgendorf, E.: "Exploration track: non-human agents and electronic personhood", Suggestion for a green paper on legal issues in robotics, Ed: C. Leroux, R. Labruto, euRobotics, The European Robotics Coordination Action, 2012, ss. 58-64. https://www.researchgate.net/publication/310167745_A_green_paper_on_legal_issues_in_robotics .

Keck, Catie: "How a Piece of Tape Tricked a Tesla Into Reading a 35MPH Sign as 85MPH", https://gizmodo.com/how-a-piece-of-tape-tricked-a-tesla-into-reading-a-35mp-1841791417.

McCurry, Justin: "South Korean woman's hair 'eaten' by robot vacuum cleaner as she slept", The Guardian, 09.02.2015, https://www.theguardian.com/world/2015/feb/09/south-korean-womans-hair-eaten-by-robot-vacuum-cleaner-as-she-slept .

[92] Çalışmada yararlanılan çevrim içi kaynakların son erişim tarihi: 20.11.2021 13:00.

Yapay Zekâ Temelli Önleyici Hukuk Mekanizmaları - Öngörücü Polislik

Dr. Öğr. Üyesi Zafer İçer

Giriş

İnsan sosyal bir varlıktır. İnsanlar için bir arada yaşamak bir ihtiyaç olup aynı zamanda tabii gerekliliktir. Bir arada yaşamak, kuralların varlığını zorunlu kılar. Nerede bir toplum varsa, orada hukuk vardır ve olmalıdır *(ubi societas, ibi jus)*. Devletin var olmadığı eski dönemlerde insanlar; aile, klan ve kabile adı altında oluşan topluluklar bünyesinde yaşamlarını sürdürmüştür. O dönemlerde suç kabul edilen fiiller, şahıslar arasında gerçekleşen uyuşmazlıklar olarak değil, toplulukların birbirlerine karşı gerçekleştirdikleri haksız fiiller olarak nitelendirilmiştir. Bu sebeple, uyuşmazlıklar şahsi öç, kısas, diyet gibi karşılıklarla çözülmeye çalışılmıştır. Kusur sorumluluğunun ve şahsilik prensibinin geçerli olmadığı bu dönemlerde, işlenen suçlara karşılık çoğu zaman ölçüsüz yaptırımların uygulanması, ihtilafların devam etmesine yol açmıştır. Zaman içerisinde insanlar arasındaki uyuşmazlıkların kalıcı, adil şekilde çözümüne odaklanılmış ve topluluklar için getirilmiş kuralları gözetecek üstün bir otoritenin varlığına ihtiyaç duyulması ile birlikte devlet mekanizması ortaya çıkmıştır[93].

Devletin en önemli görev ve ödevi, bireylerin hak ve hürriyetlerini korumaktır. Bu amaçla devlet, bir yandan önleyici alanda faaliyetleri yerine getirirken, bir yandan da suç teşkil eden davranışları gerçekleştiren kişileri toplumdan izole ederek yeniden topluma kazandırılmasını sağlayan ceza ve infaz politikalarını hayata geçirmekle yükümlüdür. Bu sebeple, suçları önleme ve suçluları yargılayarak cezalandırma yetkisi, tekel bir yetki olarak devlete aittir. Cezalandırma, suç teşkil eden davranışın rasyonel bir karşılığıdır; çünkü suçlu bir kimsenin toplum içinde yaşamaya devam etmesi, toplumun hukuki menfaatleri bakımından risk oluşturmaktadır. Aynı zamanda, suç işleyen kişinin, hukuk düzenine aykırı hareket etmesinin belirli bir karşılığının bulunması, hakkaniyetin ve adil olmanın bir gereğidir. Suçlu kimsenin cezalandırılması, toplumdaki diğer bireyler üzerinde caydırıcılığın sağlanması amacına da hizmet etmektedir[94].

Suç, bir davranış modelidir; bu sebeple suçsuz bir toplum düşünülememektedir. Suçun topyekûn ortadan kaldırılması mümkün değildir, ancak suçun azaltılması her zaman imkân dahilindedir. Bu sebeple, suçluların cezalandırılması kadar, suçun henüz işlenmeden önlenmesi de oldukça önemlidir. Önleyici mekanizmalarla suçlu davranışların en aza indirilmesi devletin bir görevidir. Ceza muhakemesi, suç işlendikten sonra devreye giren bir

[93] Zafer İçer, Suça Teşebbüste Hazırlık Hareketleri İle İcra Hareketlerinin Birbirinden Ayrılması, İstanbul 2021, s.1 vd.
[94] Nur Centel, Cezanın Amacı ve Belirlenmesi, Turhan Tufan Yüce'ye Armağan, İzmir 2001, s.337 vd.

süreç olup suçun önlenmesi faaliyeti ise idari bir nitelik arz etmektedir. Bu sebeple, suçun önlenmesine ilişkin faaliyetler idarenin görev ve sorumluluğundadır. Ceza hukuku araçlarıyla suçla mücadele ise, suça ilişkin icra hareketlerinin başlaması ile birlikte mümkün olabilmektedir. Bundan önceki alan "hazırlık evresi" olduğundan ve ceza hukukunda hazırlık hareketleri kural olarak cezalandırılmadığından, elverişli hareketlerle doğrudan doğruya icraya başlanmadığı sürece, bir kimsenin cezalandırılabilmesi mümkün değildir[95].

Günümüzde, önleyici hukuk mekanizmaları ve öngörücü polis uygulamalarının artmasının bazı sebepleri vardır. Bunlardan en önemlisi, suç işlendikten sonra, suçun meydana getirdiği zararlı sonuçların hiçbir zaman tam anlamıyla telafi edilememesidir. Yalnızca yargılama faaliyeti ve bunun sonucunda kişi hakkında hükmedilen yaptırım, ihlale uğrayan hukuki değerin telafisini çoğu zaman mümkün kılmamaktadır. Özellikle bireyin yaşamına, vücut bütünlüğüne, cinsel dokunulmazlığına yönelik ihlaller gerçekleştiğinde, ortaya çıkan neticenin tekrar eski haline getirilmesi olanaklı değildir. Bu değerlerin korunduğu suçları işleyen failler hakkında uygulanan yaptırım, ne kadar ağır olursa olsun, pek çok açıdan mağduru ve toplum vicdanını tatmin edememektedir. Suçu önleyici mekanizmaları önemli hale getiren hususlardan biri de budur[96].

Diğer taraftan, ceza adaletinde yaşanan değişimin de önleyici mekanizmaların önemini arttırdığı ifade edilmelidir. Ceza hukuku araçları, suçun işlenmesi sonrası devreye girer. Bu sebeple, geleneksel ceza adaleti, suç failine odaklı bir anlayış doğrultusunda gelişim göstermiştir. Bu anlayışın odağında hiçbir zaman mağdur olmamış, mağdurun haklarının korunması her zaman ikinci plana itilmiştir. Hukuki değeri ihlal eden davranışların önlenebilirliği konusunda ortaya çıkan gayretlerin yeterli olmaması, suç işlendikten sonra pek çok açıdan ortaya çıkan zararın telafisinin mümkün olmaması, zarar verici davranışların henüz gerçekleşmeden önlenmesinin ya da yaptırıma bağlanmasının önemini ortaya çıkarmıştır. Bu konuda, süreç içerisinde oluşan toplumsal mutabakat, suç politikasına yön vermiştir. Yasa koyucunun palyatif olmayan çözümler üretme çabası, ceza normlarında yeni suç formlarının öngörülmesiyle sonuçlanmıştır. Bu yöntemde, hukuki değerleri daha etkili koruma adına, cezalandırılabilirliğin sınırlarının genişletilmesi öngörülmüş ve bu amaçla tehlike suçları ile hazırlık hareketlerinin cezalandırıldığı suçlara normatif düzenlemelerde yer verilmiştir. Böylelikle, belirli hukuki değerlerin henüz zarara uğramasından önce, tehlikeli ve daha ağır bir suç potansiyeli taşıyan davranışları cezalandırarak ceza hukukunun önleyici işlevi arttırılmaya çalışılmıştır.

Günümüzde, modernleşmiş toplumlar ve modern yaşam tarzlarıyla birlikte, insanlar arasındaki ilişkilerin düzeyi, yoğunluğu fazlalaştığı gibi, niteliğinde de değişimler yaşanmış ve bu durum potansiyel suç tehditlerinde artışa sebebiyet vermiştir. Bilhassa teknolojinin

---

[95] Adem Sözüer, Suça Teşebbüs, İstanbul 1994, s.194 vd.; İçer, Suça Teşebbüste, s.22-23.

[96] Zafer İçer – Başak Buluz, Yapay Zekanın Ceza Muhakemesindeki Rolü ve Geleceği, 9. Uluslararası Suç ve Ceza Film Festivali, İstanbul 2019, s.14, https://robotic.legal/yapay-zekanin-ceza-muhakemesindeki-rolu-ve-gelecegi/, Erişim Tarihi.: 01.12.2021.

gelişimiyle birlikte yeni suç formlarının ortaya çıkması, bu potansiyeli üst seviyeye çıkarmıştır. Milyonlarca insanın yaşadığı büyük şehirlerde, metropollerde, evde, işte, okulda, sosyal yaşamda, kamusal alanlarda bireylerin suça maruz kalma ihtimallerinin, geçmişe nazaran artık çok daha fazla olduğu söylenebilir. Hukuki değerleri ihlal edici davranış türlerindeki çeşitlilik, suçların karmaşıklığı, suç işleme imkanlarının artması ve bilhassa insan davranışlarının öngörülemezliği ve bilinemezliği, suçla mücadelede karşımızda duran kayda değer zorluklardır[97].

Bu zorluklara karşın, yapay zekâ temelli inovatif teknolojilerin güvenlik alanına sirayet etmesi ile birlikte, önleyici hukuk mekanizmaları ve bilhassa öngörücü polislik açısından yeni bir sayfanın açıldığı ifade edilmelidir. Yapay zekâ tabanlı uygulamalar, insan davranışlarının öngörülemezliğinden kaynaklanan dezavantajları minimize etmekte ve insan kaynaklı güvenlik risklerinin hızlı ve yüksek başarı ile tespit edilebilmesine olanak sağlamaktadır. Kamu güvenliğinin sağlanması ve suçun önlenmesi adına, kamu gücünü kullanan birim ve organlar tarafından hukuki çerçevede hayata geçirilen bu uygulamalar; yalnızca kolluk uygulamalarından ibaret olmayıp şüpheli, sanık veya hükümlünün suç işleme riskinin değerlendirilerek ceza muhakemesi ve infaz süreçlerinde salıverilmesine ilişkin risk temelli kararlarla ilgili destek sistemlerini de içerisinde barındıran bir dizi mekanizmayı kapsamaktadır.

Yapay zekâ temelli önleyici hukuk mekanizmaları, öngörücü kolluk uygulamalarını da içerisinde barındıran üst bir kavramdır. Yapay zekâ temelli önleyici hukuk mekanizmaları; idare, ceza muhakemesi ve infaz hukuku süreçlerinde uygulanma kabiliyetini haiz, bir kişinin ilk kez ya da tekraren suç işlemesinin önüne geçmeyi hedefleyen ve bu amaçla suç riskinin, olasılığının yapay zekâ tabanlı sistemler vasıtasıyla analiz edilip bu çerçevede hukuki düzlemde şahıslarla ilgili birtakım işlemler yapılmasına ya da kararlar alınmasına imkân sağlayan mekanizmaları ifade etmektedir. Bu bağlamda, yapay zekâ temelli önleyici hukuk mekanizmalarının, yalnızca suçun önlenmesini amaçlayan idari faaliyetlerle sınırlı anlaşılmaması gerekir. Bu mekanizmalar, aynı zamanda suçun tekraren işlenmesini engellemeye yarayan muhtelif adli işlem ve kararların alınmasında, adli makamlara yardımcı olan yapay zekâ tabanlı uygulamaları da içerisinde barındırmaktadır.

Suç riskine ilişkin tahmin ve analizlerin yapılabilmesine imkân tanıyan bu uygulamaların bütünü, *"yapay zekâ temelli önleyici hukuk mekanizmaları"* olarak adlandırılmakta iken, bu mekanizmaların en önemli ayağını *"yapay zekâ temelli öngörücü kolluk uygulamaları"* oluşturmaktadır. Görev tanımının en temel unsuru suçun işlenmesinin önlenmesi olan önleyici kolluk faaliyetlerinin, yapay zekâ temelli destek sistemleri aracılığıyla yerine getirilmesi ve öngörücü kolluk uygulamaları sayesinde, suçlu davranışların işlenmeden tespit edilerek önlenmesi, bireysel ve toplumsal hak ve menfaatlerin korunmasında kritik bir rol oynamaktadır. Gerek hak ve hürriyetler alanında meydana getirdiği etki alanının genişliği sebebiyle toplumun tüm kesimlerini ilgilendirmesi, gerekse potansiyel suçların önüne

[97] İçer, Suça Teşebbüste, s.7.

geçilmesinde sağladığı başarı düzeyi ile işlevselliğinin diğer mekanizmalara nazaran çok daha fazla olması, önleyici hukuk mekanizmaları içerisinde, yapay zekâ temelli öngörücü kolluk mekanizmalarına ayrı bir parantez açılması gerekliliğini beraberinde getirmektedir.

1. Yapay Zekâ Temelli Öngörücü Kolluk Uygulamaları

Suç potansiyelinin arttığı günümüzde, suçu önleme noktasında klasik yöntemlerin yetersiz kalması, devletleri yeni tür mekanizmaları hayata geçirmeye sevk etmektedir. Son yıllarda, suçla mücadele yöntem ve araçlarında önemli değişim ve gelişimler yaşanmaktadır. Bilhassa, güvenlik alanında ve suçun önlenmesine ilişkin faaliyetlerde, yapay zekâ sistemlerinin kullanımının yaygınlaşmaya başladığı gözlemlenmektedir[98].

Öngörücü kolluk uygulamaları *(predictive policing),* suç potansiyeli taşıyan kimselerin, suç şüphesi içeren davranışların ya da suç işleme niyetinin, analitik yöntemlerle tahmin edilmesi suretiyle suç işleme riskinin öngörülmesini sağlayan ve bu çerçevede gerekli önleyici tedbirlerin hayata geçirilmesine imkân veren kolluk uygulamalarının bütünü olarak ifade edilebilir[99]. PredPol olarak kısaltılan Predictive Policing yöntemi, Azınlık Raporu (Minority Report, 2002) filminde çarpıcı bir şekilde işlenmiştir. Psişik güçlere sahip kâhinler ve bazı teknolojik aygıtlar aracılığıyla cinayetlerin işlenmesinden önce kolluk güçlerine müdahale imkânı, 2000'li yılların başında bilim kurgudan öte bir anlam ifade etmese de, günümüzde yapay zekâ teknolojisinin kaydettiği gelişme, yakın gelecekte öngörücü polisliğin hangi seviyelere gelebileceği konusunda somut fikirler vermektedir.

Yapay zekâ temelli öngörücü kolluk uygulamaları denildiğinde, geleneksel önleyici mekanizmalar dışında, büyük veri ya da öğretilmiş veri kaynakları kullanılarak oluşturulan algoritmalar vasıtasıyla, makine öğrenimi ya da derin öğrenme yöntemleri ile çalışan sistemler anlaşılmalıdır. Bu sistemler, suçların gerçekleşeceği yerleri ve zamanları, suç mağduru olma olasılığı en yüksek olan bireyleri veya demografileri tahmin etmek, suç potansiyeli ve riskini matematiksel ve istatistiksel olarak ortaya koymak suretiyle, genel suç potansiyelinin belirlenmesine yardımcı olmanın yanı sıra somut bir kişi ile ilgili suç işleme riskinin hesaplanmasını da kapsayan, çok geniş bir uygulama alanına sahiptir[100].

Teknolojinin suçun önlenmesi ve ortaya çıkartılması noktasında önemli kolaylıklar sağladığı bir gerçektir. Bu uygulamalar bazen suçu önleyici, bazen de suçun ortaya çıkarılması amacıyla kullanılabilmektedir. Örneğin telekomünikasyon yoluyla iletişimin denetlenmesi, istihbari alanda olduğu gibi, bir koruma tedbiri olarak delil toplama amacıyla şüpheli ve sanık hakkında da uygulanabilmektedir. Bununla birlikte günümüzde, X-ray cihazları, CCTV

[98] İçer – Buluz, s.14.
[99] Walter L. Perry vd., Predictive Policing: The Role of Crime Forecasting In Law Enforcement Operations, RAND Safety and Justice Program, 2013, s.1; Eren Sözüer, Öngörücü Kolluk Uygulamaları ve İnsan Hakları, Yapay Zekâ Çağında Hukuk, Kasım 2020, s.4, https://istanbulbarosu.org.tr/files/komisyonlar/yzcg/2020kasimbulten.pdf, Erişim Tarihi: 01.12.2021.
[100] Sözüer, Öngörücü Kolluk, s.4.

(kapalı devre televizyon), MOBESE gibi kamera sistemleri, yüz tanıma teknolojileri, uzaktan ses ve görüntü kaydına imkân veren teknik araçlar, yapay zekâ destekli sistemler, robot polisler, insansız hava araçları ve diğer mobil uygulamalar, bireylerin izlenmesi ve gözetlenmesi yoluyla özellikle önleyici kolluk mekanizmalarının yaygın araçları olarak kullanılmaya başlanmıştır[101].

1.1. Robot Polisler ve Yapay Polis İstasyonları

Robot polisler, yapay zekâ destekli öngörücü polisliğin ilgi çekici örneklerinden birini oluşturmaktadır. Amerika Birleşik Devletleri'nin Los Angeles kentinde, *K5* adı verilen robot polis, bir parkta test edilmiştir. Çevresindeki hareketleri kayıt altına alan bu polis robotu, herhangi bir şekilde olaya müdahale edemezken, devriye gezdiği sırada verileri anlık olarak polis merkezine iletebilmektedir. Bu sayede, önemli kamusal alanlarda güvenliğin sağlanması ve suç oranının azaltılması hedeflenmektedir[102].

Aynı amaçla kullanıma sunulan robot köpekler ise New York'ta test edilmiştir. New York Şehri Polis Teşkilatı (NYPD); hayat kurtarmaya, insanları korumaya yardımcı olmak amacıyla, uzaktan kumandalı *Digidog*'lar için Boston Dynamics firmasıyla bir sözleşme imzalamış, sonra yaşanan gelişmeler üzerine bu sözleşme sonlandırılmıştır. Ülkede yaşanan birtakım toplumsal hadiselerde, robot köpeklerin kullanılması (denenmesi) tepkilere yol açmış ve bu uygulamanın polis güçlerinin artan militarizasyonu olduğu, robot köpeğin distopik Black Mirror (Metalhead) serisinde yer alan varlıklara benzediği yönünde eleştiriler dile getirilmiştir[103].

Yine Amerika Birleşik Devletleri'nde ilk olarak Massachusetts Eyalet Polisi tarafından kullanılmaya başlanan *Spot* adı verilen robot polis köpeği, şüpheli paketleri araştırabilmekte ve şüphelinin nerede saklanabileceğini tespit edebilmektedir. Kendisine yönelik müdahalelere karşı dengesini koruyabilen, düştüğünde kendi başına kalkabilen bu köpekler, hızlı koşabilme ve ihtiyaç halinde karşısındakine saldırabilme özelliğine de sahiptir. Bu yönüyle, saldırganların durdurulması ve karşı konulması açısından da verimli bir yapıdadır[104].

Dubai'de, emniyet yetkilileri tarafından tanıtılan robot polis ise üzerindeki dokunmatik ekran sayesinde vatandaşların suç ihbarlarını alabilmekte ve ceza ödemelerini kabul edebilmektedir. Bunun yanında ihtiyaç duyulan çeşitli bilgileri sağlayabilen bu robot polisler, kentin çeşitli yerlerine konuşlandırılmaktadır. Bu uygulama sayesinde, insan polislerin daha kritik ve

---

[101] Zafer İçer – Elif Dönmez, Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları, Ceza Hukuku Dergisi, Yıl:15, Sayı: 43, Ağustos 2020, s. 422.

[102] Katie Flaherty, A RoboCop, A Park and A Fight: How Expectations About Robots are Clashing Reality, *NBC News*, 4 Ekim 2019, https://www.nbcnews.com/tech/tech-news/robocop-park-fight-how-expectations-about-robots-are-clashing-reality-n1059671, Erişim Tarihi: 01.12.2021.

[103] BBC, New York City Police Scrap 'Creepy' Robotic Dogs, 29 Nisan 2021, https://www.bbc.com/news/world-us-canada-56937657, Erişim Tarihi: 01.12.2021.

[104] Cumhuriyet, Robot Polis Köpekleri Göreve Başladı, 27 Kasım 2019, https://www.cumhuriyet.com.tr/video/robot-polis-kopekleri-goreve-basladi-1704607, Erişim Tarihi: 01.12.2021.

önemli yerlerde görevlendirilmesi ve böylelikle insan kaynağının daha verimli şekilde kullanılması mümkün olabilmektedir. Dubai'de, 2050 yılı itibarıyla polis kuvvetlerinin dörtte birinin robotlardan oluşması ve bu suretle kolluk faaliyetlerinin mevcut insan kaynağının güçlendirilmesi amaçlanmaktadır[105].

Çin'in Zhengzhou Tren İstasyonu'nda devriye görevi yapan ve *E-Patrol Robot Sheriff* adı verilen robot polislerin ise, polislik görevinin yanında hava kalitesini ve sıcaklığı ölçerek, kapalı alanlarda yangın tehlikesi ve benzeri riskli durumları önceden fark edip uyarılarda bulunabilmesi gibi farklı özellikleri göze çarpmaktadır[106].

Robot polislerin stabil versiyonu ise, yapay polis istasyonlarıdır. Mobilize olmayan bu istasyonların örneğine Çin'de rastlanmaktadır. Trafik düzeninin sağlanması ve suçluların yakalanması amacına hizmet eden ve tümüyle yapay zekâ destekli bir sistem tarafından yönetilen polis istasyonu, güvenlik kameralarıyla donatılan pek çok bölgede, yüz tanıma teknolojisi aracılığıyla suçluların ya da trafik ihlali yapanların tespit edilmesi ve yakalanmasında fayda sağlamaktadır[107].

1.2. Yüz Tanıma Teknolojileri

Yapay zekâ temelli öngörücü polislik uygulamalarının en çarpıcı ve yaygın örneğini yüz tanıma teknolojileri oluşturmaktadır. Bu teknoloji, kamusal alanlarda, meydanlarda, caddelerde bireylerin yoğun olarak bulundukları lokasyonlarda konumlandırılan yüksek çözünürlüklü kameralar ve yapay zekâ destekli sistemler aracılığıyla işlevsellik kazanmakta ve bu teknolojinin kullanımıyla suçların önlenmesi, potansiyel suçluların tespiti ve suç şüphesi altında bulunan şüphelilerin yakalanması amaçlanmaktadır[108].

Yüz tanıma teknolojisinde, yapay zekâ aracılığıyla, biyometrik bir veri olan insan yüzünün tespit edilip işleme konulması ve sistemdeki veriler ile mukayese edilerek belirli sonuçlara ulaşılması söz konusudur. Bu teknoloji üç basamaklı bir işlem silsilesini içermekte olup ilk etapta insan yüzleri kaydedilerek *(enrolment)* referans veri seti oluşturulmaktadır. İkinci aşamada tanımlama *(identification)* yapılmakta ve elde edilen referans veri ile stoktaki veriler

---

[105] BBC, Dubai'de İlk Robot Polis Göreve Başlıyor, 24 Mayıs 2017, https://www.bbc.com/turkce/haberler-40038611, Erişim Tarihi: 01.12.2021; Hitachi, Teknoloji, Suça Karşı Savaşta Silahımız, https://social-innovation.hitachi/tr-tr/stories/technology/hidden-weapon-in-the-fight-against-crime/, Erişim Tarihi: 01.12.2021.

[106] Milliyet, Robot Polisler, Devriye Görevine Başladı, 21.02.2017, https://www.milliyet.com.tr/teknoloji/robot-polisler-devriye-gorevine-basladi-2400315, Erişim Tarihi: 01.12.2021.

[107] LOG, Çin, Yapay Zekâ Tarafından Yönetilen İnsansız Polis İstasyonu Hazırlığında, 13 Kasım 2017, https://www.log.com.tr/cin-yapay-zeka-tarafindan-yonetilen-insansiz-polis-istasyonu-hazirliginda/, Erişim Tarihi: 01.12.2021.

[108] Ayrıntılı bilgi için bkz. İçer – Dönmez, s.421 vd.

mukayese edilmektedir. Son olarak, bu eşleşmelerin doğrulaması *(verification)* yapılmakta ve sistem bu süreç sonucunda belirli bir çıktı sağlamaktadır[109].

Almanya'da 2007 yılından bu yana, Federal Kriminal Polis Bürosu tarafından yüz tanıma teknolojileri test edilmektedir. 2017 yılında G20 zirvesinde çıkan olaylardan sonra bu sistemlerin kullanılması yasa dışı kabul edilmiş ve eyalet polisi yasasında var olan video kayıtlarının otomatik değerlendirilmesine yönelik birtakım düzenlemelerin, yüz tanıma teknolojilerinin kullanımını meşrulaştırmadığı ifade edilmiştir[110].

İngiltere menşeili *WeSee* firması, insanların tespit edemeyeceği ayrıntıları yakalayarak şüpheli kişileri yüz ifadelerinden belirleyebilen yapay zekâ tabanlı bir teknoloji geliştirmiştir. Şüpheli kişilerin ifadeleri ve yüzlerinin veri kaynağı olarak kullanıldığı ve bu verilerin yüksek çözünürlüklü kameralar aracılığıyla en ince detayına kadar elde edilebildiği teknoloji sayesinde, insanların duruşlarından, jest ve mimiklerinden, duygu durumu tespiti yapılması ve niyetlerinin okunması amaçlanmaktadır. Şüpheli davranışların hızlı bir şekilde belirlenmesi ve böylelikle suçun işlenmesinin önüne geçilmesi hedefiyle geliştirilen teknoloji, örneğin terörist saldırı gerçekleştirme potansiyeli bulunan bir kişinin yapay zekâ tarafından hızlıca tespit edilmesini sağlamakta ve böylelikle kolluk güçlerinin vakit kaybetmeksizin ilgili kişi üzerinde önleyici tedbirleri uygulayabilmesine imkân tanımaktadır[111].

İngiltere'nin çeşitli bölgelerinde hayata geçirilen bu uygulamalar, etik ve hukuki tartışmaları beraberinde getirmiştir. Bilhassa insan hakları savunucuları, yüz tanıma teknolojisinin kamusal alanlarda kullanımının yalnızca kişisel verileri ihlal etmediğini, bu uygulamanın rıza dışı parmak izi alınması ya da DNA analizi yapılması ile eş değer olduğunu ve bunun kişi haklarını ihlal ettiğini ileri sürmüşlerdir[112].

İtalya'da ise, kişisel verilere yönelik müdahale oluşturması sebebiyle, yüz tanıma teknolojilerinin halka açık yerlerde genel olarak kullanılması yasaklanmış; ancak istisnai olarak, suçun önlenmesi ve suçla mücadele amacıyla bu sistemlerin kullanılmasına pozitif düzenlemelerde izin verilmiştir[113].

Konuyla ilgili bir diğer tartışma, yüz tanıma teknolojisinden kaçınmak amacıyla kişilerin çeşitli önlemler almaları üzerine gündeme gelmiştir. İngiltere'nin Romford bölgesinde polis tarafından yapılan uygulamalarda, yüz tanıma teknolojisine sahip kameraların bulunduğu alanlara giren kişilerin kameralar tarafından taranmayı reddetmeleri üzerine haklarında idari para cezası uygulanması, bu davranışa yaptırım uygulanıp uygulamayacağı ile ilgili hukuki

---

[109] İçer – Dönmez, s.425.
[110] İçer – Dönmez, s.423.
[111] Daniel Thomas, Niyet Okuma Teknolojisi: Polisler Duygularınızı Yüz Tanıma Sistemiyle Tespit Edebilecek, BBC, 18 Temmuz 2018, https://www.bbc.com/turkce/haberler-dunya-44865198, Erişim Tarihi: 01.12.2021.
[112] Clive Coleman, Police Facial Recognition Surveillance Court Case Starts, BBC, 21 Mayıs 2019, https://www.bbc.com/news/uk-48315979, Erişim Tarihi: 01.12.2021.
[113] Italy24 News, Facial Recognition Prohibited in Italy: But Only for Now and Exceptions, 2 Aralık 2021, https://www-italy24news-com.cdn.ampproject.org/c/s/www.italy24news.com/News/amp/286487, Erişim Tarihi: 06.12.2021.

tartışmaları beraberinde getirmiş; kişilerin yüzlerini örtmelerinin bir hak olup olmadığı sorusu sorulmuştur[114]. Özellikle COVID-19 pandemisi sürecinde maske kullanımının artması sebebiyle bu tartışmalar artarak devam etmiştir. Maske takılmasının, yüz tanıma teknolojilerinin etkinliğini belirli bir ölçüde azalttığı tespit edilse de[115], bazı teknoloji şirketleri maske takan kişilerin yüzlerini yüzde 99,9'luk bir başarıyla tanıyabilen sistemler geliştirerek bu konudaki tartışmaları başka bir boyuta taşımıştır[116].

Yalnızca yüz verisinden değil, ses ve göz bebeğindeki iristen ve hatta yürüyüş şeklinden kişileri tanıyıp ayrıştırabilecek, suçlu ve şüphelileri tespit edilebilecek kamera destekli tanıma sistemleri de bulunmakta olup Rusya İçişleri Bakanlığı tarafından bu özellikleri haiz bir sistemin 2021 yılının sonlarına doğru kullanımına başlanmasının planlandığı duyurulmuştur[117] .

Bu gelişmeler, uzaktan görüntüleme yapabilme özelliğine sahip beyin görüntüleme teknolojilerinin kullanılması ihtimalini de gündeme getirmektedir. Suçun önlenmesi ve suçluların tespitinde kullanılan bu teknolojilerin, kişilerin nörolojik özellikleri, beyin haritası ve nöral ağ yapıları gibi veri kaynaklarından yararlanabilmesi durumunda, uygulamaların başarı oranının artacağında şüphe yokken; bilişsel özgürlüğe[118] müdahale oluşturan bu uygulamalar, konunun kaotik ve distopik bir yapıya bürünmesine de zemin oluşturacaktır[119].

1.3. Potansiyel Suçları Tahmin Eden Yazılımlar

Toplum güvenliğinin sağlanması amacıyla, bazı global firmalar suç öngörme yazılımı adı altında çeşitli yapay zekâ uygulamaları geliştirdiklerini açıklamıştır. *Hitachi* şirketi, CCTV kameralar, toplu ulaşım haritaları, hava durumu raporları ve hatta sosyal medya yayınları gibi büyük bir veri kaynağı ağından alınan büyük miktardaki verileri hızla inceleyerek belirli bir bölgede suçların nerede işlenmesinin daha muhtemel olduğunun öngörülebildiğini duyurmuştur. Şirket bu teknolojinin en önemli özelliğinin, suçun öngörülmesiyle ilgili verilerin analizi konusunda insani önyargıların bertaraf edilmesi olduğunu, makine öğrenimi

---

[114] Lizzie Dearden, Police Stop People for Covering Their Faces from Facial Recognition Camera Then Fine Man £90 after He Protested, Independent, 31 Ocak 2019, https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html, Erişim Tarihi: 01.12.2021.

[115] TRT Haber, Maskeler, Yüz Tanıma Sistemlerinin Kafasını Karıştırdı, 29 Temmuz 2020, https://www.trthaber.com/haber/dunya/maskeler-yuz-tanima-sistemlerinin-kafasini-karistirdi-505480.html, Erişim Tarihi: 01.12.2021.

[116] BBC, Facial Recognition Identifies People Wearing Masks, 7 Ocak 2021, https://www.bbc.com/news/technology-55573802, Erişim Tarihi: 01.12.2021.

[117] Sputnik Türkiye, Rusya'da Suçluları Bulabilmek İçin Yeni Kamera Tanıma Sistemi: Ses, Göz, Dövmeden Tespit Yapılabilecek, 26.02.2020, https://tr.sputniknews.com/20200226/rusyada-suclulari-bulabilmek-icin-yeni-kamera-tanima-sistemi-ses-goz-dovmeden-tespit-yapilabilecek-1041478197.html, Erişim Tarihi: 01.12.2021.

[118] Mehmet Ergen & Yeşim Işıl Ülman, Nörobilim, Nöroteknoloji, Yalan Tespiti ve Etik, Acıbadem Üniversitesi Sağlık Bilimleri Dergisi, Cilt: 3, Sayı: 3, Temmuz 2012, s.153.

[119] Zafer İçer, Yapay Zekâ Destekli Nörohukuk Sisteminde Suç ve Cezaya Yaklaşım, XI. Eğitim Denetimi Kongresi (5-7 Aralık 2019, Antalya), Eğitim, Hukuk ve Yapay Zekâ Bildiri Kitabı, s.112.

teknolojisi sayesinde yalnızca veriler kullanılarak hareket edildiğini, bu öngörülerden hareketle, şehirler dâhilinde sıklıkla suç işlenen noktaları gösteren ısı haritalarının oluşturulduğunu ve böylece kaynakların suça tepki vermek yerine, suçu önleyecek şekilde kullanılmasının mümkün hâle getirildiğini açıklamıştır[120].

Tahmine dayalı polislik teknolojisine dair bir diğer ilgi çekici örnek olarak *Palantir*[121] *Technologies* adlı bir şirketin New Orleans'taki uygulamalarını göstermek mümkündür. Şirket, insanların suç örgütleriyle bağlantılarını izleyen, suç geçmişlerini özetleyen, sosyal medyayı analiz eden ve bireylerin şiddet uygulama veya mağdur olma ihtimalini tahmin eden gizli bir polis departmanı programına yazılım sağlamış ve bu kapsamda şehirde silahlı şiddete karışma riski en yüksek olan yaklaşık 3900 kişilik bir liste hazırlanmıştır[122].

İngiltere'nin West Midlands bölgesindeki polis teşkilatının, ciddi şiddet içeren suçların önceden tahmin edilip meydana gelmeden durdurulması amacıyla, *Ulusal Veri Analiz Çözümü (NDAS)* adı verilen yeni bir yapay zekâ yazılımının üzerinde çalıştığı basına yansımıştır. Bu yazılım sayesinde bir kişinin potansiyel suç işleme durumunu eldeki veriler ve istatistiklerle tespit edebilmenin ve suç işlenmeden suçun engellenmesinin amaçlandığı belirtilmiştir[123].

Avrupa'nın çeşitli ülkelerinde suçla etkin mücadele politikası kapsamında, öngörücü polislik uygulamaları denenmeye ve kullanılmaya başlanmıştır. Özellikle terörle mücadele kapsamında, terör riskini hesaplayan bazı yapay zekâ destekli uygulamalar, kolluk faaliyetlerine entegre edilmeye çalışılmaktadır[124]. İdari mercilerin öngörücü polislik uygulaması geliştirmesi için çeşitli teknoloji firmaları ile anlaşmaları ve bu konudaki iş birliklerini geliştirmeleri, bu yöndeki adımların önemli bir parçasını oluşturmaktadır[125].

Toplumun genel güvenliğinin ve asayişin sağlanması için kullanımına başlanan uygulamalara da rastlanmak mümkündür. Almanya'nın bazı kentlerinde, bölgesel ve zamansal olarak

---

[120] bkz. dn. 105.

[121] Palantir, J.R.R. Tolkien'in yarattığı kurgu evrenin bir parçası olan Orta Dünya'da yer alan ve birbirleriyle bağlantı hâlinde olan, kullanıldıklarında diğer taşlarla bağlantıya geçerek onların yakınını görmeye imkân sağlayan görme taşlarıdır. Etimolojik olarak Sindarin lisanında "uzakları gösteren" anlamına gelmektedir.

[122] Ali Winston, Palantir has secretly been using New Orleans to test its predictive policing technology, The Verge, 27 Şubat 2018, https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd, Erişim Tarihi: 01.12.2021.

[123] Milliyet, İngiliz Polisi Suçu Önlemek İçin Yapay Zekâ Kullanacak, 29 Kasım 2018, http://www.milliyet.com.tr/teknoloji/ingiliz-polisi-sucu-onlemek-icin-yapay-zeka-kullanacak-2786584, Erişim Tarihi: 01.12.2021; Hürriyet, Azınlık Raporu filmi gerçek oluyor! Suçu işlenmeden önleme dönemi başlıyor, 29 Kasım 2018, http://www.hurriyet.com.tr/avrupa/azinlik-raporu-filmi-gercek-oluyor-sucu-islenmeden-onleme-donemi-basliyor-41035280, Erişim Tarihi: 01.12.2021.

[124] Sözüer, Öngörücü Kolluk, s.5.

[125] Örneğin Fransa'da Nice kentinin yerel makamları, *Thales* isimli bir savunma teknolojisi ile terör saldırılarını hesaplayabilecek bir öngörücü kolluk uygulaması geliştirmesi için anlaşmıştır. Bkz. La Quadrature du Net, In France, Smart City Policing is Spreading Like Wildfire, 17 Ağustos 2018, https://www.laquadrature.net/en/2018/08/17/smartcity_policing_like_wildfire/, Erişim Tarihi: 01.12.2021; Sözüer, Öngörücü Kolluk, s.5.

hırsızlık suçunun işlenme olasılığını hesaplayan *Precobs* isimli yazılım kullanılırken[126], Hollanda'nın Amsterdam kentinde "suç öngörme sistemi" adı altında, zamana ve mekâna dayalı olarak suçun işlenme riskini tahmin edebilen bir uygulama hayata geçirilmiştir[127].

1.4. Spesifik Suçların Önlenmesine Yönelik Uygulamalar

Kamusal alanlarda asayişin sağlanması ve klasik suçların önlenmesi amacının yanında, çeşitli yazılımlar aracılığıyla spesifik suçların önüne geçilmesine yönelik uygulamalar da geliştirilmektedir. MIT'de görevli bilim insanları, vergi kaçakçılığının tümüyle önlenmesinin ve vergi kaçıranların otomatik olarak tespit edilebilmesinin ancak yapay zekâ yazılımları ile mümkün olabileceğini dile getirmektedir[128].

ABD'de, *QuantaVerse* firması, finansal suçların önüne geçebilmek, mali kurumların ve banka müşterilerinin dolandırıcılığa karşı korunmasını sağlamak amacıyla *CAE Checkup* isimli yapay zekâ sistemini geliştirmiştir[129].

Ülkemizde Tarama Ağı Projesi ile yapay zekâ ve makine öğrenmesi teknolojileri kullanılarak araç veya yükün içerisindeki belirli özelliklere sahip yasa dışı unsurları otomatik tanımlayacak bir sistemin uygulamaya konulduğu bildirilmiştir. Ticaret hacmi yüksek gümrük kapısı ve limanlara kurulan *X-Ray Araç ve Konteyner Tarama Sistemi* sayesinde, araç ve konteynerlerin röntgen filminin çekilerek saatlerce süren gümrük kontrollerinin dakikalar içinde hızlı ve nitelikli olarak gerçekleşmesinin sağlanacağı ve böylece gümrük kaçakçılığı suçunun önüne geçileceği kaydedilmiştir[130].

Karapara aklamanın önüne geçilmesi amacıyla büyük şirketlere yazılım hizmeti sunan *fintech/regtech* girişimleri de bulunmakta olup bu girişimler, firmaların finansal suçlarla mücadele edebilmesine ve regülasyonlara uyum süreçlerini destekleyen çözümler üretebilmesine olanak sağlayan yapay zekâ tabanlı çözümler sunmaktadır. Şirketleri finansal suçlarla karşı karşıya kalmaktan koruyan ve yasaya uygun faaliyet göstermelerine yardımcı olan bu girişimler, yapay zekâ destekli çözümler sunarak şirketlerin ticari ve finansal faaliyetlerinin sorunsuz gerçekleştirilebilmesine imkan sağlamaktadır. Bu girişimlerden biri olan *Sanction Scanner,* veritabanında 200'den fazla ülkenin yasaklılar, arananlar ve siyasi nüfuz sahibi kişiler gibi yüksek risk teşkil eden kişilerin verilerini barındırmakta ve tüm bu verileri gerçek zamanlı olarak izleyerek yapay zekâ desteği ile yapılandırmaktadır. Gelişmiş

---

[126] Dominik Gerstner, Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in BadenWürttemberg, Germany, European Journal for Security Research, Cilt: 3, Sayı: 2, 2018, s.119, https://link.springer.com/article/10.1007/s41125-018-0033-0, Erişim Tarihi: 09.12.2021.

[127] Sözüer, s.5.

[128] CNN Turk, Vergi Kaçıranlar Yapay Zekâ ile Tespit Edilecek, 11 Ekim 2015, https://www.cnnturk.com/teknoloji/vergi-kaciranlar-yapay-zeka-ile-tespit-edilecek , Erişim Tarihi: 01.12.2021.

[129] Fintech Istanbul, Finansal Suçları Engellemek İçin Yapay Zekâ Devrede, 26 Aralık.2017, https://fintechistanbul.org/2017/12/26/finansal-suclari-engellemek-icin-yapay-zeka-devrede/ , Erişim Tarihi: 01.12.2021.

[130] BTHaber, Kaçakçılığa Karşı Yapay Zeka Taraması, 5 Aralık 2019, https://www.bthaber.com/kacakciliga-karsi-yapay-zeka-taramasi/ , Erişim Tarihi: 01.12.2021.

algoritmalar ve ikili sınıflandırma *(binary classification)* gibi yöntemlerle aynı kişiye ait farklı listelerdeki verileri toplayıp bunları tek bir profil altında göstererek şirketleri uyarabilmekte ve şirketlerin risk değerlendirmelerini çok kısa bir zaman içerisinde yerine getirmelerine yardımcı olmaktadır[131].

2. Önleyici Uygulamaların Avantajları ve Dezavantajları

Yapay zekâ temelli öngörücü ve önleyici polis uygulamaları, tüm dünyada iç güvenliğin sağlanması, bilhassa terörizmle mücadele kapsamında gelişmekte ve yaygınlaşmaktadır. Bu gelişme, son yıllarda önleyici ceza hukuku *(preventive criminal law)* kavramının ortaya çıkmasına yol açmıştır[132]. Günümüzde artık ülkeler suç işlendikten sonra değil, suç işlenmeden önce etkin tedbirlerin alınmasını tercih etmekte ve bu tercihi bireyin hak ve hürriyetlerini, kamu düzen ve barışını koruma hedefiyle hayata geçirmektedir. Suçun önlenmesinde teknolojinin kullanımı İngiltere'de "hayati" ve "mükemmel bir silah" olarak kabul edilirken[133], Amerika Birleşik Devletleri'nde bu sistemlerin kullanımının kolluk süreçleri açısından "paha biçilmez" olduğu ifade edilmektedir[134].

Önleyici ceza hukuku uygulamalarının temel amacı, suçun henüz işlenmeden önce engellenmesidir. Suç işlendikten sonra önleyici ceza hukuku tedbirleri devre dışı kalmakta, onun yerini suç şüphesine dayalı şekillenen ceza muhakemesi süreci almaktadır. Siyasi ve toplumsal gelişmelere bağlı olarak, zaman zaman ülkeler, hak ve özgürlüklere müdahalenin şartlarının zorlaştırıldığı özgürlükçü bir anlayış benimseyebilmekte iken, kimi zaman da yine aynı sebeplere bağlı olarak güvenliğin sağlanması noktasında proaktif bir yaklaşım sergileyebilmektedir. Bu yaklaşım doğrultusunda ülkeler, toplumun güvenliğini sağlamak amacıyla vatandaşlarını potansiyel risk faktörü olarak tanımlamak suretiyle önleyici ceza hukuku uygulamalarına[135] ağırlık verebilmektedir[136].

Şüphesiz, teknolojide yaşanan değişim ve teknolojinin sağladığı imkanlar, önleyici ceza hukuku anlayışının elini güçlendirmiştir. Özellikle yapay zekâ destekli uygulamalar, suçun önlenmesi açısından pratik faydalar sağladığından, bu imkânın kullanılması en kolay ve ilk tercih edilen yöntem olarak ön plana çıkmaktadır. Bu uygulamaların kullanılması, suçların

---

[131] Sanction Scanner, https://sanctionscanner.com/ (Erişim Tarihi: 01.12.2021); Türkiye Yapay Zeka İnisiyatifi, Finansal Suçlara Karşı Yapay Zekalı Çözümler Sunuyoruz, 20 Temmuz 2020, https://turkiye.ai/finansal-suclara-karsi-yapay-zekali-cozumler-sunuyoruz/ , Erişim Tarihi: 01.12.202.

[132] Ali Emrah Bozbayındır, The Advent of Preventive Criminal Law: An Erosion of the Traditional Criminal Law?, Criminal Law Forum-The Official Journal of the Society for the Reform of Criminal Law, Cilt:29, Sayı:1, 2018, s. 35-48.

[133] Gov.uk Surveillance Camera Commissioner's IFSEC Speech, 27 Haziran 2016, https://www.gov.uk/government/speeches/surveillance-camera-commissioners-ifsec-speech , Erişim Tarihi: 01.12.2021.

[134] Matthew P.J. Ashby, The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis, European Journal on Criminal Policy and Research, 2017, Cilt:23, s.1.

[135] Bunun en somut örneğini, Amerika Birleşik Devletleri'nde yaşanan 11 Eylül saldırısı sonrasında, pek çok ülkede hayata geçirilen önleyici ceza hukuku uygulamaları oluşturmaktadır.

[136] İçer – Dönmez, s.435.

önlenmesine yardımcı olmasının yanı sıra; insan, araç ve malzeme kaynağının daha verimli kullanılması, zaman ve emekten tasarruf gibi polis teşkilatı ve kolluk birimlerinin faaliyetleri bakımından da kayda değer avantajlar sağlamaktadır.

Öte yandan, yapay zekânın kullanıldığı her alanda olduğu gibi, önleyici uygulamalar bakımından da bu sistemlerin kullanılması bazı riskleri beraberinde getirmektedir. Bunlardan ilki, sistemin hatalı sonuçlar üretme riskidir. Örneğin yüz tanıma sistemlerinde ışık, hava koşulları gibi dış faktörlerin, sistemin hatalı sonuçlar üretmesine yol açabileceği ifade edilmektedir[137]. Bir başka örnek olarak, COVID-19 pandemi sürecinde maske kullanımı, yüz tanıma teknolojilerinin hata oranını arttırmıştır[138]. Dolayısıyla dış dünyadaki değişkenler, algoritmik yanılgılara yol açabilmektedir. Yapay zekâ sistemlerin mutlak kesinlik arz eden sonuçlar üretmesinin günümüzde zor olduğu, bunun için kusursuz algoritmalara ihtiyaç duyulduğu ifade edilmekte ise de, her geçen gün yapay zekâ algoritmalarının geliştirilmesine yönelik önemli çalışmaların yapıldığı bilinmektedir. Bu alandaki çalışmalar geliştikçe, hata payının azalacağı ve yapay zekâ temelli uygulamaların her geçen gün kusursuza yakın bir işlevsellik ortaya koyacağı öngörülebilir.

Bir diğer risk, yapay zekâ sistemlerine yönelik harici müdahalelerdir. Bu uygulamalar verileri algılayarak çeşitli sonuçlar ürettiğinden, veri manipülasyonu yoluyla sisteme yönelik saldırılar gerçekleştiğinde sistem hatalı sonuçlar üretebilecek ve bu durum suçla mücadelede zafiyet meydana getirebilecektir.

Önyargılı analizler, sistemlerin bir diğer zayıf noktasıdır. Örneğin yüz tanıma teknolojilerinde, referans veri setlerinin beyaz ırktan insanların yüzleriyle oluşturulduğu ve sistemin başka ırkları tanımakta zorlandığı ve hatalı sonuçlar üretebildiği gözlemlenmiştir[139]. Özellikle *Google, Amazon, Uber* gibi şirketler tarafından çeşitli amaçlarla kullanılan bu uygulamaların ırkçı analizlerde bulunduğu yönünde iddialar gündeme gelmiştir[140].

Potansiyel suçluların tespiti ve suçun önlenmesinde kullanılacak bu uygulamaların önyargılı sonuçlar üretmesi, masum kimselerin çeşitli önleyici ve bastırıcı tedbirlere tabi olması gibi son derece tehlikeli sonuçlar doğurabilecektir. Nitekim bu hususta en yaygın endişe, tahmine dayalı polisliğin, kolluk kuvvetlerinin tarihsel olarak sahip olduğu önyargıları basitçe yeniden üretip büyütmekle birlikte, bu karar verme sürecini çok az kişinin anladığı gelişmiş

---

[137] İçer – Dönmez, s.429.

[138] TRT Haber, Maskeler Yüz Tanıma Sistemlerinin Kafasını Karıştırdı, 29 Temmuz 2020, https://www.trthaber.com/haber/dunya/maskeler-yuz-tanima-sistemlerinin-kafasini-karistirdi-505480.html, Erişim Tarihi: 01.12.2021.

[139] The Guardian, What is facial recognition and how sinister is it?, 29 Temmuz 2019, https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it , Erişim Tarihi: 01.12.2021.

[140] BBC, Yapay Zeka: Irkçı Algoritmalardan Nasıl Kaçınırız?, 15 Nisan 2017, https://www.bbc.com/turkce/haberler-dunya-39599214 (Erişim Tarihi: 01.12.2021); https://nayn.co/amazona-irkcilik-suclamasi-yuz-algilama-servisi-cinsiyetci-ve-irkci/ , Erişim Tarihi: 01.12.202. ; Sabah, ABD'de Yüz Tanıma Tekniği Irkçı Çıktı, 31 Temmuz 2018, https://www.sabah.com.tr/dunya/2018/07/31/abdde-yuz-tanima-teknigi-irkci-cikti , Erişim Tarihi: 01.12.2021.

yazılımlarla filtreleyerek önyargılı kolluk uygulamalarına haksız meşruiyet kazandıracağı düşüncesidir[141].

Yapay zekâ temelli uygulamalar, kesin nitelikte olmayan, tahmin ve olasılığa dayalı sonuçlar ürettiğinden bu uygulamaların ortaya koyduğu sonuçların insan tarafından rasyonel şekilde değerlendirilmesinde fayda ve gereklilik bulunmaktadır. Kesin sonuçlar ortaya koyamaması sebebiyle yapay zekâ temelli uygulamaların, önleyici ve öngörücü polislik alanında destek sistemler olarak kabul edilmesi şarttır. Bu sistemin insanların kontrol ve gözetiminde kullanılması, nihai olarak alınacak kararlar ve uygulanacak tedbirlerin bir insan kararına dayandırılması, hesap verilebilirliğin sağlanması ve olası negatif sonuçlarda sorumluluğun gerçek bir kimseye yüklenebilmesi bakımından önem arz etmektedir.

3. Uygulamaların Haklar Alanında Meydana Getirdiği Sorunlar

Yapay zekâ temelli önleyici/öngörücü polislik uygulamaları, hareket serbestisi başta olmak üzere, bireylerin temel hak ve hürriyetlerini savunmasız bırakabilmektedir. Bu uygulamalar, önleyici kolluk mekanizmaları olarak kullanılabilir olmakla beraber, bu müdahale tarzlarının hukuki açıdan belirginleştirilmesi, hukuk güvenliğinin sağlanması açısından elzemdir ve hukuk devleti olmanın bir gereğidir[142].

Kamu gücü tarafından uygulamaya konulan bu mekanizmalar, başta kişisel veriler olmak üzere, bireye ait pek çok hak ile yakından ilişkilidir. Ses, görüntü algılamak suretiyle veri işlenmesine ve çıktılar elde edilmesine imkân tanıyan bu sistemler, kişilerin verilerini kaynak olarak kullanmaktadır. Bilhassa yüz verisi, hatta gözbebeğindeki irisi ayrıştırabilecek kadar benzersiz biyometrik verileri işleyebilen bu sistemler, bireyin en özel/giz alanına yönelik müdahaleleri beraberinde getirmekte ve bu hallerde ihlalin ağırlığı artmaktadır.

Özünde, özel hayatın gizliliği ve özel hayata saygı hakkının bir unsuru olan kişisel verilerin gizliliği ve korunması hakkı, başka bağımsız ve bağlantılı haklarla ilişki içindedir. Bunlardan biri olan "otomatik veri işleme faaliyetine dayalı bir karara tabi olmama hakkı", kişisel verilerin korunması hakkı bünyesinde, AB Genel Veri Koruma Tüzüğü'nde (m.22) öngörülen yeni bir tür hak olup buna göre, veri sahibi, kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkına sahiptir. Yapay zekâ tabanlı öngörücü uygulamalar, bu hak yönünden ciddi bir risk teşkil etmekte ve insan unsurunun tümüyle ya da kısmen devre dışı kaldığı pek çok karar mekanizmasına temel oluşturmaktadır. Bu durum, insan iradesi ve kontrolünden bağımsız olarak otomatik veri işleme sonucu, bireylerin çeşitli müdahalelere maruz kalma tehlikesini beraberinde getirmektedir.

---

[141] Kristian Lum – William Isaac, To predict and serve?. Significance, 13: 14-19, 2016, s. 19. https://doi.org/10.1111/j.1740-9713.2016.00960.x , Erişim Tarihi: 01.12.2021.

[142] Veli Özer Özbek – Koray Doğan – Pınar Bacaksız, Ceza Muhakemesi Hukuku, Ankara, 2019, s. 175; İçer – Dönmez, s.422.

Kişisel verilerin korunması hakkı ile bağlantılı haklardan bir diğeri de, yeni bir alt hak kategorisi olarak nitelendirebileceğimiz "kişisel verilerin akıbetini belirleme hakkı"dır. Alman Anayasa Mahkemesi, kişisel verilerin kaderini tayin hakkını, genel kişilik hakkının uzantısı olarak nitelendirmekte ve bu hakkın, bireyin kişisel verilerinin sınırsız şekilde toplanması, depolanması, kullanılması ve aktarılmasına karşı korunmasını da kapsadığını belirtmektedir[143] . Şu hâlde, bilhassa kişisel verilere yönelik müdahale oluşturan önleyici kolluk uygulamaları, bireylerin özel hayatının gizliliğine ve genel kişilik hakkına yönelik kapsamlı bir müdahaleyi içerisinde barındırmaktadır.

Daha geniş bir perspektiften değerlendirme yapılacak olursa, kişisel verilerin korunması hakkından bağımsız olan "bireyin kendini yönetme", "maddi ve manevi varlığını geliştirme hakkı" kapsamında, "serbest bir yaşam sürme" ve "rahatsız edilmeme hakkı" da büyük ölçüde bu uygulamalardan etkilenmektedir. Bu hakkın getirdiği bir sonuç olarak devletin, vatandaşların özel alanına müdahale etmemesi ve bu alanın uygulamaların kapsamının dışında bırakılması oldukça önemlidir. Ancak her hakka yönelik olduğu gibi, bu hakka yönelik müdahalelerin de belirli şartlar altında meşru sayılabilmesi olanak dahilindedir. Bu uygulamaların müdahale oluşturduğu yeni tür hakların, demokratik bir toplumda ve bir hukuk devletinde, kamu güvenliğinin, kamu düzeninin, başkalarının hak ve özgürlüklerinin korunması için gerekli sınırlamalara tabi tutulabileceğinde tereddüt yoktur. Bu noktada belirli bir dengenin gözetilmesi gerekmekte olup uygulamaların belirli, öngörülebilir şartlara tabi tutularak ölçülü şekilde uygulamaya konulması elzemdir. Buradaki temel sorun, bu müdahalenin şartlarının doğru bir biçimde belirlenmesi ve sahadaki somut uygulamaların buna uygun olarak şekillendirilebilmesidir. Şüphesiz, benimsenen veya tercih edilen yöntem, o ülkenin hukuk standardının seviyesinin belirlenmesinde önemli bir kriter oluşturacaktır.

Sonuç ve Değerlendirme

Hemen her alanda insan tarafından icra edilen işleri kolaylaştırıcı işleve sahip olan yapay zekâ sistemleri, suçu önleyici faaliyetler bağlamında da kolluk kuvvetlerine yeni olanaklar sağlamaktadır. Yapay zekâ temelli önleyici hukuk mekanizmaları başlığı altında ele alınan bu uygulamaların en önemlisini, büyük veriden faydalanılmak suretiyle suçun, suçlunun önceden başarılı bir şekilde tahmin edilmesi ve bu sayede suçların önlenmesini hedefleyen, yapay zekâ temelli öngörücü polislik uygulamaları oluşturmaktadır.

Robot polisler ve yapay polis istasyonları, insansız önleyici devriye uygulamalarına ve güvenliğin mobilize bir özellik kazanmasına imkân sağlarken; yüz tanıma sistemleri, tahmin algoritmaları ve veri trafiği izleme uygulamaları da potansiyel suçların erkenden teşhis edilerek önlenmesini mümkün kılmaktadır. Kolluk faaliyetlerini kolaylaştıran ve kamu düzeninin sağlanmasında son derece etkili sonuçlar doğurabilen bu uygulamalar, insan, araç

[143] İçer – Dönmez, s.444.

ve malzeme kaynağının verimli kullanılması gibi ek faydaları ile birlikte güvenlik siyaseti açısından vazgeçilemeyecek avantajlar sunmaktadır.

Bu avantajlarına rağmen, güvenliğin sağlanması ve suçun önlenmesi amacıyla geliştirilen yapay zekâ temelli öngörücü mekanizmaların, yasal düzenlemeler yoluyla, hak ve özgürlük-güvenlik arasındaki denge gözetilerek uygulamaya konulması, bu mekanizmaların meşruiyet kazanabilmesi bakımından olmazsa olmaz bir koşuldur. Aynı zamanda bu kriterler, hukuk devleti ilkesinden sapılmaması adına da son derece önemlidir.

Öngörücü polislik uygulamalarının, suçun önlenmesine imkân tanıyan avantajlarının yanında, pek çok etik ve hukuki riski bünyesinde ihtiva etmesi, bu uygulamalara mesafeli yaklaşılmasının en temel gerekçesini oluşturmaktadır. Öngörücü polisliğin barındırdığı bu risklerin, temel olarak hukuka aykırı delil yasağına, kişinin kendi aleyhine delil vermeye zorlanamaması ilkesine *(nemo tenetur),* özel hayata saygı hakkına ve ayrımcılık yasağına ilişkin olduğunu söylemek mümkündür. Öte yandan, yapay zekâ sistemlerinin harici müdahaleler yoluyla manipüle edilebilir olması, önleyici faaliyetlerin amacından sapmasının yolunu açmakta ve sistemlerin güvenilirliğinin sorgulanmasına sebebiyet vermektedir.

Tüm risklerin ortaya koyduğu sonuç; teknolojinin geldiği nokta itibarıyla yapay zekâ temelli önleyici hukuk mekanizmalarıyla elde edilen verilerin kesin nitelikte olamayacağı ve otomatik sistemlerin tek başına kolluk faaliyeti icra etmelerinin hukukun evrensel ilkeleriyle bağdaşmayacağıdır. Bu itibarla, yapay zekâ temelli önleyici hukuk uygulamalarının destek sistemler olarak kullanılması, son tahlilde bireyin haklarına yönelik müdahalenin insan kararına dayandırılması ve suç izleme faaliyetlerinde asli unsurun insan olmaya devam etmesi, şeffaflık, hesap verilebilirlik ve hukuki sorumluluk açısından olası problemlerin önüne geçecek, aynı şekilde teknolojik risklerin minimizasyonu bakımından da fayda sağlayacaktır.

Kaynakça

Ashby, Matthew P.J., (2017), "The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis", European Journal on Criminal Policy and Research, Cilt:23.

BBC (2017). Dubai'de İlk Robot Polis Göreve Başlıyor, 24 Mayıs 2017, https://www.bbc.com/turkce/haberler-40038611, Erişim Tarihi: 01.12.2021.

BBC (2017). Yapay Zeka: Irkçı algoritmalardan nasıl kaçınırız?, 15 Nisan 2017, https://www.bbc.com/turkce/haberler-dunya-39599214, Erişim Tarihi: 01.12.2021.

BBC (2021). Facial Recognition İdentifies People Wearing Masks, 7 Ocak 2021, https://www.bbc.com/news/technology-55573802, Erişim Tarihi: 01.12.2021.

BBC (2021). New York City Police Scrap 'Creepy' Robotic Dogs, 29 Nisan 2021, https://www.bbc.com/news/world-us-canada-56937657, Erişim Tarihi: 01.12.2021.Bozbayındır, A.E., (2018), "The Advent of Preventive Criminal Law: An Erosion of the Traditional Criminal Law?" Criminal Law Forum-The Official Journal of the Society for the Reform of Criminal Law, Cilt:29, Sayı:1.

BTHaber (2019). Kaçakçılığa Karşı "Yapay Zekâ" Taraması, 5 Aralık 2019, https://www.bthaber.com/kacakciliga-karsi-yapay-zeka-taramasi/, Erişim Tarihi: 01.12.2021.

Centel, N. (2001). Cezanın Amacı ve Belirlenmesi, Turhan Tufan Yüce'ye Armağan, İzmir, Dokuz Eylül Üniversitesi Yayınları.

CNN Turk (2015). Vergi Kaçıranlar Yapay Zekâ ile Tespit Edilecek, 11 Ekim 2015, https://www.cnnturk.com/teknoloji/vergi-kaciranlar-yapay-zeka-ile-tespit-edilecek, Erişim Tarihi: 01.12.2021.

Coleman, C. (2019). Police Facial Recognition Surveillance Court Case Starts, BBC, 21 Mayıs 2019, https://www.bbc.com/news/uk-48315979, Erişim Tarihi: 01.12.2021.

Cumhuriyet (2019). Robot Polis Köpekleri Göreve Başladı, 27 Kasım 2019, https://www.cumhuriyet.com.tr/video/robot-polis-kopekleri-goreve-basladi-1704607, Erişim Tarihi: 01.12.2021.

Dearden, L. (2019). Police Stop People for Covering Their Faces from Facial Recognition Camera Then Fine Man £90 after He Protested, Independent, 31 Ocak 2019, https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html, Erişim Tarihi: 01.12.2021.

Ergen, M. – Ülman, Y. I. (2012). Nörobilim, Nöroteknoloji, Yalan Tespiti ve Etik, Acıbadem Üniversitesi Sağlık Bilimleri Dergisi, Cilt: 3, Sayı: 3.

Fintech İstanbul (2017). Finansal Suçları Engellemek İçin Yapay Zeka Devrede, 26 Aralık 2017,

https://fintechistanbul.org/2017/12/26/finansal-suclari-engellemek-icin-yapay-zeka-devrede/, Erişim Tarihi: 01.12.2021.

Flaherty, K. (2019). A RoboCop, A Park and A Fight: How Expectations About Robots are Clashing Reality, *NBC News*, 4 Ekim 2019, https://www.nbcnews.com/tech/tech-news/robocop-park-fight-how-expectations-about-robots-are-clashing-reality-n1059671, Erişim Tarihi: 01.12.2021.

Gerstner, D. "Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in BadenWürttemberg, Germany", European Journal for Security Research, Cilt: 3 Sayı: 2, 2018. https://link.springer.com/article/10.1007/s41125-018-0033-0, Erişim Tarihi: 09.12.2021.

Gov.uk (2016). Surveillance Camera Commissioner's IFSEC Speech, 27 Haziran 2016, https://www.gov.uk/government/speeches/surveillance-camera-commissioners-ifsec-speech, Erişim Tarihi: 01.12.2021.

Hitachi, Teknoloji, Suça Karşı Savaşta Silahımız, https://social-innovation.hitachi/tr-tr/stories/technology/hidden-weapon-in-the-fight-against-crime/, Erişim Tarihi: 01.12.2021.

Hürriyet (2018). Azınlık Raporu Filmi Gerçek Oluyor! Suçu İşlenmeden Önleme Dönemi Başlıyor, 29 Kasım 2018, http://www.hurriyet.com.tr/avrupa/azinlik-raporu-filmi-gercek-oluyor-sucu-islenmeden-onleme-donemi-basliyor-41035280, Erişim Tarihi: 01.12.2021.

Italy24 News (2021). Facial Recognition Prohibited in Italy: But Only for Now and Exceptions, 2 Aralık 2021, https://www-italy24news-com.cdn.ampproject.org/c/s/www.italy24news.com/News/amp/286487, Erişim Tarihi: 06.12.2021.

İçer, Z. – Buluz, B. (2019). Yapay Zekanın Ceza Muhakemesindeki Rolü ve Geleceği, 9. Uluslararası Suç ve Ceza Film Festivali, (https://robotic.legal/yapay-zekanin-ceza-muhakemesindeki-rolu-ve-gelecegi/, Erişim Tarihi: 01.12.2021.

İçer, Z. – Dönmez, E. (2020). Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları, Ceza Hukuku Dergisi, Yıl:15, Sayı: 43.

İçer, Z. (2021). Suça Teşebbüste Hazırlık Hareketleri İle İcra Hareketlerinin Birbirinden Ayrılması, İstanbul.

İçer, Z. (2019). Yapay Zekâ Destekli Nörohukuk Sisteminde Suç ve Cezaya Yaklaşım, XI. Eğitim Denetimi Kongresi (5-7 Aralık 2019, Antalya), Eğitim, Hukuk ve Yapay Zeka Bildiri Kitabı.

La Quadrature du Net (2018). In France, Smart City Policing is Spreading Like Wildfire, 17 Ağustos 2018, https://www.laquadrature.net/en/2018/08/17/smartcity_policing_like_wildfire/, Erişim Tarihi: 01.12.2021.

LOG (2017). Çin, Yapay Zekâ Tarafından Yönetilen İnsansız Polis İstasyonu Hazırlığında, 13 Kasım 2017, https://www.log.com.tr/cin-yapay-zeka-tarafindan-yonetilen-insansiz-polis-istasyonu-hazirligi nda/, Erişim Tarihi: 01.12.2021.

Lum, K. – Isaac, W. (2016). To predict and serve?. Significance, 13: 14-19. https://doi.org/10.1111/j.1740-9713.2016.00960.x, Erişim Tarihi: 01.12.2021.

Milliyet (2017). Robot Polisler, Devriye Görevine Başladı, 21.02.2017, https://www.milliyet.com.tr/teknoloji/robot-polisler-devriye-gorevine-basladi-2400315, Erişim Tarihi: 01.12.2021.

Milliyet (2018). İngiliz Polisi Suçu Önlemek İçin Yapay Zeka Kullanacak, 29 Kasım 2018, http://www.milliyet.com.tr/teknoloji/ingiliz-polisi-sucu-onlemek-icin-yapay-zeka-kullanacak-2786584, Erişim Tarihi: 01.12.2021.

Nayn Co, https://nayn.co/amazona-irkcilik-suclamasi-yuz-algilama-servisi-cinsiyetci-ve-irkci/, Erişim Tarihi: 01.12.2021.

Özbek, V. Ö. – Doğan, K. – Bacaksız, P. (2019) Ceza Muhakemesi Hukuku, Ankara.

Perry, W.L. vd. (2013). Predictive Policing: The Role of Crime Forecasting In Law Enforcement Operations, RANDSafety and Justice Program.

Sabah (2018). ABD'de Yüz Tanıma Tekniği Irkçı Çıktı, 31 Temmuz 2018, https://www.sabah.com.tr/dunya/abdde-yuz-tanima-teknigi-irkci-cikti-4354238, Erişim Tarihi: 01.12.2021.

Sanction Scanner, https://sanctionscanner.com/, Erişim Tarihi: 01.12.2021.

Sputnik Türkiye (2020). Rusya'da Suçluları Bulabilmek İçin Yeni Kamera Tanıma Sistemi: Ses, Göz, Dövmeden Tespit Yapılabilecek, 26 Şubat2020, https://tr.sputniknews.com/20200226/rusyada-suclulari-bulabilmek-icin-yeni-kamera-tanima-sistemi-ses-goz-dovmeden-tespit-yapilabilecek-1041478197.html, Erişim Tarihi: 01.12.2021.

Sözüer A. (1994). Suça Teşebbüs, İstanbul.

Sözüer, E. (2020). Öngörücü Kolluk Uygulamaları (Predictive Policing) ve İnsan Hakları, Yapay Zekâ Çağında Hukuk, Kasım 2020, https://www.istanbulbarosu.org.tr/files/komisyonlar/yzcg/2020kasimbulten.pdf, Erişim Tarihi: 01.12.2021.

The Guardian (2019). What is facial recognition and how sinister is it?, 29 Temmuz 2019, https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it, Erişim Tarihi: 01.12.2021.

Thomas, D. (2018). Niyet Okuma Teknolojisi: Polisler Duygularınızı Yüz Tanıma Sistemiyle Tespit Edebilecek, *BBC*, 18 Temmuz 2018, https://www.bbc.com/turkce/haberler-dunya-44865198, Erişim Tarihi: 01.12.2021.

TRT Haber (2020). Maskeler, Yüz Tanıma Sistemlerinin Kafasını Karıştırdı, 29 Temmuz 2020, https://www.trthaber.com/haber/dunya/maskeler-yuz-tanima-sistemlerinin-kafasini-karistirdi-505480.html, Erişim Tarihi: 01.12.2021.

Türkiye Yapay Zekâ İnisiyatifi (2020). Finansal Suçlara Karşı Yapay Zekalı Çözümler Sunuyoruz, 20 Temmuz 2020, https://turkiye.ai/finansal-suclara-karsi-yapay-zekali-cozumler-sunuyoruz, Erişim Tarihi: 01.12.2021.

Winston, A. (2018). Palantir has secretly been using New Orleans to test its predictive policing technology, *The Verge*, https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd, (Erişim Tarihi: 01.12.2021).

Yüz Tanıma Teknolojilerinin Temel Hak ve Özgürlükler Üzerindeki Etkileri

Av. Tuğçe Duygu Köksal

Giriş

Teknolojik gelişmeler ışığında, George Orwell'in kaleme aldığı *1984* eserinde geçen "*Büyük Birader Sizi İzliyor...*"[144] cümlesi son yıllarda neredeyse gerçeğe dönüşmüş durumdadır. Kapalı devre kamera sistemlerinden, yüz tanıma teknolojilerinin kullanımının geniş bir yelpazede kitle izlemesi yöntemlerinin karşımıza çıkması temel hak ve özgürlükler üzerindeki etkilerin de tartışılmasına yol açmaktadır.

Bu çalışmanın konusunda ele alınacak olan yüz tanıma teknolojilerinin çalışma sistemi, bireylerin kişisel verilerinin kullanımı ve toplanması üzerine kuruludur. Yüz tanıma teknolojilerinin temas ettiği kişisel veriler, biyometrik verileri ve pek çok hassas nitelikteki kişisel veriyi de barındıran bir yelpaze oluşturmaktadır. Dolayısıyla da temel hak ve özgürlüklere; başta özel hayat ve aile hayatının korunması hakkı olmak üzere, çok farklı yönleriyle müdahale teşkil ettiğine kuşku bulunmamaktadır. Yüz tanıma sistemleri gerek kamusal alanda önleyici tedbir amaçlı kolluk güçleri tarafından, gerek ise kamu ya da özel sektörde kurumsal gereklilikler bakımından başvurulan bir teknoloji haline gelmiştir. Yüz tanıma, kameralar aracılığı ile belli bir meşru amaç doğrultusunda bireyin tanımlanmasına hizmet eden ve dijital olarak görüntüsünü toplayarak veriyi depolayan bir süreç içerir. Yüz tanıma, bireylerin yüzlerini içeren dijital görüntülerin otomatik olarak işlenmesidir. Yüz şablonlarını kullanarak bu kişilerin kimliklerinin belirlenmesi veya doğrulanması için kullanılır. Yüz tanıma teknolojisinin bir türü olan canlı yüz tanıma, tüm bireylerin gerçek zamanlı olarak biyometrik verilerini yakalama yeteneğine sahiptir, bireyler otomatik olarak ve ayrım gözetmeksizin kameranın kapsama alanından geçer[145]. Toplanan veriler kimlik doğrulama, eşleştirme ya da çeşitli kategorilerde bireyleri sınıflandırma gibi amaçlara hizmet edebilir.

Yüz tanıma teknolojilerinin kullanım alanlarına ilişkin çeşitli kategoriler göze çarpmaktadır. Bu noktada ilk akla gelen, bu teknolojinin önleyici kolluk tedbiri olarak kolluk teşkilatı tarafından kullanımıdır. Bir diğer kullanım şekli sınır güvenliğinin sağlanmasına yöneliktir. Diğer taraftan, kamu ve özel sektörde faaliyet gösteren kurumlarda hizmetlere erişimde kimlik doğrulama ya da eşleştirme amacıyla kullanım söz konusu olabilmektedir. Yüz tanıma

[144] George Orwell, 1984, Can Yayınları, 74. Baskı, İstanbul 2021.
[145] Detaylı bilgi için bkz. ICO, The use of live facial recognition technology in public places, 18 Haziran 2021, https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf, Erişim Tarihi: 08.12.2021.

teknolojilerinin kullanıldığı bu alanlarda bireylerin hassas verilerini de kapsayan kişisel verilerinin izlenmesi, toplanması ve depolanması sürecinde hem kişisel verilerin korunması hem de hizmetlere erişim ya da bir hakkın kullanımı açısından hakkın kullanımı üzerinde caydırıcı bir etkinin oluşması söz konusu olabilir. Bu çerçevede uluslararası alanda dile getirilen endişeler çeşitli raporlara yansıdığı gibi, temel hak ve özgürlüklere müdahale riskinin minimize edilmesine yönelik uluslararası alanda kılavuzlar da geliştirilmiştir.

1. **Eleştirilerin kapsamı**

Son yıllarda özellikle de toplantı ve gösteri yürüyüşü hakkının kullanılması kapsamında yüz tanıma sistemlerine kamu otoriteleri tarafından başvurulmasındaki artış, insan haklarının korunması bağlamında kaygıların dile getirilmesine ve bu teknolojilerin kullanılmasına son verilmesine yönelik çağrılara neden olmuştur. Nitekim yüz tanıma teknolojilerinin, ifade özgürlüğü ile toplantı ve gösteri yürüyüşü hakkını kullananlar üzerinde caydırıcı etki yaratma kapasitesinin bulunması ve suç işleyenleri tespit etmenin ötesinde keyfi kullanıma yol açarak muhalif görüşteki bireyleri fişleme pratiğine imkân tanıması, eleştirilerin odak noktasında yer almaktadır. Çin, Birleşik Krallık, Hindistan ve Rusya'da yüz tanıma sisteminin kullanımına ilişkin basına yansıyan örneklerde çeşitli uluslararası sivil toplum kuruluşlarının endişelerini dile getirdiği görülmektedir[146].

Bu kapsamda, özgürlük ve güvenlik hakkı bakımından da yüz tanıma sistemlerinin kullanılması yöntemiyle oluşturulan kimlik doğrulama ve eşleştirme çalışmalarında hata oranlarının yüksek olduğuna dikkat çekilmektedir[147]. Yüz tanıma sistemlerinin işleyişine ilişkin yapılan çalışmalarda, özellikle yüz tanıma sistemlerinde kullanılan ve insan eliyle üretilen, öğretilmiş algoritmaların ayrımcı uygulamalara yol açabildiği ve ırk, etnik köken ya da toplumsal cinsiyet eşitliği açısından belli grupların orantısız şekilde etkilendiğine değinilmektedir. Örneğin, bir sivil toplum kuruluşu olan American Civil Liberties Union (ACLU) tarafından yüz tanıma yazılımının önyargılı olabileceği gündeme getirilmiştir[148]. Bu çalışmadan çıkan sonuçlarda, ten rengine göre değişen şekilde bireylerin basit nitelikteki suçlardan tutuklanma olasılığı daha yüksektir. Bireylerin sabıkaları yüz tanıma için kullanılan veri tabanına eklenmektedir. Bu şekilde yüz tanıma yazılımı kullanılarak tespit edilmeleri halinde eşleşme olacağından, daha sıklıkla şüpheli olarak tespit edilmelerine neden olabilir. Bu örnek de dikkate alındığında yüz tanıma teknolojisi kişisel verileri kullandığından, bu

---

[146] Human Rights Watch, Russia: Broad Facial Recognition Use Undermines Rights, 15 Eylül 2021, https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights, Erişim Tarihi: 08.12.2021.

[147] Jacquelyn Burkell, Jane Bailey, Valerie Steeves, Facial recognition technology is biased with higher error rates against people of colour, 27 Ağustos 2020, https://scroll.in/article/971374/facial-recognition-technology-is-biased-with-higher-error-rates-against-people-of-colour#:~:text=Numerous%20studies%20report%20that%20facial,be%20misidentified%20as%20a%20criminal, Erişim Tarihi: 08.12.2021.

[148] ACLU, ACLU Comment on Facial Recognition and Biometric Technology Moratorium Act, 15 Haziran 2021, https://www.aclum.org/en/news/aclu-comment-facial-recognition-and-biometric-technology-moratorium-act, Erişim Tarihi: 08.12.2021.

teknolojiyle yüz görüntülerinin toplanması ve işlenmesi, kişisel verilerin korunmasına ilişkin usuli güvencelerle uyumlu olmalı; ayrıca masumiyet karinesini ihlal eden uygulamalara fırsat verecek keyfilikteki kullanımlar engellenmelidir.

Öyle ki 11 Ağustos 2020 tarihinde Birleşik Krallık'ta bir mahkeme, yüz tanıma teknolojisinin insan haklarını ihlal ettiğine karar vermiştir. Bu karar, yüz tanıma teknolojisinin temel hak ve özgürlükleri ihlal ettiği, bireylerin mahremiyetini ihlal ettiği ve ayrımcı olduğu yönündeki tespitlere yargı üzerinden verilebilecek bir başka örnektir. Bu karardan çıkan tespitler, yüz tanıma teknolojisinin kullanımını askıya almaktan ziyade; bu teknolojinin ne zaman kullanılabileceği konusunda daha iyi parametrelerin devreye alınması gerektiğini ortaya koymaktadır[149].

Uluslararası arenada bu endişeler dile getirilirken IBM, teknolojinin 'ırksal adaletsizliği ve ayrımcılığı teşvik etmek' için kullanılabileceği endişeleri üzerine yapılan bilgilendirmede yüz tanıma sistemlerini kolluk kuvvetlerine satmayacağını açıklamıştır[150]. Akabinde Amazon'un teknoloji birimi Amazon İnternet Servisleri (AWS), geliştirdiği yüz tanıma hizmetinin emniyet birimleri tarafından kullanılmasını bir yıl ertelediğini bildirmiştir[151].

Bu çerçevede bakıldığında, kuruluşların ve devletlerin güvenlik amaçlı kullandıkları öğretilmiş algoritmalara dayalı işlev gösteren yüz tanıma sistemleri ile kişisel verilerin korunması ve bireylerin temel hak ve özgürlüklerine saygı gibi çatışan menfaatler arasındaki dengenin nasıl kurulması gerektiğine odaklanmak gerekir.

Diğer taraftan, yüz tanıma sistemlerinin kullanımı yoluyla toplanan verilerin kategorize edilmesi ve toplanmasında güdülenden başka amaçlarla kullanılması keyfiyetine karşı etkin güvencelerin ve bireyler tarafından kullanılabilecek başvuru yollarının bulunmaması da ayrı bir tartışma konusunu oluşturmaktadır. Bu teknolojilerin kullanımını sınırlayan ve bireylerin temel hak ve özgürlüklerini teminat altına alan bir çerçevenin varlığı bir hukuk devletinin olmazsa olmaz gerekliliğidir.

Uluslararası Af Örgütü, yüz tanıma teknolojilerinin kimlik tespiti ve kitlesel gözetim amacıyla kullanıldığı durumlarla ilgili yaptığı açıklamada bazı tespitlerde bulunmuştur. Buna göre, "*birey bazında suça ilişkin makul şüphe olmaksızın verilerin yaygın bir biçimde ve toplu halde izlenmesi, toplanması, saklanması, analiz edilmesi ve diğer amaçlarla kullanılmasını ve hassas kişisel bilgilerin (biyometrik bilgiler) toplanmasını mümkün kılar. Bu durum, gelişigüzel kitlesel gözetim kapsamına girmektedir"*. Uluslararası Af Örgütü, bu

[149] Detaylı bilgi için bkz. https://ukhumanrightsblog.com/2020/08/13/facial-recognition-technology-not-in-accordance-with-law/ Erişim Tarihi: 26.12.2021.

[150] IBM abandons 'biased' facial recognition tect, 9 Haziran 2020, https://www.bbc.com/news/technology-52978191, Erişim Tarihi: 08.12.2021.

[151] Karen Hao, The two-year fight to stop Amazon from selling face recognition to the police, 12 Haziran 2020, https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/, Erişim Tarihi: 08.12.2021.

açıklamasında gelişigüzel kitlesel gözetimin gizlilik, ifade özgürlüğü, örgütlenme ve barışçıl toplanma özgürlüğü haklarına yönelik orantısız bir müdahale olduğuna dikkat çekmiştir[152].

Birleşmiş Milletler Düşünce ve İfade Özgürlüğünün Korunması ve Geliştirilmesi Özel Raportörü David Kaye'in 2019 tarihli raporunda da altını çizdiği üzere; "*Hukuka aykırı gözetimin gittikçe yaygınlaştığı bağlamlarda, hedef alınan topluluklar, buna benzer gözetim girişimlerinin farkında oluyor veya buna dair kuşku duyuyorlar. Bu da toplulukların ifade ve örgütlenme özgürlüğü haklarını kullanma kapasitelerini şekillendiriyor ve sınırlandırıyor*[153]."

Avrupa Konseyi, Türkiye'nin de taraf olduğu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[154] (108 No'lu Sözleşme) çerçevesinde yayımladığı kılavuz ile devlet otoritelerine yüz tanıma sistemlerinin kullanılmasına yönelik tavsiyelerde bulunmuştur[155]. Bu Sözleşme'nin 6. maddesinde özel veri kategorileri düzenlenmiş ve buna göre, "*iç hukukta uygun güvenceler sağlanmadıkça, ırksal kökeni, siyasi düşünceleri, dini veya diğer inançları ortaya koyan kişisel veriler ile sağlık veya cinsel hayatla ilgili kişisel veriler, otomatik işleme tabi tutulmaz. Aynı şey ceza mahkumiyetiyle ilgili kişisel veriler için de geçerlidir*." Yüz tanıma sistemlerinin hassas veri kategorilerine temas etmesi nedeniyle kanunilik kriterinin ve keyfiliğe karşı usuli güvencelerin sağlanması büyük önem taşımaktadır. Nitekim yüz tanıma teknolojilerinin mevcut gözetim sistemlerine entegre edilmesi ciddi bir risk oluşturmaktadır. Avrupa Konseyi'nin yüz tanıma teknolojilerinin kullanımlarını kapsayan yönergesindeki temel amaç, bireylerin geniş çaplı gözetimine izin veren bu yöndeki uygulamaların temel haklar üzerindeki olumsuz etkilerini minimize eden önlemlerin alınması ve ilkelerin uygulanması yoluyla insan hakları ve temel özgürlüklerin güçlendirilmesini sağlamaktır.

Yüz tanıma sistemlerinin kullanımının kamu düzeni ve ulusal güvenlik bakımından fayda ve önemi, bireylerin temel hak ve özgürlükleri ile çatışması halinde adil dengenin gözetilmesi gereğini ortadan kaldırmaz. Irk, din, toplumsal cinsiyet, siyasi görüş gibi ön yargılara dayalı izleme ve profilleme oluşmasını kolaylaştıracak keyfi uygulamaların önüne geçilmesi önemlidir. Sorunun özü, yüz tanıma teknolojisinin toplum için ne anlama geldiği, mevcut

---

[152] Uluslararası Af Örgütü, ABD: Yüz tanıma teknolojisinin kitlesel gözetimde kullanılması yasaklansın, 17 Haziran 2020, https://www.amnesty.org.tr/icerik/abd-yuz-tanima-teknolojisinin-kitlesel-gozetimde-kullanilmasi-yasaklansin, Erişim Tarihi: 08.12.2021.

[153] David Kaye, Gözetim ve İnsan Hakları: Özel Raportör'ün Düşünce ve İfade Özgürlüğünün Korunması ve Geliştirilmesi Hakkındaki Raporu, 2019, § 21.

[154] TBMM, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu, (1/966), https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss700.pdf, Erişim Tarihi: 08.12.2021.

[155] Council of Europe, Guidelines on Facial Recognition, T-PD(2020)03rev4, 28 Ocak 2021, https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3, Erişim Tarihi: 08.12.2021.

eşitsizlikleri ve ihlalleri nasıl güçlendirdiği ve demokrasi, özgürlük, mahremiyet, eşitlik ve sosyal fayda kavramlarına uyup uymadığıdır[156].

Örneğin, Rusya'da, kapalı devre kamera sistemleri tarafından toplanan yüz görüntülerine erişmek için kolluk kuvvetlerinin kullandığı sistemi geliştirme konusunda bir kanun teklifi söz konusu olmuştur. Bu kapsamda, hedef bireyler ve onlarla ilişki içinde olan bireylerin hareketlerinin izlemesi amaçlanmakta ve cinsiyet, yaş veya ırk gibi veri aramaları için filtrelerin genişletilmesi amaçlanmaktaydı. İnsan Hakları İzleme Örgütü, Rusya makamlarının hiçbir düzenleme, gözetim veya veri koruması olmaksızın ve etki analizi yapılmadan yüz tanıma teknolojisinin ülke genelinde yaygınlaştırmaya devam ettiğine ilişkin bir açıklama yapmıştır. Bu teknolojinin keyfi kullanımının özellikle muhalifler üzerinde caydırıcı etki oluşturacağından endişe edilmektedir.

Yakın bir tarihte, bir sosyal ağ olan Facebook da teknolojiyle "*doğru dengeyi bulmak*" amacıyla, bir milyardan fazla kullanıcının yüz tarama verilerini sileceğini, yüz tanıma sistemini kapatarak kullanıcı profilini taramayı bırakacağını duyurmuştur[157]. Bununla birlikte; yüz tanıma sistemi kullanılarak elde edilen bir kişisel verinin internet üzerinde tamamen ortadan kaldırılmasının mümkün olup olmadığı ayrı bir tartışma konusu olarak karşımıza çıkmaktadır. Nitekim internet üzerinde her verinin iz bıraktığı düşünüldüğünde, tarama bilgilerinin izlerinin tamamen ortadan kaldırılması teknik olarak söz konusu olmayacaktır.

Öte yandan, Birleşmiş Milletler İnsan Hakları Komiserliği tarafından 2021 yılında "Dijital Çağda Özel Hayata Saygı Hakkı" konulu bir rapor yayımlanmıştır. Bu rapor, özel olarak yapay zekanın kullanımı ve çeşitli alanlarda temel haklar üzerindeki etkilerine odaklanmaktadır. Yeterli güvenlik önlemleri alınana kadar insan hakları için ciddi bir risk oluşturan yapay zeka sistemlerinin satışı ve kullanımı konusunda acilen bir moratoryuma ihtiyaç olduğunu vurgulamaktadır. Raporda, insan hakları hukukuna uygun olarak kullanılamayan yapay zeka uygulamalarının da yasaklanması çağrısında bulunulmaktadır. Nitekim Birleşmiş Milletler Irk Ayrımcılığının Ortadan Kaldırılması Komitesi (CERD) de 36 numaralı genel yorumu ile devletlerin kolluk faaliyetleri kapsamında kullandığı yüz tanımlama gibi algoritmik profilleme sistemlerinin ırkçılık oluşturabileceğine dikkat çekmiş ve insan hakları ile bağdaşır hale getirilmesi gerektiğini vurgulamıştır[158].

---

[156] EDRI, Facial recognition and fundamental rights 101, 4 Aralık 2019, https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/, Erişim Tarihi: 08.12.2021.

[157] Kashmir Hill, Ryan Mac, Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System, 5 Kasım 2021, https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html#:~:text=the%20main%20story,Facebook%2C%20Citing%20Societal%20Concerns%2C%20Plans%20to%20Shut%20Down%20Facial%20Recognition,more%20than%20one%20billion%20users, Erişim Tarihi: 08.12.2021.

[158] Committee on the Elimination of Racial Discrimination, General recommendation No. 36, Preventing and Combating Racial Profiling by Law Enforcement Officials, 24 Kasım 2020, https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/1_Global/CERD_C_GC_36_9291_E.pdf, Erişim tarihi: 19.11.2021.

Diğer taraftan, Avrupa Komisyonu'nun 21 Nisan 2021 tarihinde Avrupa Birliği'ne sunduğu yapay zekâ teknolojileri ile ilgili çerçeve düzenleme taslağında biyometrik teknolojilerin kullanılması ile gerçek zamanlı gözetimin yapılması kural olarak yasaklanmış; ancak üç durum bundan hariç tutulmuştur[159]. Bunlar da özellikle kaçırılan çocuklar olmak üzere; suç mağdurlarının tespiti, kişilerin yaşamı ve vücut bütünlüğüne yönelik acil tehditlerin (örneğin terör saldırılarının) önlenmesi ve Avrupa Yakalama Emri *(European Arrest Warrant)* düzenlenebilecek kapsamdaki suçların faillerinin yakalanmasıdır. Bu durum özellikle istihbari, önleyici ve adli faaliyetlerin birbirinin içine girdiği "gri alanlarda" temel hak ve özgürlüklere müdahale teşkil edebilecektir. Bu çerçevede usuli güvenceleri haiz bir kanuni düzenlemenin bulunmaması ve demokratik toplumda gereklilik kriterlerinin somut olayda karşılanmaması halinde özel hayat ve aile hayatına saygı hakkı başta olmak üzere aşağıda değinilecek olan Avrupa İnsan Hakları Mahkemesi'nin [AİHM] içtihadı ile bağdaşmayan olasılıklar ortaya çıkabilir.

Özellikle de yüz tanıma teknolojisi yoluyla elde edilen görüntü verilerinin 'hassas veri' olarak kabul edildiği göz önünde bulundurulduğunda ve kamuya açık yerlerde toplanan bu verilerden bireylerin haberinin olmadığı durumlarda; doğruluğa ve keyfi kullanım riskine karşı koyma imkanının bulunmaması[160], bir hukuk devletinde önemli bir eksiklik olarak karşımıza çıkar. Bu kapsamda kanuni düzenlemelerin AİHM içtihadıyla uyumlu biçimde yapılması önem arz etmektedir.

2. Türkiye mevzuatı ve AİHM içtihadı

Kolluk tarafından kişisel verilerin ne şekilde toplanacağı ve ne şekilde kullanılacağının açıkça kanunda öngörülmüş olması gerekmektedir. Bununla birlikte, Türkiye mevzuatında kolluk faaliyetleri sırasında toplanan ve işlenen kişisel verilerin korunmasına ilişkin çerçeve bir mevzuat bulunmamaktadır. Kolluk tarafından suç önleme faaliyetinde kullanılan ve 5442 sayılı İl İdaresi Kanunu'nun 11/H. maddesine dayandığı söylenen Kent Güvenlik Yönetim Sistemi [KGYS] ve Plaka Tanıma Sistemi ile güdülen amaç; asayiş ve güvenliğin sağlanması ile suç işlenmesinin önlenmesi, suç delillerinin toplanmasının sağlanmasıdır. Bununla birlikte; bunlar kolluk tarafından alınan bir tedbir olmakla keyfi kullanıma karşı uygulama sınırlarının belli olması, verilerin kim tarafından, ne şekilde toplanıp, işlenip, depolanacağının kanuni dayanağının bulunması gerekmektedir. Dolayısıyla kamusal alanda KGYS kullanılarak

[159] European Commission, Proposal For a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021/0106(COD), Brüksel, 21 Nisan 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN , Erişim tarihi: 26.11.2021.

[160] European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf, Erişim Tarihi: 08.12.2021.

kameralı gözetlemenin kanunilik kriterini taşıyan bir yasal dayanağı bulunmadığı açıktır[161]. Kitle izlemesi çerçevesinde en önemli güvenlik araçlarından biri olan bu kameraların, kamusal alanda da olsa izleme ve veri toplama faaliyeti çerçevesinde kişilerin özel ve aile hayatının korunmasına saygı hakkına müdahalede bulunduğu, bu müdahalenin her somut olayda kanunilik ve demokratik toplumda gereklilik bağlamında usuli teminatlar çerçevesinde değerlendirilmesi gerektiği açıktır.

Öte yandan, Türkiye mevzuatına bakıldığında, Polis Vazife ve Salahiyeti Kanunu'nun (PVSK) 5. maddesi ile sadece kolluk kuvvetlerine fotoğraf alma ve denetleme yetkisi tanınmıştır. Yine 5271 sayılı CMK 75/1. maddesi uyarınca, "*bir suça ilişkin delil elde etmek için şüpheli veya sanık üzerinde iç beden muayenesi yapılabilmesine ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine; Cumhuriyet Savcısı veya mağdurun istemiyle ya da re'sen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet Savcısı tarafından karar verilebilir. (...)"*. Bu karar hâkim onayına tabidir. Bununla birlikte, insan bedeninden örnek alınabilmesi için kanuni düzenlemenin şartları bu iken; hassas veri olan yüz görüntüsünün alınması açısından özel bir kanuni düzenleme yapılmaması kanunda bir hukuki boşluğa işaret etmektedir.

Bireylerin görüntülerinin alınması, doğrudan doğruya temel hak ve özgürlükler kapsamında maddi ve manevi bütünlüğün korunması ile ilgili olduğundan ve bu konudaki sınırlama ancak, Anayasa'nın 13. maddesi ile de düzenlendiği üzere, Anayasa'da öngörülen meşru amaca uygun ve kanuni düzenleme ile yapılabileceğinden; yüz tanıma teknolojilerinin kullanımı için bir kanuni düzenleme yapılması gerekir. Öyle ki Danıştay İdari Dava Daireleri Kurulu da mesai takibi için yüz tanıma sisteminin kullanılmasının kanunilik ilkesini karşılamadığına kanaat getirmiştir[162].

Diğer taraftan, kapalı devre kamera sistemlerinin önleyici kolluk tedbiri olduğu kadar adli bir delil elde etme yöntemi olarak kullanıldığını da görmekteyiz. Bu konuda özellikle kanuni dayanak ve kişisel verilerin korunması bağlamında usuli güvencelerin sağlanmasına ilişkin endişeler dile getirilmekte iken, teknolojinin bir getirisi olan yüz tanıma sistemlerinin aynı kaygıların devam etmesine neden olması kaçınılmazdır. Bu noktada özellikle kolluk güçleri tarafından kullanım konusunda hata ve önyargılı karar vermek suretiyle eşleştirme, buna dayalı fişleme ve soruşturma başlatılması ihtimali üzerinde durulmaktadır[163].

---

[161] Tevfik Sönmez Küçük, Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi, Yeditepe Hukuk Fakültesi Dergisi, C. XV, S. 1, 2018, s. 73.

[162] Danıştay İdari Dava Daireleri Kurulu, E. 2015/2958, K. 2018/682, T. 28/02/2018.

[163] Biometrics and Forensics Ethics Group Facial Recognition Working Group, Ethical issues arising from the police use of live facial recognition technology, Şubat 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf, Erişim Tarihi: 08.12.2021.

Yüz tanıma sistemlerinin kullanılmasının toplantı ve gösteri yürüyüşü hakkının etkin şekilde kullanılması üzerinde caydırıcı etki oluşturması, bunun en önemli çıktısıdır. Bu teknolojilerin kullanımı özellikle gazeteciler, insan hakları savunucuları ve ayrımcılık riski altındaki kırılgan gruplarda yer alan bireyler için daha da zararlı olabilir. Yüz tanıma sistemlerinin örgütlenme özgürlüğünü kullanan bireyler üzerindeki kullanımı ve bu kullanımın temel hak ve özgürlükler üzerindeki etkisi önemli boyutlara ulaşabilmektedir.

Yüz tanıma teknolojisi aracılığıyla kitlesel gözetim, yalnızca mahremiyet hakkını değil; aynı zamanda demokrasiyi, özgürlüğü ve toplumda saygınlık, özerklik ve eşitlikle kendini geliştirme fırsatını da tehdit etmektedir. Yüz tanımanın farklı kullanımları, yalnızca insanların yüzlerini neyi ve neden analiz ettiklerine bağlı olarak değil; aynı zamanda analizin gerekçesi nedeniyle de farklı haklara sahip olacaktır. Bu, sistemin gereklilik ve orantılılık için yasal gereklilikleri karşılayıp karşılamadığını içerir.

Kamuya açık alanlarda yüz tanıma teknolojilerinin kullanımına başvurulması halinde, devlet otoritelerinin insan hakları etki değerlendirmelerini oluşturması ve kullanımın kanunilik, meşru amaç ve demokratik toplumda gereklilik testini geçmesini sağlaması gerekir. Bu adil dengenin kurulmaması beraberinde çeşitli hakların ihlali iddialarını gündeme getirebilir.

AİHM, faaliyetlerinin doğası gereği gizli izlemeye maruz kalma riskleri olduğunu iddia eden iki avukat ve iki sivil toplum kuruluşunun başvurusunda Bulgaristan'daki gizli izleme yasalarının AİHM tarafından ortaya konan usuli güvenceleri karşılamıyor olması nedeniyle AİHS'nin 8. maddesinin ihlalini oluşturduğuna karar vermiştir[164]. Kararda, Bulgaristan'da gizli izleme tedbirlerini düzenleyen yasal düzenlemenin AİHS'nin 8. maddesi kapsamında gerekli olan keyfiliğe ve kötüye kullanıma karşı asgari güvencelerin gerisinde kaldığı vurgulanmıştır. Bu çerçevede, özellikle, izleme yoluyla elde edilen verinin depolanması ve imhasına ilişkin erişilebilir kurallar olmaması, gözetimin konusu olacakların ayrım gözetmeyen bir izlemeye cevaz vermeyecek biçimde tanımlanmamış olması, gözetimin süresi, ilgiliye bildirim ve yetkilendirme usulü gibi gözetim sistemindeki yasal boşluklara dikkat çekilmiştir. Ayrıca, iletişim verilerinin saklanması ve bunlara erişim açısından da yasal düzenlemenin kanunilik kriterini taşımadığı ve müdahaleyi demokratik toplumda gerekli kılmayacağı ifade edilmiştir.

Benzer şekilde, bu konuda Büyük Daire tarafından karara bağlanan *Big Brother Watch ve diğerleri v. Birleşik Krallık* başvurusunda, sivil toplum kuruluşlarından oluşan başvuruculaların istihbarat servisleri tarafından izlenmiş olmalarına ilişkin iddiaları değerlendirilmiş ve Birleşik Krallık mevzuatının gizli kitlesel izlemeye ilişkin yasal usuli güvenceleri içermediği gerekçesiyle ihlal kararı verilmiştir[165]. AİHM, ilgili kararda "*devletlerin modern toplumda*

[164] Ekimdzhiev ve diğerleri v. Bulgaristan, No.70078/12, 11.01.2022 (bu yayın tarihinde henüz kesinleşmemiştir); aynı yönde bkz, Centrum För Rättvisa v. İsveç [BD], No. 35252/08, T. 25.05.2021.
[165]Big Brother Watch ve diğerleri v. Birleşik Krallık [BD], No. 58170/13, 62322/14, 24960/15, T. 25.05.2021.

karşı karşıya kaldıkları çok sayıda tehdit nedeniyle, kitlesel bir müdahale rejimi yürütmenin başlı başına Sözleşmeyi ihlal etmediğini değerlendirmiştir" şeklinde hüküm kurmuştur. Ancak, böyle bir rejimde, "*alınan önlemlerin gerekliliği ve orantılılığı konusunda sürecin her aşamasında bir değerlendirme yapılmalı, operasyonun amacı ve kapsamı tanımlanırken başlangıçta bağımsız yetkilendirmeye tabi olmalı ve operasyonun denetime ve bağımsız, makabline şamil incelemeye tabi olması gerekmektedir*"[166].

Öte yandan, kolluk veri tabanlarına bireylerin kaydedilmesi ve bir çeşit fişleme faaliyetine sebebiyet verilmesi, bu faaliyetin dayanağının sorgulanması ve kanuni bir düzenleme bulunmaması ya da öngörülebilir olmaması da ihlale yol açabilecek meselelerdir. Bu noktada AİHM *Catt v. Birleşik Krallık* kararında[167], başvurucunun siyasi nitelikteki toplantı ve gösterilere katılmış olmasına ilişkin verilerin radikalizm başlığı altında polis veri tabanında işlenmesinde, yine kanunda zaman limiti bulunmaması ve usuli garantilerin öngörülmemiş olması nedeniyle AİHS'nin 8. maddesinin ihlaline karar vermiştir.

Diğer taraftan, kolluk tarafından durdurma ve kimlik sorma sırasında ırk ve etnik kökene dayalı ayrımcılık yapıldığına ilişkin bir başvuru da AİHM önünde derdesttir[168]. Özellikle de önleyici kolluk faaliyeti kapsamında yüz tanıma sistemlerinin devreye sokulduğu hallerde, bu teknolojinin denetiminin ve bu teknolojinin kullanılmasına ilişkin usuli teminatların bireysel başvuru yoluyla sorgulanması da söz konusu olabilecektir.

Öyle ki uzun zamandır tartışmaların odağında olan yüz tanıma sistemlerinin özellikle de kolluk faaliyetlerinde kullanılması gerek Avrupa Birliği düzeyinde gerek sivil toplum kuruluşları tarafından yürütülen önemli çalışmalarda, kampanya ve raporlamalara konu olmuştur. Diğer taraftan, özellikle devletlerin yüz tanıma sistemlerini kolluk faaliyetlerinin gerçekleştirilmesine yönelik meşru amaçlar dışında kitlesel gözetime yol açacak şekilde kullanması, kişisel verilerin korunmasına ilişkin pozitif yükümlülüklerin yanı sıra; bireylerin örgütlenme özgürlüğünün kullanılmasına karşı bir baskılama aracına da dönüşebilir.

Kamusal alanda yüz tanıma sistemlerinin kullanılması konusunda pilot uygulamalar Çin ve Birleşik Krallık'ta kullanılmaya başlandığında endişeler sivil toplum kuruluşları tarafından dile getirilmeye başlanmıştı. Özellikle de yüz tanıma yazılımlarının çeşitli amaçlarla kullanımında azınlık gruplara mensup bireylerin tespiti ve duygu tanıma yöntemi olarak

---

[166] Kararın özet çevirisi için bkz: Benan Molu, İHAM Büyük Dairesi'nin Big Brother Watch ve Diğerleri v. Birleşik Krallık kararının özet çevirisi: "Kitlesel dinleme ve iletişim hizmeti sağlayıcılarından iletişim verilerinin alınması rejimi, özel hayatı ve ifade özgürlüğünü ihlal eder.", 25 Haziran 2021, https://anayasagundemi.com/2021/06/25/iham-buyuk-dairesinin-big-brother-watch-ve-digerleri-v-birlesik-krallik-kararinin-ozet-cevirisi-kitlesel-dinleme-ve-iletisim-hizmeti-saglayicilarindan-iletisim-verilerinin-alinmasi/, Erişim Tarihi: 26.11.2021.

[167] Catt v. Birleşik Krallık, No. 43514/15, T. 24.01.2019.

[168] Ayrımcılık saikiyle durdurma iddiası bakımından bkz. WaBaile v. İsviçre, No. 43868/18, T. 28.08.2020 tarihinde Hükümet'e bildirilmiştir. Aynı yönde, Seydi ve diğerleri v. Fransa, No. 35844/17, T. 06.10.2021 tarihinde Hükümet'e bildirilmiştir.

kullanılması riski ve bu teknolojilerin keyfi kullanım ihtimali basına yansıyan tartışmalara konu olmuştur[169].

AİHM'nin özellikle kişisel verilerin kolluk güçleri tarafından tutulmasına, saklanmasına ve usuli güvencelerin sağlanmasına ilişkin hatırı sayılır bir içtihadı bulunmaktadır[170]. Bu doğrultuda en son 2020 yılında *Gaughran v. Birleşik Krallık* davasında da gerçek bir inceleme yapılmadan, basit nitelikte bir suçtan mahkûm olmuş bir kişinin DNA profilinin, parmak izlerinin ve fotoğrafının sınırsız süreli olarak tutulmasının orantısız niteliği nedeniyle ihlal kararı verilmiştir[171].

Yüz tanıma teknolojileri özelinde, bu teknolojilerin önleyici kolluk faaliyetlerinde kullanılmasına ilişkin olarak *Glukhin başvurusu* Rusya Hükümeti'ne 12 Temmuz 2021 tarihinde bildirilmiştir[172]. Bu başvuru, arananlar listesinde olan başvurucunun polis tarafından Moskova metrosunda bir trende, metroya yerleştirilen yüz tanıma kameralarıyla kimliğinin belirlenmesi ve yakalanmasına ilişkindir. Başvuru kapsamında polis tarafından başvurucu aleyhine kullanılan delillerin, kamuya açık yayımlanan bir videonun ekran görüntüleri ile metro güvenlik kameraları tarafından yapılan kayıtların ekran görüntülerini içermekte olduğu tespit edilmiştir. AİHM, Hükümet'e bildirdiği bu başvuruda, özellikle yüz tanıma sistemlerinin kolluk faaliyetinde kullanılmasına temel teşkil eden mevzuatın kanunilik, meşru amaç ve demokratik toplumda gereklilik kriterlerini taşıyıp taşımadığını sorgulamaktadır. Başvurucunun arama listesine alınması ve yüz tanıma sisteminin kullanılması suretiyle ekran görüntülerinin ve kayıtlarının saklanması, incelenmesi, aktarılması, işlenmesi, imha edilmesine ilişkin usuli güvencelerin kapsamı ve bu konuda alınmış yargı kararları Hükümet'e soru olarak yöneltilmiştir. Dolayısıyla da ileride bu başvuru, özel hayat ve aile hayatının korunması hakkına bir müdahale olarak ele alınacak ve somut olayın şartları dikkate alınarak ölçülülük testinden geçirilecektir.

Sonuç

Özel sektörde ve kamu sektöründe faaliyet gösteren kurumlar ve kolluk kuvvetleri, yüz tanıma teknolojisini çeşitli alanlarda test etmeye başlamış görünmektedir. Bununla birlikte; yüz tanıma teknolojilerinin kullanımına ilişkin artacak ilginin bireylerin temel hak ve özgürlükleri üzerinde çeşitli açılardan müdahalelere neden olması kaçınılmazdır. Biyometrik verilerin söz konusu olması ve bahse konu kişisel verinin hassas niteliği nedeniyle; özel hayat

[169] Huawei'nin Uygur Türkleri'ni Hedef Alan Bir Yüz Tanıma Sisteminin Testinde Yer Aldığı Ortaya Çıktı, https://www.webtekno.com/huawei-uygur-turkleri-yuz-tanima-sistemi-testi-h103148.html, Erişim Tarihi: 08.12.2021; Jake Wakefield, Yapay zekayla duygu tanıma teknolojisi 'Uygurlar üzerinde denendi', 26 Mayıs 2021, https://www.bbc.com/turkce/haberler-dunya-57250838, Erişim Tarihi: 08.12.2021.

[170] Avrupa İnsan Hakları Mahkemesi, Kişisel Verilerin Korunması, Tematik Bilgi Notu, Mayıs 2021, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf, Erişim Tarihi: 08.12.2021.

[171] Gaughran v. Birleşik Krallık, No. 45245/15, T. 13.02.2020.

[172] Glukhin v. Rusya, No. 11519/20, T. 23.06.2021 tarihinde Hükümet'e bildirilmiştir.

ve aile hayatının korunması hakkı, diğer haklarla bağlantılı olarak ayrımcılık yasağı, özgürlük ve güvenlik hakkı ile ifade özgürlüğü üzerindeki müdahalenin yakından denetlenmesi gerekir. Bu çerçevede etki analizlerinin yapılması ve temel hak ve özgürlüklere müdahale riskinin en aza indirilerek kanuni çerçevede demokratik toplumda gereklilik kriterlerinin sağlanması esas olmalıdır. Yine yüz tanıma sistemleri üzerinde gerçekleştirilecek testler ile hata ve önyargı ihtimallerinin ortadan kaldırılmasına yönelik insan faktörünü devreden çıkartmadan entegre bir sistem oluşturulmalı ve şeffaf şekilde denetlenebilmeli, hesap verilebilirlik sağlanmalıdır.

Kaynakça

ACLU (2021, Haziran 15). ACLU Comment on Facial Recognition and Biometric Technology Moratorium Act. https://www.aclum.org/en/news/aclu-comment-facial-recognition-and-biometric-technology-moratorium-act, Erişim Tarihi: 08.12.2021.

Avrupa İnsan Hakları Mahkemesi (2021, Mayıs). Kişisel Verilerin Korunması, Tematik Bilgi Notu. https://www.echr.coe.int/Documents/FS_Data_ENG.pdf, Erişim Tarihi: 08.12.2021.

Baıley, J. & Burkell, J. & Steeves, V. (2020, Ağustos 27). Facial recognition technology is biased with higher error rates against people of colour. https://scroll.in/article/971374/facial-recognition-technology-is-biased-with-higher-error-rates-against-people-of-colour#:~:text=Numerous%20studies%20report%20that%20facial,be%20misidentified%20as%20a%20criminal, Erişim Tarihi: 08.12.2021.

Biometrics and Forensics Ethics Group Facial Recognition Working Group (2019, Şubat). Ethical issues arising from the police use of live facial recognition technology. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf, Erişim Tarihi: 08.12.2021.

Committee on the Elimination of Racial Discrimination, General recommendation No. 36 (2020, Kasım 24). Preventing and Combating Racial Profiling by Law Enforcement Officials. https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/1_Global/CERD_C_GC_36_9291_E.pdf, Erişim tarihi: 19.11.2021.

Council of Europe (2021, Ocak 28). Guidelines on Facial Recognition, T-PD(2020)03rev4. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3, Erişim Tarihi: 08.12.2021.

EDRI (2019, Aralık 4). Facial recognition and fundamental rights 101. https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/, Erişim Tarihi: 08.12.2021.

European Commission (2021, Nisan 21). Proposal For a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021/0106(COD), Brüksel. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN , Erişim tarihi: 26.11.2021.

European Union Agency for Fundamental Rights (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf, Erişim Tarihi: 08.12.2021.

Hao, K. (2020, Haziran 12). The two-year fight to stop Amazon from selling face recognition to the poliçe. https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/, Erişim Tarihi: 08.12.2021.

Huawei'nin Uygur Türkleri'ni Hedef Alan Bir Yüz Tanıma Sisteminin Testinde Yer Aldığı Ortaya Çıktı. https://www.webtekno.com/huawei-uygur-turkleri-yuz-tanima-sistemi-testi-h103148.html, Erişim Tarihi: 08.12.2021.

Human Rights Watch (2021, Eylül 15). Russia: Broad Facial Recognition Use Undermines Rights. https://www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights, Erişim Tarihi: 08.12.2021.

IBM abandons 'biased' facial recognition tect (2020, Haziran 9). https://www.bbc.com/news/technology-52978191, Erişim Tarihi: 08.12.2021.

ICO (2021, Haziran 18). The use of live facial recognition technology in public places. https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf, Erişim Tarihi: 08.12.2021.

İçer, Z.; Dönmez, E. Yüz Tanıma Teknolojilerinin Önleyici Ceza Hukuku ve Ceza Muhakemesi Süreçlerindeki Kullanımı ve Sınırları, *Ceza Hukuku Dergisi***,** C. 15, S. 43, 2020.

Kaye, D. (2019). Gözetim ve İnsan Hakları: Özel Raportör'ün Düşünce ve İfade Özgürlüğünün Korunması ve Geliştirilmesi Hakkındaki Raporu.

Küçük, T.S. (2018). Kişisel Verilerin Korunması Hakkı Çerçevesinde Kamuya Açık Alanların Kamu Tüzel Kişileri Tarafından Video Kamera Aracılığı ile Önleyici Amaçla İzlenmesi, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, C. XV, S. 1, ss. 49-89.

Molu, B. (2021, Haziran 25). İHAM Büyük Dairesi'nin Big Brother Watch ve Diğerleri v. Birleşik Krallık kararının özet çevirisi: "Kitlesel dinleme ve iletişim hizmeti sağlayıcılarından

iletişim verilerinin alınması rejimi, özel hayatı ve ifade özgürlüğünü ihlal eder.". https://anayasagundemi.com/2021/06/25/iham-buyuk-dairesinin-big-brother-watch-ve-digerleri-v-birlesik-krallik-kararinin-ozet-cevirisi-kitlesel-dinleme-ve-iletisim-hizmeti-saglayicilarindan-iletisim-verilerinin-alinmasi/, Erişim Tarihi: 26.11.2021.

Orwell, G. (2021). *1984*, Can Yayınları, 74. Baskı, İstanbul.

Özkan, H. (2016). Mobese İzleme ve Kayıtlarının Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi, *Ceza Hukuku Dergisi*, C. 11, S. 30.

TBMM. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu, (1/966). https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss700.pdf, Erişim Tarihi: 08.12.2021.

Uluslararası Af Örgütü (2020, Haziran 17). ABD: Yüz tanıma teknolojisinin kitlesel gözetimde kullanılması yasaklansın. https://www.amnesty.org.tr/icerik/abd-yuz-tanima-teknolojisinin-kitlesel-gozetimde-kullanilmasi-yasaklansin, Erişim Tarihi: 08.12.2021.

Wakefield, J. (2021, Mayıs 26). Yapay zekayla duygu tanıma teknolojisi 'Uygurlar üzerinde denendi'. https://www.bbc.com/turkce/haberler-dunya-57250838, Erişim Tarihi: 08.12.2021.

Avrupa İnsan Hakları Mahkemesi karar ve başvuruları

Gaughran v. Birleşik Krallık, No. 45245/15, T. 13.02.2020.
CentrumFörRättvisa v. İsveç [BD], No. 35252/08, T. 25.05.2021.
BigBrother Watch ve diğerleri v. Birleşik Krallık [BD], No. 58170/13, 62322/14, 24960/15, T. 25.05.2021.
Ekimdzhiev ve diğerleri v. Bulgaristan, No.70078/12, 11.01.2022 (bu yayın tarihinde henüz kesinleşmemiştir).
Catt v. Birleşik Krallık, No. 43514/15, T. 24.01.2019.
WaBaile v. İsviçre, N.o. 43868/18, T. 28.08.2020 tarihinde Hükümet'e bildirilen başvuru.
Glukhin v. Rusya, No. 11519/20, T. 23.06.2021 tarihinde Hükümet'e bildirilen başvuru.
Seydi ve diğerleri v. Fransa, No. 35844/17, 06.10.2021 tarihinde Hükümet'e bildirilen başvuru.

Danıştay kararları

Danıştay 5. Daire, 2013/7949 E. 15/11/2013 tarihli karar

Danıştay 11.Dairesi, 2017/816 E., 2017/4906 K. 13/0672017 tarihli karar
Danıştay İdari Dava Daireleri Kurulu, 2015/2958 E. 2018/682 K., T. 28.02.2018.

Derin Sahte (*Deepfake*) Teknoloji Karşısında Türk Ceza Hukuku

Dr. Buket Abanoz Öztürk

Giriş

Derin sahte[173] teknoloji, bir kişinin görüntüsünün başka bir kişinin vücuduna yerleştirilerek sahte görsel ve işitsel içerik üretilmesini mümkün kılmaktadır[174]. Her gün gelişmekte olan derin sahte teknoloji, insanın duyu organlarıyla kolayca ayırt edemeyeceği kadar gerçekçi görünen görüntü, ses veya video üretilmesine imkân vermektedir. Bununla birlikte, herkesin erişimine ve kullanımına açık olan mobil uygulama ve araçlarla herhangi bir kişi, kolaylıkla anlık sahte içerik üretebilmektedir. Belirtilen bu özellikleriyle söz konusu teknoloji, temel hak ve özgürlüklere ciddi şekilde müdahale edebilecek bir potansiyele sahiptir ve birçok suçun işlenmesinde araç olarak kullanılabilir.

Derin sahte ses veya görüntü üretilmesi veya kullanılmasından doğan Türk Ceza Hukuku sorumluluğu henüz yeterince değerlendirilmemiştir. Nitekim söz konusu teknolojinin ortaya çıkaracağı hukuki sorunları değerlendiren çalışma sayısı neredeyse yok denecek kadar azdır[175] . Dolayısıyla bu çalışma, söz konusu teknolojinin beraberinde getirdiği potansiyel tehlike ve zararların belirlenmesi ve sınıflandırılması amacını taşıyan keşfedici bir çalışma olup kendisinden sonraki çalışmalar için kaynak teşkil etmeyi amaçlamaktadır. Çalışmada derin öğrenme teknolojisinin kullanımıyla oluşturulan sahte içerikler karşısında Türk Ceza Hukuku'ndaki mevcut düzenlemelerin yeterli olup olmadığı sorusu tartışmaya açılmaktadır. Bu kapsamda, söz konusu teknoloji karşısında yeni suç tiplerinin düzenlenmesi gerektiği görüşü de değerlendirilmektedir. Bu değerlendirmede, yeni hukuki değerlerin ortaya çıkıp çıkmadığı ve söz konusu müdahalelere karşı mevcut ceza hukuku düzenlemelerimizin sağladığı koruma dikkate alınmaktadır.

Bu kapsamda, çalışmada öncelikle derin sahte kavramı ve bu teknolojinin alt yapısı ortaya koyulmuştur. Ardından derin sahte teknolojinin ortaya çıkarabileceği tehlike ve zararlar

---

[173] "Deepfake" kavramına karşılık olarak, Türkçe'de *"derin taklit"*, *"derin hile"*, *"derin sahte"*, *"derin sahtecilik"*, *"dip düzmece*", *"sahte görüntü üretmek için kullanılan sistem"* ve *"derin öğrenme teknolojisinin kullanımıyla sahte içerik oluşturma"* gibi çeşitli ifadeler kullanılmaktadır. Çalışmada *deepfake* kavramına karşılık olarak, bu kavrama en yakın ifade olarak gördüğümüz "derin sahte" kavramı kullanılmıştır.

[174] UNICRI, UNCCT, Algorithms and Terrorism, The Malicious use of artificial intelligence for terrorist purposes, 2021, s. 15, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf, Erişim Tarihi: 30.09.2021.

[175] Adem Akkır, Gökcan Yıldırım, Bir Bilişim Suçu "Deepfake", MGC Legal, 13.03.2018, https://www.mgc.com.tr/bir-bilisim-sucu-deepfake, Erişim Tarihi: 16.03.2021; E. Eylem Aksoy Retornaz, Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etmei Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deepfake), On İki Levha Yayıncılık, Mayıs 2021.

belirlenerek söz konusu teknolojinin hangi hukuki değerlere müdahale ettiği tespit edilmiştir. Ceza hukukunun son çare ilkesi (ultima ratio) de dikkate alınarak söz konusu tehlike veya zararlar karşısında ceza hukuku korumasının gerekip gerekmediği araştırılmıştır. Eğer söz konusu müdahaleler ceza hukuku korumasını gerektiriyorsa; bu takdirde tespit edilen hukuki değerlerin korunmasında Türk ceza hukukundaki mevcut düzenlemelerin yeterli olup olmadığı incelenerek yeni suç tiplerine ihtiyaç olup olmadığı sorusu yanıtlanmaya çalışılmıştır. Bu kapsamda, Türk Ceza Kanunu'nun ikinci kitap özel hükümler bölümünde yer alan suç tipleri ile sınırlı bir inceleme yapılmasının dahi bir makale çalışmasını aşacak nitelikte olduğu belirtilmelidir. Bu nedenle, söz konusu teknolojinin özellikle bireylere karşı işlenen suçlar bakımından kullanım örnekleri incelenerek diğer suç tiplerine işaret etmekle yetinilmiştir. Ayrıca derin sahte içeriklerle seçimlerin haksız yönlendirilmesi riskinin de yakın gelecekte ciddi bir sorun olabileceği dikkate alınarak 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun da incelemeye dahil edilmiştir.

1. Derin Sahte Teknoloji

Deepfake kavramı, "deep (learning)" derin öğrenme ve "fake" (content) sahte içerik kelimelerinden oluşmaktadır. Derin sahte (*deepfake)* veya sentetik medya (*synthetic media*) olarak da adlandırılan söz konusu sahte görsel veya işitsel içerikler derin öğrenme teknolojisi ile üretilmektedir[176].

Derin sahte gibi gerçek olmayan bir görsel veya işitsel içerik oluşturmak için yüz değiştirme (*face replacement*), yüz canlandırma (*face re-enactment*), yüz oluşturma (*face generation*), konuşma sentezi (*speech synthesis*), sığ sahtecilik[177] (*shallowfakes*) kullanılabilmektedir[178]. Bir insanın yüzünü sabit bir görüntüde tanımlamak ve sonra başka bir yüzle değiştirmek için programlanan yapay zekâ; bunun için saniyede 30 ila 60 fotoğraf arasında tekrarlanarak bir video üretmektedir[179]. Bununla birlikte, 2014 yılında keşfedilen ve mevcut veri setlerinden yeni veriler yaratabilen bir algoritma seti olan *Üretken Çekişmeli Ağlar* (*Generative Adversarial Networks*, (GAN) kullanılarak da derin sahte içerikler üretilebilir[180]. Örneğin,

---

[176] Buket Abanoz Öztürk, "Deepfake İkilemi: Sadece Eğlence mi? Tehditler ve Hukuki Tartışmalar", Lexpera Blog, 07.04.2021, https://blog.lexpera.com.tr/deepfake-ikilemi-sadece-eglence-mi-tehditler-ve-hukuki-tartismalar/, Erişim Tarihi: 11.09.2021.

[177] *Shallowfakes* (sığ sahtecilik), konuyu yanıltıcı bir şekilde tasvir etmek için kasıtlı olarak yavaşlatmak veya hızlandırmak gibi basit düzenleme araçlarıyla oynanmış veya bağlam dışında sunulan videolar, ses kayıtları veya bir konuşmanın bazı değiştirilmemiş kliplerini seçerek bir araya getirmek, metnin tonunu kaldırmak veya yumuşatmak veya bir videonun başlangıç ve bitiş zamanlarını değiştirerek bağlam eklemekten oluşabilir. Bu tür bir düzenleme, aslında orijinal içeriği değiştirmemekle birlikte izleyicinin videoya bakışını yeniden düzenler. Böylece söz konusu videoya yeni bir anlam yükleyebilir. Bkz. Vincenzo Ciancaglini, Craig Gibson, David Sancho, Malicious Uses and Abuses of Artificial Intelligence, Trend Micro Research, 2020, s. 55, https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf, Erişim Tarihi: 12.09.2021.

[178] Ciancaglini, Gibson, Sancho, s. 53-54.

[179] Akkır, Yıldırım, Bir Bilişim Suçu "Deepfake".

[180] Ciancaglini, Gibson, Sancho, s. 53-54; Jennifer Baker, "Deepfakes could break the ınternet", Cpo Magazine, https://www.cpomagazine.com/cyber-security/deepfakes-could-break-the-internet/, 21 Ekim 2019; Çiğdem Eylül

fotoğraflar üzerinde eğitilmiş bir GAN, depolanan fotoğraflardan oluşan bir veri kümesine benzeyen yenilerini oluşturabilir. Derin sahte, gerçekçi bir sahte içerik oluşturmak için genellikle çok sayıda görüntü verisi gerektirse de yakın gelecekte GAN'ların daha az veri konusunda eğitileceği ve insan yüzlerini, seslerini ve tüm vücutlarını değiştirebileceği belirtilmektedir[181].

2. Derin Sahte Teknolojinin Gelişimi

Derin sahte videoların, 2017 yılında anonim bir Reddit kullanıcısı tarafından ünlülerin yüzlerinin pornografik filmlerde kadınların vücutlarına yerleştirildiği videoların yayınlanmasıyla ortaya çıktığı bilinmektedir[182]. Derin sahte pornografisi, aktör veya aktrisin yüzlerinin derin sahte ile zaten var olan bir pornografik yayın ile değiştirilerek oluşturulan bir tür sahte pornodur. Söz konusu videolar, ilgili platform tarafından hızla yayından kaldırılmasına rağmen daha önce görülmemiş bu yüz değiştirme tekniğinin potansiyeli hem medyanın hem de kamuoyunun dikkatini çekmiştir.

Belirtilen bu ilk örneklerden sonra, derin sahte kullanımı devlet başkanlarını, siyasi figürleri ve komedyenleri kapsayacak şekilde genişlemiştir[183]. Fakat viral hale gelen derin sahte videoların kayda değer bir kısmının suç işlemek amacıyla değil, bu teknolojinin potansiyel tehlikesine dikkat çekmek amacıyla yapıldığı görülmektedir. Örneğin, 2018 yılında Amerikalı aktör Jordan Peele'nin sesi ve görüntüsü manipüle edilerek, eski ABD Başkanı Barack Obama'nın Donald Trump'a küfrettiğini gösteren bir derin sahte video üretilmiştir[184]. Bu video, söz konusu teknolojinin tehlikelerini göstermek ve farkındalık yaratmak amacını taşımaktadır[185].

Bununla birlikte, derin sahte videoların suç işlemek amacıyla kullanıldığını gösteren vakalar da yaşanmıştır. Derin sahte videoların suçun işlenmesinde kullanılma oranını gösteren yayınlanmış bir rapor olmasa da söz konusu vakaların özellikle siyasi liderlere karşı kullanıldığı tespit edilmektedir. Örneğin, 2019 yılında Malezya'da bir kabine bakanıyla yardımcısının eşcinsel ilişkileri olduğunu itiraf eden derin sahte bir video yayınlanmıştır. Bu videoda, bakanın yolsuzluk iddiasıyla soruşturulmasına ilişkin bir çağrı da yer almaktadır. Söz konusu derin sahte video, ülkede siyasi olarak tahribat yaratmış ve koalisyon hükümetini istikrarsızlaştırmayı başarmıştır[186]. 2020 yılında ise Amerika Birleşik Devletleri Temsilciler

---

Öneren, "Deepfake İnterneti Yıkabilir", Sanal Hukuk, https://www.sanalhukuk.net/deepfake-interneti-yikabilir/, Erişim Tarihi:16.03.2021.

[181] Ciancaglini, Gibson, Sancho, s. 54.

[182] Samantha Cole, "We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now", https://www.vice.com/en/article/bjye8a/reddit-fake-porn-app-daisy-ridley, Erişim Tarihi: 24.01.2018.

[183] Ciancaglini, Gibson, Sancho, s. 56.

[184] Fagan, Kaylee. "A viral video that appeared to show Obama calling Trump a 'dips---' shows a disturbing new trend called 'deepfakes'". Business Insider, Erişim Tarihi: 3.11.2020.

[185] Ciancaglini, Gibson, Sancho, s. 56.

[186] Nic Ker, "Is the political aide viral sex video confession real or a Deepfake?", Malay Mail, 12 Jun 2019, https://www.malaymail.com/news/malaysia/2019/06/12/is-the-political-aide-viral-sex-video-confession-real-or-a-deepfake/1761422, Erişim Tarihi: 30.09.2021.; Ciancaglini, Gibson, Sancho, s. 57.

Meclisi Başkanı Nancy Pelosi'nin bir videosu yavaşlatılarak, sarhoş olduğu izlenimi uyandırılmıştır. Bu video ise sığ sahte videoların da siyasi bir tehdit olarak kullanılabildiğini göstermiştir[187]. Yine 2020 yılında, Rus Genelkurmay başkanı Leonid Volkov'un derin sahte görüntüsü ve sesi kullanılarak Letonya Parlamentosu Dış İlişkiler Komitesi başkanı Rihards Kols ile çevrimiçi görüşmeler yapıldığı, bu görüşmelerde Kırım ve Rus siyasi tutukluların durumu gibi konuların görüşüldüğü de ortaya çıkmıştır[188].

Gerçek bir kişinin sesi ve görüntüsü manipüle edilerek sahte bir video üretildiğinde bu sahte içerik; o kişiyi aşağılamak veya küçük düşürmek için kullanılabildiği gibi ilgili sahte video ile tehdit etmek için de kullanılmaktadır. Örneğin, 2021 yılında Amerika'da bir kadın, kızının rakip takımında yer alan ponpon kızların görüntülerini derin sahte yazılımıyla manipüle ederek sigara, alkol ve uyuşturucu madde kullanırken gösteren içerikler üretmiştir. Bu sahte içeriklerle genç kızları tehdit eden kadın, genç kızların şikâyeti üzerine yakalanmıştır[189].

Derin sahte teknoloji, sadece sahte görüntü değil *derin sahte ses* içeriği ile de suçun işlenmesinde kullanılmaktadır. Söz konusu teknoloji, bir kişiye gerçekte hiç söylemediği şeyleri derin sahte ses teknoloji ile söyletebilir. Bu kapsamda, derin sahte teknoloji kullanılarak gerçekleştirilen ilk siber dolandırıcılık vakasının 2019 yılında yaşandığı tespit edilmiştir[190]. Ses klonlama yöntemiyle bir Alman enerji şirketinin 244 bin dolar değerinde dolandırıldığı ifade edilmektedir. Olayda siber saldırganlar, İngiltere'de faaliyet gösteren bu şirketin yöneticisini Almanya'daki ortağın sesini yapay zekâ ile birebir kopyalayarak aramışlar ve Macaristan'daki bir tedarikçiye acil olarak 244 bin dolar ödeme yapmasını istemişlerdir. İngiltere'deki yönetici, telefonda firmanın Almanya'daki büyük hissedarı olan şirketin CEO'sunun sesini duyduğu için hiçbir şeyden şüphelenmemiş ve oluşan nakit açığı kısa sürede başka bir ödeme ile kapatılacağından ödemeyi gerçekleştirmiştir. Ancak daha sonra açığı kapatacak ödeme gelmeyince Macaristan'a gönderilen paranın Meksika'ya ve oradan da başka yerlere gönderildiği anlaşılmıştır[191].

---

[187] Beatrice Dupuy, "Not Real News: Altered video makes Pelosi seem to slur words", AP News, 24 May 2019, https://apnews.com/article/social-media-donald-trump-nancy-pelosi-ap-top-news-not-real-news-4841d0ebcc704524a38b1c8e213764d0, Erişim Tarihi: 30.09.2021.

[188] "Dutch MPs in video conference with deep fake imitation of Navalny's Chief of Staff, NL Times, 24.04.2021, https://nltimes.nl/2021/04/24/dutch-mps-video-conference-deep-fake-imitation-navalnys-chief-staff, Erişim Tarihi: 30.09.2021.

[189] Kim Bellware, "Cheer mom used deepfake nudes and threats to harrass daughter's temmates, police say", The Washington Post, 13.03.2021 https://www.washingtonpost.com/nation/2021/03/13/cheer-mom-deepfake-teammates/, Erişim Tarihi: 30.09.2021.

[190] Sabah Gazetesi, "CEO'nun Sesini Yapay Zeka İle Taklit Ettiler 1,4 Milyon TL Çaldılar", 3 Eylül 2019, https://www.sabah.com.tr/ekonomi/2019/09/03/ceonun-sesini-yapay-zekayla-taklit-ettiler-14-milyon-tl-caldilar, 26.03.2021; UNICRI, UNCCT, Algorithms and Terrorism, The Malicious use of artificial intelligence for terrorist purposes, 2021, s. 37, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf, Erişim Tarihi: 30.09.2021.

[191] Abanoz Öztürk, "Deepfake İkilemi: Sadece Eğlence mi? Tehditler ve Hukuki Tartışmalar".

2020 yılında İngiltere'de bir velayet davasında, davayı manipüle etmek için mahkemeye derin sahte bir ses kaydı sunulmuştur. Bu ses kaydında, babanın karşı tarafı tehdit ettiğini gösteren ifadeler yer almaktadır. Delil veya suç uydurmak cezalandırılabilir bir eylem olmakla birlikte, söz konusu derin sahte ses kaydı, gelişen teknoloji karşısında elektronik delillerin güvenilirliği konusunda ciddi endişeleri gündeme getirmiştir[192]. Nitekim ses ve görüntü kaydı, ceza muhakemesinde önemli bir delil aracı olarak kullanılmaktadır. Günümüzde bir suçun aydınlatılmasında akla gelen ilk delil, kamera görüntüsüdür. Fakat derin sahte teknoloji karşısında, görüntü ve ses kaydının sıhhati bakımından da artık ciddi bir şüphe söz konusu olabilir.

Özetle, derin sahte teknolojinin yukarıda belirtilen kötü niyetli kullanımları tespit edilmekle birlikte söz konusu teknoloji, 2017 yılında ortaya çıkmasından bu zamana kadar suç işlemek amacıyla henüz geniş çapta kullanılmamıştır. Derin sahte videoların kayda değer bir kısmı hâlâ rıza dışı pornografik amaçlar için üretilmektedir. Nitekim Hollandalı siber güvenlik girişimi *Deeptrace* tarafından Ekim 2019'da yayınlanan bir raporda, tüm çevrimiçi derin sahte videoların %96'sının pornografik olduğu belirtilmektedir[193]. Fakat derin sahte içerik üretme teknolojisinin gelişimi, herkesin kolay bir şekilde anlık sahte içerikli videolar üretebilmesine imkân veren boyutlara ulaşmıştır. Bu kapsamda, faillerin artık yüksek düzeyde teknik beceriye ihtiyaç duymadan derin sahte içerik üretebiliyor olmalarının, suçların işlenmesi amacıyla kullanımını da arttıracağı tahmin edilmektedir[194].

3. Derin Sahte Teknoloji Karşısında Yeni Suç Tiplerine İhtiyaç Olup Olmadığı Sorunu

Derin sahte ses ve görüntü üretilmesi veya kullanılması karşısında ceza hukukunda yeni suç tiplerine ihtiyaç olup olmadığı sorusunu cevaplayabilmek için öncelikle söz konusu teknolojinin ortaya çıkarabileceği tehlike ve zararların belirlenerek bu teknolojinin hangi hukuki değerlere müdahale ettiğinin tespit edilmesi gerekmektedir. Ardından ceza hukukunun son çare ilkesi (ultima ratio) de dikkate alınarak söz konusu tehlike veya zararlar karşısında ceza hukuku korumasının gerekip gerekmediği araştırılmalıdır. Eğer söz konusu müdahaleler ceza hukuku korumasını gerektiriyorsa; bu takdirde tespit edilen hukuki değerlerin ve ihlal şekillerinin Türk ceza hukukundaki mevcut suç tiplerinde zaten korunup korunmadığı incelenmelidir. Bu kapsamda aşağıda, önce derin öğrenme teknolojisi kullanılarak üretilen sahte içeriklerin ortaya çıkarabileceği tehlike ve zararlar ortaya konulmuş, ardından Türk Ceza Kanunu'ndaki düzenlemeler incelenerek yeni suç tiplerine ihtiyaç olup olmadığı sorusu yanıtlanmaya çalışılmıştır.

---

[192] Ciancaglini, Gibson, Sancho, s. 58.
[193] Henry Ajder, Girgio Patrini, Francesco Cavalli & Laurence Cullen, The State of Deepfakes, Landscape, Threats, and Impact, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf, Erişim Tarihi: 19 Mart 2021.
[194] Ciancaglini, Gibson, Sancho, s. 59.

3.1. Derin Sahte Teknolojinin Ortaya Çıkarabileceği Potansiyel Tehlike ve Zararlar

Sahte görüntü ve seslerin birçok suçun işlenmesi amacıyla kullanılması riski, derin sahte teknolojinin potansiyel bir tehdit olarak kabul edilmesine neden olmaktadır. Nitekim derin sahte içerikler, Amerika Birleşik Devletleri'nde 2018 yılında kurulan Yapay Zekâ Ulusal Güvenlik Komisyonu (*National Security Commission on Artificial Intelligence*) tarafından tıpkı insansız hava araçları, yapay zekâ destekli savunma araçları veya otonom silahlar gibi ulusal güvenliği tehdit eden yeni araçlar olarak kabul edilmektedir[195]. Komisyon tarafından 2021 yılında yayımlanan raporda, yapay zekanın gelişmesiyle birlikte derin sahte video uygulamaları, herhangi bir kişi tarafından kolayca indirilip kullanılabileceği gibi dijital dezenformasyon ve siber saldırılar için teröristler tarafından da kullanılabilecek bir tehlike olarak görülmektedir[196]. Benzer şekilde, 2021 yılında yayımlanan Avrupa Parlamentosu ve Avrupa Birliği Konseyi Yapay Zekâ Tüzüğü'nde de derin sahte içeriklerin tehlikelerine işaret edilerek şeffaf olmaları konusunda yükümlülükler getirildiği görülmektedir[197].

İnternet, sosyal medya ve anlık iletişimin hızıyla birleştiğinde derin sahte içerikler hem kolaylıkla üretilebilecek hem de kısa sürede geniş kitlelere ulaşabilecek potansiyele sahiptir[198]. Yapay zekâ destekli söz konusu teknoloji, belirtilen bu özellikleriyle temel hak ve özgürlüklere ciddi şekilde müdahale edebilecek bir potansiyele sahiptir ve aşağıda yer alan durumları da içeren birçok suçun işlenmesi amacıyla kullanılma riski bulunmaktadır[199]:

1. *Bireylerin imajını ve güvenilirliğini zedelemek,*
2. *Bireyleri çevrimiçi ortamda taciz etmek, aşağılamak veya küçük düşürmek,*
3. *Çocuklara karşı birçok çevrimiçi suçun işlenmesini kolaylaştırmak,*
4. *Belgede sahteciliği kolaylaştırmak,*
5. *Siber dolandırıcılık,*
6. *Çevrimiçi kimlikleri tahrif etmek,*
7. *Finansal piyasaları bozmak,*
8. *Bilgi dezenformasyonuna neden olmak ve kamuoyunu manipüle etmek,*
9. *Seçim sonuçlarını etkilemek,*
10. *Azınlık gruplarına yönelik şiddet eylemlerini kışkırtmak,*
11. *Aşırı ve hatta terörist grupların anlatılarını desteklemek,*
12. *Toplumsal huzursuzluğu ve siyasi kutuplaşmayı kışkırtmak,*
13. *Ceza muhakemesinde delil olarak kullanılan ses ve görüntü kayıtlarını tahrif etmek veya manipüle etmek.*

---

[195] National Security Commission on Artificial Intelligence, Final Report, s. 9, 45, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf, Erişim Tarihi: 12.09.2021.
[196] National Security Commission on Artificial Intelligence, Final Report, s. 22.
[197] Regulation of the European Parliament and of the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intellgence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, Erişim Tarihi: 12.09.2021.
[198] UNICRI, UNCCT, s. 16.
[199] Ciancaglini, Gibson, Sancho, s. 52.

Bu kapsamda, derin sahte teknolojinin bireylerin onur, şeref ve haysiyetlerine, özel hayatlarının gizliliğine, kişisel verilerinin rızaları dışında kullanılması veya paylaşılmasına ve malvarlıklarına yönelik suçların işlenmesinde araç olarak kullanılabileceği tespit edilmektedir. Ayrıca adliyenin gereksiz meşgul olmaması ve bireylerin adil yargılanma haklarının koruma altına alınmasını sağlayan suç uydurma veya sahte delil üretme ile adil yargılamayı etkilemeye teşebbüs suçlarının işlenmesinde de araç olarak kullanılabileceği görülmektedir. Belirtilen bu suçlar derin sahte ses, görüntü veya video içeriğinin üretilmesi, kullanılması, ifşa edilmesi veya yayılması hareketleriyle işlenebilmektedir.

Bu noktada, yukarıda tespit edilen tehlike ve zararların ceza hukukuyla korunması gereken yeni bir hukuki değer ortaya çıkardığını söylemek zor gözükmektedir. Nitekim söz konusu teknoloji ***sahte ya da yalan içerik üretilmesi veya yayılması***na imkân vermektedir. Salt yalan veya sahte içerik üretmenin suç olarak düzenlenmesinin gerekip gerekmediği tartışılabilir. Sahte videoların ömürleri çok uzun değildir; ancak kısa süreli kafa karışıklığı veya panik yaratabilirler. Nitekim bu nedenle Amerika'da bilhassa ulusal güvenlik, seçimlerin manipüle edilmesini engellemek ve bilgi dezenformasyonunu önüne geçmek amacıyla *deepfake* kanunları çıkarıldığı görülmektedir. İlgili düzenlemelerde derin sahte teknoloji ile üretilen videolara söz konusu teknolojiyle üretildiklerini gösteren bir filigran yerleştirilmesi zorunluluğu getirilmektedir[200]. Bu şekilde düzenleyici işlemlerle, üretilen sahte haber veya içeriklerin ortaya çıkarabileceği zararlar azaltılabilir. Fakat bir adım daha ileri gidilerek, Teksas eyaletinde seçimlere zarar vermek amacıyla bir adayı karalamak veya seçim sonucunu etkilemek amacıyla seçime 30 gün kala derin sahte video yapılmasını, kabahat (misdemeanor) olarak kabul eden ve bir yıla kadar hapis cezası ve 4.000 dolar para cezası ile cezalandıran bir kanun bulunmaktadır[201]. Benzer şekilde, Fransa'da da 2018 yılında ülkenin temel çıkarlarını tehlikeye sokmak ve seçim sonuçlarını etkilemek amacıyla seçime üç ay kala yapılan yalan haberlerin hâkim kararıyla engellenmesine izin veren bir düzenleme kabul edilmiştir[202].

Bununla birlikte, söz konusu derin sahte içeriklerin, başka suçların işlenmesinde araç olarak kullanılması durumunda söz konusu hazırlık hareketinin cezalandırılması için yeni suç tiplerinin oluşturulması gerektiği yaklaşımı karşısında; ceza hukukunun son çare olma ilkesinin gözden kaçırılmaması gerektiği ifade edilmelidir. Derin sahte teknoloji, suçun işlenmesinde araç olarak kullanılabileceği gibi insanlığa faydalı ve iyi amaçlar için de kullanılabilecek niteliktedir. Dolayısıyla nötr bir araç olduğu düşünüldüğünde; söz konusu teknolojinin ceza hukukuyla korunması gereken hukuki değerleri zarara uğratması durumunda ceza hukukunun müdahale etmesi gerekir. Bu kapsamda; derin sahte teknolojinin ortaya çıkarabileceği potansiyel tehlike ve zararların bireylere ilişkin suçların, finans ve banka

[200] Jason Chipman, Matthew Ferraro, Stephen Preston, First Federal Legislation on Deepfakes Signed into Law, Jdsupra, 24 December 2019, https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/, Erişim Tarihi: 18.03.2021.
[201] Chipman, Ferraro, Preston, First Federal Legislation on Deepfakes Signed into Law.
[202] Zachary Young, "French Parliament passes law against 'fake news'", Politico, 4 July 2018, Erişim Tarihi: 6.12.2021.

işlenişine karşı suçların ve adliyeye karşı suçların işlenmesinde araç olarak kullanılabileceği tespit edilmektedir. Bu anlamda Türk Ceza Kanunu'nda düzenlenen kişilere, topluma, millete ve devlete karşı suçlar kapsamında korunan hukuki değerlerin ötesinde yeni bir hukuki değeri ihlal ettiğini söylemek zor gözükmektedir. Fakat söz konusu suç tiplerinde haksızlığın işleniş şekli, kapsamı ve boyutu dikkate alınarak cezanın artırılmasını gerektiren nedenler bakımından değerlendirilmesi de gerekebilir. Bu nedenle, aşağıda Türk Ceza Kanunu'ndaki düzenlemeler incelenecektir.

3.2. Derin Sahte Teknoloji Karşısında Türk Ceza Hukukundaki Düzenlemelerin İncelenmesi

5237 sayılı Türk Ceza Kanunu'nda derin sahte görüntü veya ses içeriği üretilmesini özel olarak suç haline getiren bir düzenleme bulunmadığı görülmektedir. Fakat derin sahte içerikler, bazı suçların işlenmesinde araç olarak kullanılabilmektedir. Ayrıca derin sahte videoların konusu olan ses ve görüntü, kişisel veridir. Bu bağlamda kişisel verilerin korunmasına ilişkin suçlar gündeme gelebilir. Bu nedenle, sırasıyla özel hayata ve hayatın gizli alanına karşı suçlar, şeref ve haysiyete karşı suçlar, hürriyete karşı suçlar, bilişim sistemine karşı suçlar, mal varlığına karşı suçlar ve adliyeye karşı suçlar incelenerek söz konusu teknolojinin kullanılması durumunda ortaya çıkabilecek suçlar incelenecektir.

a. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Derin sahte videoların üretilmesinde kullanılan ses ve görüntüleri, kişisel veridir. Nitekim 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda kişisel veri; *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmaktadır. Bu tanıma göre; kişinin, yaşı mesleği, sesi, görüntüsü, imzası veya özgeçmişi gibi bilgiler kişiyi belirgin kıldığı müddetçe kişisel veri olarak kabul edilmektedir[203]. Bu durumda, ses ve görüntüsü derin sahte içerikte kullanılan kişinin, kişisel verilerinin kullanıldığına şüphe olmamalıdır. Bununla birlikte, vücudu kullanılan kişi ve kişinin yüzü bu vücuda aktarılan kişi olmak üzere derin sahte içeriklerde en az iki kişi yer almaktadır. Vücudu kullanılan kişinin de tanınabilir olduğu durumlarda rızası dışında söz konusu görüntüsünün kullanılması, kişisel verilerin korunmasına ilişkin suçları veya özel hayatın gizliliğinin ihlalini gündeme getirebilir.

Kişisel verilerin korunmasını isteme hakkı, anayasal güvence altındadır ve Anayasa m. 20'de bu hakkın, *kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme,*

[203] 6698 sayılı kanun "işlenmeleri halinde ilgili kişilerin mağdur olmasına veya ayrımcılığına maruz kalmasına neden olma riski taşıyan verileri özel nitelikli kişisel veriler (hassas veriler) olarak tanımlamıştır. Bu bağlamda; "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" başlığını taşıyan 6. maddesine göre özel nitelikli kişisel veriler (hassas veriler); *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verileri"* dir. Bu veriler "işlenmeleri halinde ilgili kişilerin mağdur olmasına veya ayrımcılığa maruz kalmasına neden olma riski taşıyan verilerdir". Hassas veriler kanunda sınırlı sayıda belirlenmiş olduğundan genişletilemez. Hassas veriler ancak 6698 sayılı kanunun 6. maddesinde yer alan istisnai hallerde işlenebilecektir.

bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtilmektedir. Türk Ceza Kanunu'nda da kişisel verilerin korunmasına ilişkin suç ve yaptırımlar belirlenmiştir. Kanunun kişilere karşı suçlar başlıklı ikinci kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde yer alan 135. maddesinde "kişisel verilerin kaydedilmesi suçu", 136. maddesinde "kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu" ve 138. maddesinde "kişisel verileri yok etmeme" eylemleri suç olarak düzenlenmiştir. Kişisel verilere ilişkin suç tiplerinde korunan hukuki değer de kişinin özel hayatı olarak ifade edilmektedir[204]. Bununla birlikte, 134. maddede ise "özel hayatın gizliliğini ihlal" suçu düzenlenmiştir. Kişisel verilere ilişkin suçlar ile özel hayatın gizliliğinin ihlali suçu arasındaki ayrımın belirsiz olduğu ve 134. maddenin bir torba düzenleme olarak nitelendirildiği de ifade edilmelidir[205]. Bu nedenle, derin sahte içeriklerin üretilmesi ve kullanılması durumunda her iki suç tipinin de tartışılması gerekecektir.

Derin sahte teknoloji ile bir kişinin görüntüsü rızası olmaksızın ele geçirilerek bir video içeriğine yerleştirildiğinde; TCK m. 136 gereği, ***kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu*** oluşabilir. Nitekim TCK m. 136'da "kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesinden" bahsedilmektedir ve kişinin görüntüsünün, onun kişisel verisi olduğuna şüphe bulunmamaktadır. Fakat burada korunan kişisel veri, kişinin özel hayat alanına dahil olduğu için herkesin ulaşabileceği bir ortamda paylaşılmamış, herkes tarafından bilinmeyen ve paylaşılmadığı sürece bilinmesi mümkün olmayan veriler olmalıdır. Dolayısıyla kişinin görüntü veya sesi, herkesin erişimine açık bir YouTube videosundan veya sosyal medya paylaşımlardan elde edilerek bir derin sahte içerik üretildiğinde bu suçun oluşmayacağı söylenebilir. Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu, iki yıldan dört yıla kadar hapis cezasını gerektiren bir suçtur. Bu suçun cezasının artırılmasını gerektiren nitelikli halleri 136. maddenin ikinci fıkrasında ve 137. maddede sıralanmıştır. Fakat bu nitelikli haller arasında ses ve görüntünün manipüle edilmesine ilişkin bir düzenleme bulunmamaktadır.

Bununla birlikte, kişilerin cinsel içerikli görüntüleri kullanılarak derin sahte porno içeriği üretildiğinde veya kullanıldığında ise benzer şekilde ***kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu***nun gündeme gelmesi beklenir. Nitekim kişinin özel hayat alanına giren tüm faaliyetler özel hayatın gizliliğini ihlal suçunun konusunu oluştururken; konuşma, haberleşme ve kişisel veri niteliğindeki hususlar ilgili suçların (m. 132, m. 133, m. 135, m. 136, m.138) konusunu oluşturmaktadır[206]. Bireyin kimliğini tanımlanabilir kılan her türlü bilgi kişisel veri olarak tanımlandığına göre, cinsel yaşamına dair görüntü de kişisel veri olabilir. Fakat Yargıtay'ın cinsel içerikli görüntülerin rıza dışında ifşasını, TCK m. 134/f. 2'e göre kişilerin özel hayatına ilişkin görüntü ve seslerin hukuka aykırı olarak ifşa edildiğinden

[204] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, Türk Ceza Hukuku Özel Hükümler, 14. Baskı, Seçkin Yayıncılık, 2019, s. 581.
[205] Güçlü Akyürek, Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Seçkin Yayınevi, Ankara, 2013, s. 213.
[206] Özbek, Doğan, Bacaksız, s. 572.

bahisle özel hayatın gizliliğini ihlal suçu kapsamında değerlendirdiği görülmektedir[207]. Bu kapsamda cinsel içerikli görüntüler, gizli yaşam alanına dahildir ve özel hayatın gizliliği hakkı kapsamında korunmaktadır[208]. Kişi, cinsel içerikli görüntüleri yalnızca kendisinin uygun gördüğü kişilerle ve uygun gördüğü ölçüde paylaşma hakkına sahiptir. Bu durumda bireyin cinsel içerikli görüntülerinin ifşası özel hayatın gizliliğini ihlal suçunu oluştururken; bireyin diğer görüntülerinin ifşası kişisel verilerin hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacaktır. Bununla beraber, cinsel içerikli görüntülerin ifşasının, haksızlığın içeriği, herhangi bir ses ve görüntü ile aynı olmadığı, söz konusu düzenlemenin bu suçla etkin mücadelede yeterli olmadığı da ifade edilmektedir[209]. Bu nedenle söz konusu teknoloji ile cinsel içerikler üretildiğinde veya kullanıldığında yeni bir suç tipine ihtiyaç olduğu da belirtilmektedir. Bu kapsamda doktrinde, TCK'nın 136. maddesine eklenecek bir hüküm ile *"cinsel içerikli görüntüleri rızaya aykırı olarak ifşa etme, yayma, erişilebilir kılma veya üretme suçunun"* düzenlenmesi önerilmektedir[210].

b. Şeref ve Haysiyete Karşı Suçlar

Derin sahte içeriklerle bir kişiye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat ediliyorsa; TCK'nın 125. maddesinde düzenlenen ***hakaret suçu*** gündeme gelebilir. Hakaret suçu, 3 aydan 2 yıla kadar hapis veya adli para cezasını gerektiren bir suçtur. TCK m. 125/f. 2 gereği hakaret suçu sesli, yazılı veya görüntülü bir iletiyle de işlenebilir. Dolayısıyla derin sahte fotoğraf veya video ile kişinin saygınlığını zedeleyecek bir içerik oluşturulduğunda bu suç oluşacaktır. Bununla birlikte, hakaret suçunun alenen işlenmesi, TCK m.125/f. 4 gereği, cezanın altıda biri oranında artırılmasını gerektirmektedir. Bu kapsamda, derin sahte görüntü ve ses içeriği ile bir kişinin onur, şeref ve saygınlığı sosyal medyada paylaşılarak rencide edildiği takdirde; söz konusu videoların aleniyet şartını sağladığı da dikkate alınarak hakaret suçunun cezanın artırılmasını gerektiren nitelikli halinin oluştuğu da söylenebilecektir.

Bununla beraber, derin sahte içeriklerin paylaşılması hem kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi hem de hakaret suçunu oluşturduğu takdirde; TCK'nın 44. maddesindeki fikri içtima kuralı gereği fail ağır cezayı gerektiren suçtan sorumlu tutulacaktır[211]. Bu durumda TCK m. 136 gereği *verileri hukuka aykırı olarak verme veya ele geçirme suçu*ndan (2yıl- 4 yıl); ifşa edilen görüntünün cinsel içerikli ise TCK m. 134/f. 2 gereği, *özel hayatın gizliliğini ihlal suçu*ndan (2-5 yıl) cezalandırılacaktır[212]. Fakat kişinin görüntü veya sesi, herkesin erişimine açık bir YouTube videosundan veya sosyal medyada

[207] Y. 12 CD, E. 2014/11530, K. 2015/384, T. 19.01.2015; Y. 12. CD, E. 2019/ 12886, K. 2020/513, T. 15.1.2020.
[208] Özbek, Doğan, Bacaksız, s. 572.
[209] Retornaz, Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etmei Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deepfake), s. 84-85.
[210] Retornaz, s. 84, 96.
[211] YCGK, E. 2012/12-1510, K. 2014/221, T. 17.06.2014.
[212] Yargıtay 4 CD, E. 2015/24024, K. 2015/39927, T. 14.12.2015; Yargıtay 12 CD, E. 2016/10995, K. 2017/7760, T. 23.10.2017.

herkese açık paylaşımlardan elde edilerek bir derin sahte içerik üretilmişse; bu takdirde korunmaya değer bir özel hayat söz konusu olmayacağı için ilgili içerik kişinin onur, şeref ve saygınlığını rencide edici nitelikte ise doğrudan hakaret suçu gündeme gelebilir.

c. Hürriyete Karşı Suçlar

Derin sahte video içeriğiyle bir kişi, kendisinin veya yakınlarının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit ediliyorsa bu takdirde; TCK'nın 106. maddesinde düzenlenen **tehdit** suçu gündeme gelebilir. Tehdit suçu, altı aydan iki yıla kadar hapis cezasını gerektiren bir suçtur. Tehdit suçunun cezanın artırılmasını gerektiren nitelikli halleri TCK m. 106/f. 2'de belirtilmektedir. Fakat söz konusu düzenlemede, teknolojinin sağladığı kolaylık ve aleniyet gibi yıkıcı bir etkiyi dikkate alan bir nitelikli hal bulunmamaktadır.

Derin sahte video içeriğiyle bir kişi, hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlanıyorsa bu takdirde; TCK'nın 107. maddesinde düzenlenen **şantaj** suçu gündeme gelebilir. Şantaj suçu, bir yıldan üç yıla kadar hapis cezasını ve adli para cezasını gerektiren bir suçtur. Fail kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde yine şantaj suçunun temel şeklinden cezalandırılmaktadır.

Bununla beraber, derin sahte içeriklerin paylaşılması hem kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi hem de tehdit veya şantaj suçunu oluşturduğu takdirde; TCK m. 44'te düzenlenen fikri içtima kuralı gereği, fail cezası ağır olan suçtan sorumlu tutulacaktır. Bu durumda TCK m. 136 gereği *verileri hukuka aykırı olarak verme veya ele geçirme suçu*ndan (2yıl- 4 yıl); ifşa edilen görüntünün cinsel içerikli ise TCK m. 134/f. 2 gereği, *özel hayatın gizliliğini ihlal suçu*ndan (2-5 yıl) cezalandırılacaktır. Fakat kişinin görüntü veya sesi, herkesin erişimine açık bir YouTube videosundan veya sosyal medyada herkese açık paylaşımlardan elde edilerek bir derin sahte içerik üretilmişse; bu takdirde korunmaya değer bir özel hayat verisi söz konusu olmayacağı için ilgili içerik ile kişi tehdit ediliyorsa veya şantaj için kullanılıyorsa doğrudan bu suçlar gündeme gelebilir.

d. Malvarlığına Karşı Suçlar

Derin sahte videolar ile bir kişi aldatılarak bir yere para göndermesi veya havale yapması istenildiğinde; TCK'nın 157. maddesinde düzenlenen dolandırıcılık suçu oluşabilir. Malvarlığına yönelik herhangi bir değer, taşınır, taşınmaz, hatta alacak hakkı da suçun hukuki konusu olabilir. Derin sahte videoların dolandırıcılık suçunda kullanım örnekleri incelendiğinde, takibi zorlaştırmak amacıyla *bitcoin* veya dijital paranın da sıklıkla kullanılabildiği görülmektedir.

Dolandırıcılık suçunun oluşabilmesi için hileli hareketlerle bir kimsenin aldatılması ve mağdurun veya başkasının zararına olarak, failin kendisine veya başkasına bir yarar sağlamış olması gerekir[213]. Bir telefon görüşmesinde derin sahte ses içeriğiyle banka hesap sahibi veya bir video konferans görüşmesinde derin sahte ses ve görüntü teknolojisi kullanılarak şirketin yöneticisi gibi davranılıp bir para transferi talimatı verildiğinde, hileli davranışlarla karşı taraf aldatılmış olacaktır. Söz konusu hileli davranış sonucu bir zarar meydana gelirse dolandırıcılık suçu oluşacaktır.

Dolandırıcılık suçu, bir yıldan beş yıla kadar hapis cezasını gerektiren bir suçtur. Bu suçun cezasının artırılmasını gerektiren nitelikli halleri 158. maddede sıralanmaktadır. Buna göre; *bilişim sistemlerinin, banka ve kredi kurumlarının araç olarak kullanılması suretiyle* (m. 158/1-f), *basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle* (m. 158/1-g) işlenmesi halinde üç yıldan on yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunmaktadır. Madde gerekçesinde bilişim sistemi, *"verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler"* olarak tanımlanmaktadır. Bu kapsamda derin sahre teknoloji bir bilişim sistemi olmamasına rağmen bu içeriklerin üretilmesi sadece bilişim sisteminin kullanılmasıyla mümkün olabilir. Bu durumda derin sahte teknoloji kullanılarak hazırlanan ses ve görüntü içeriklerinin kullanılması belirtilen söz konusu nitelikli unsurların oluşmasına neden olabilir. Nitekim manipüle edilen içeriklerde bilişim sistemi kullanıldığı gibi olayın özelliğine göre, bu içeriklerin basın ve yayın araçları ile alenileştirilerek de karşı tarafın aldatılması söz konusu olabilir.

Bununla beraber, derin sahte içeriklerin paylaşılması hem kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi hem de dolandırıcılık suçunu oluşturduğu takdirde; TCK m. 44'te düzenlenen fikri içtima kuralı gereği fail cezası ağır olan suçtan sorumlu tutulacaktır. Bu durumda fail, dolandırıcılık suçundan cezalandırılacaktır.

e. Bilişim Sistemine Karşı Suçlar

5237 sayılı TCK'nın ikinci kitabının üçüncü kısmı olan "Topluma Karşı Suçlar" kapsamında onuncu bölümünde "Bilişim Alanında Suçlar" düzenlenmiştir. Bu kapsamda Kanun'un 243. maddesinde "bilişim sistemine girme suçu", 244. maddesinde "sistemi engelleme bozma, verileri yok etme veya değiştirme suçu", 245. maddesinde "banka veya kredi kartlarını kötüye kullanılması suçu", 245/A maddesinde "yasak cihaz ve programlar kullanma suçu" düzenlenmiştir.

Siber failler, başkasına ait ses kaydı, görüntü veya videoları bir bilişim sistemine hukuka aykırı olarak girip orada kalarak elde etmişse; bu takdirde *"bilişim sistemine girme suçu"* veya sistemi bozarak, verileri yok ederek veya verilerin değiştirilmesi söz konusu ise; bu takdirde *"sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu"* gündeme gelecektir. Belirtilen bu durumlar aynı zamanda *"özel hayatın gizliliğini ihlal"* veya *"kişisel*

[213] Özbek, Doğan, Bacaksız, s. 711.

verileri hukuka aykırı olarak verme veya ele geçirme" suçlarını oluşturabilir. Fakat TCK m. 44'de düzenlenen fikri içtima kuralı gereği fail cezası ağır olan suçtan sorumlu tutulacaktır.

Banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle banka veya kredi sahiplerinin zarara uğratılması söz konusu olursa, bu takdirde TCK m. 245 gereği *banka veya kredi kartlarını kötüye kullanılması suçu* akla gelebilir. Bu suçta, kartın fiziksel olarak kullanılması zorunlu olup sadece karta ait bilgilerin değil, bizatihi kartın kullanılması aranmaktadır[214]. Örneğin, *derin sahte* teknoloji ile bir kişinin sesi ve görüntüsü klonlanarak internet bankacılığı veya telefon bankacılığı ile de kart üzerindeki bilgilerin ve şifrenin kullanılması mümkündür. Böylece kart doğrudan kullanılmadan üzerindeki bilgilerle kartın kullanılması veya kullandırılması mümkün olmaktadır. Bu durumda, TCK m. 245'te düzenlenen banka veya kredi kartlarının kötüye kullanılması suçu değil; *"bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi"* söz konusu olacağı için TCK m. 244/f. 3 gereği sistemi engelleme bozma, verileri yok etme veya değiştirme suçu oluşabilir.

Bununla beraber, TCK m. 245/A gereği *"yasak cihaz ve programlar kullanma suçu*nun" oluşabilmesi için, "bilişim suçlarının veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için imal, ithal, sevk, nakil ve kabul edilmesi veya depolanması, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması gerekir. Örneğin, derin sahte içerik üreten bir program, TCK m. 158/1-f gereği dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi için bulunduruluyorsa TCK m. 245/A hükmünde düzenlenen *yasak cihaz ve programlar kullanma suçu* da oluşacaktır. Bu suçta amaç unsuruna yer verilmesi nedeniyle sadece derin sahte içerik üreten bir programın bulundurulmasının bu suçu oluşturmayacağı belirtilmelidir.

f. Diğer Suçlar

Derin sahte teknoloji, Türk Ceza Kanunu'nda düzenlenen kamu idaresinin güvenilirliğine ve işleyişine karşı suçlar, adliyeye karşı suçlar, devletin egemenlik alametlerine ve organlarının saygınlığına karşı suçlar, devletin güvenliğine karşı suçlar başta olmak üzere failler sahte ses ve görüntü teknolojisinin sağladığı kolaylığı pek çok suçun işlenmesinde araç olarak kullanabilirler. Örneğin, *derin sahte içeriklerin halk arasında korku ve panik yaratmak amacıyla tehdit* (TCK m. 213), *suç işlemeye tahrik* (TCK m. 214), *suç ve suçluyu övme* (TCK m. 215), *halkı kin ve düşmanlığa tahrik ve aşağılama* (TCK m. 216), *suç işlemek amacıyla örgüt kurma* (propaganda) (TCK m. 220/8), *iftira* (TCK m. 267), *suç uydurma* (m. 271) , *adil yargılamayı etkilemeye teşebbüs* (m. 288) gibi pek çok suçun işlenmesinde de araç olarak kullanılabileceği görülmektedir.

[214] Özbek, Doğan, Bacaksız, s. 1003.

Bununla beraber, derin sahte içeriklerle seçimlerin haksız yönlendirilmesi riski de ciddi bir sorun olarak gözükmektedir[215]. Bu kapsamda, 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun'un 151. maddesinde düzenlenen *"Oy verme gününden önceki günün saat 18 inden sonra ve oy verme gününde umumi veya umuma açık yerlerde seçim propagandası için toplantı veya propaganda yapanlar veya bu maksatla yayınlarda bulunanlar veya her ne suretle olursa olsun seçimin düzenini bozabilecek veya oy vermenin tam bir serbestlikle yapılmasına tesir edebilecek mahiyette söz, yazı veya sair suretlerle propaganda yapanlar veya asılsız şayialar çıkaranlar bir aydan altı aya kadar hapis cezasıyla cezalandırılırlar."* hükmü gündeme gelebilir. Derin sahte içeriklerle seçimi etkilemeye çalışmak, düzenlemede yer alan *"her ne suretle olursa olsun seçimin düzenini bozabilecek veya oy vermenin tam bir serbestlikle yapılmasına tesir edebilecek mahiyette söz, yazı veya sair suretlerle propaganda"* veya *"asılsız şayia"* niteliğinde fiiller olarak karşımıza çıkabilir. Fakat aynı hükümde yer alan *"oy verme gününden önceki günün saat 18 inden sonra ve oy verme gününde"* şartının, sadece *"umumi veya umma açık yerlerde seçim propagandası için toplantı veya propaganda yapmak veya bu maksatlarda yayınlarda bulunmak"* bakımından mı yoksa hükümde sıralanan tüm fiiller bakımından mı geçerli olduğu önem arz etmektedir. Nitekim eğer tüm madde için geçerli bir ifade olduğu belirtilirse; seçimi etkilemek amacıyla derin sahte içeriklerin sadece söz konusu süre zarfı içerisinde kullanılması cezalandırılabilecektir. Bu hususta madde metninde bir kesinlik gözükmese de hükmün genel amacının seçim yasaklarının başladığı süre zarfına işaret etmesi ve seçimin haksız yönlendirilmesini koruduğu anlaşılmaktadır. Bu durumda seçimi etkilemek amacıyla üretilen derin sahte içeriklerin, m. 151 hükmü gereği seçim yasaklarının başladığı süre zarfında kullanıldığı müddetçe cezalandırılabileceği söylenebilir. Bu hususta madde metninin daha açık hale getirilmesinde ve derin sahte içeriklerin seçim sonuçlarını etkilemek amacıyla kullanılmasını engelleyecek genel mahiyette kapsayıcı bir içerik kazandırılmasında fayda bulunmaktadır.

Sonuç olarak, derin sahte teknolojinin araç olarak kullanabileceği suçların tespitinde sadece Türk Ceza Kanunu'nun ikinci kitap özel hükümler bölümünde yer alan suç tipleri ile sınırlı bir inceleme yapılmasının dahi bir makale çalışmasını aşacak nitelikte olduğu görülmektedir. Bu nedenle, söz konusu teknolojinin özellikle bireylere karşı suçlardaki kullanım örnekleri incelenerek diğer suç tiplerine işaret etmekle yetinilmiştir.

Sonuç ve Değerlendirme

Bu çalışmada, bir kişinin yüzünün başka bir kişinin vücuduna yerleştirilerek sahte görsel ve işitsel içerik üretilmesini mümkün kılan derin sahte teknoloji karşısında ceza hukuku sorumluluğu değerlendirilmiştir. İnternet, sosyal medya ve anlık iletişimin hızıyla birleştiğinde derin sahte içeriklerin hem kolaylıkla üretilebilecek hem de kısa sürede geniş

[215] Mohsin Kamshad, "Yapay Zekanın Düzenlenmesi ve Yapay Zekâ Suçları", (Çev. Jülide Yaşar), Ceza Hukukunda Robot, Yapay Zekâ ve Yeni Teknolojiler, Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ed. Yener Ünver, Seçkin Yayıncılık, 2021, s. 231.

kitlelere ulaşabilecek potansiyele sahip oldukları görülmektedir. Belirtilen bu özellikleriyle söz konusu teknolojinin, temel hak ve özgürlüklere ciddi şekilde müdahale edebilecek bir potansiyele sahip olduğu ve birçok suçun işlenmesi amacıyla kullanılma riski bulunduğu belirtilmiştir. Bu kapsamda, derin sahte teknolojinin başta hakaret (m. 125), tehdit (m. 106), dolandırıcılık (m. 157), özel hayatın gizliliğini ihlal (m. 134), kişisel verileri hukuka aykırı olarak verme veya ele geçirme (m. 136) suçları olmak üzere birçok suçun işlenmesinde araç olarak kullanılabileceği tespit edilmiştir. Ayrıca *derin sahte içeriklerin halk arasında korku ve panik yaratmak amacıyla tehdit* (TCK m. 213), *suç işlemeye tahrik* (TCK m. 214), *suç ve suçluyu övme* (TCK m. 215), *halkı kin ve düşmanlığa tahrik ve aşağılama* (TCK m. 216), *suç işlemek amacıyla örgüt kurma* (propaganda) (TCK m. 220/8), *iftira* (TCK m. 267), *suç uydurma* (m. 271), *adil yargılamayı etkilemeye teşebbüs* (m. 288) gibi pek çok suçun işlenmesinde de araç olarak kullanılabileceği görülmektedir.

Buna karşın, başka suçların işlenmesinde kullanılmak üzere bir görüntü veya sesin manipüle edilmesinin Türk Ceza Kanunu'nda suç olarak düzenlenmediği görülmektedir. Nitekim söz konusu teknoloji *sahte ya da yalan içerik üretilmesine* imkân vermektedir. Salt yalan veya sahte içerik üretmenin suç olarak düzenlenmesi gerekip gerekmediği tartışılabilir. Sahte videoların ömürleri çok uzun değildir ve kısa süreli kafa karışıklığı veya panik yaratabilirler. Bu nedenle özellikle Amerika'da bilhassa ulusal güvenlik, seçimlerin manipüle edilmesini engellemek ve bilgi dezenformasyonunun önüne geçmek amacıyla derin sahte video üretilmesini belirli durumlarda cezalandıran kanunların kabul edildiği ifade edilmiştir[216]. Özellikle sosyal medyada yalan haberle mücadele etmek amacıyla Fransa ve Almanya gibi ülkelerin ardından Batı Avrupa ülkelerinde de çeşitli düzenlemelerin yapıldığı görülmektedir [217].

Bununla birlikte, başka suçların işlenmesi için sahte içerik oluşturmak şeklindeki hazırlık hareketinin cezalandırılması yaklaşımı karşısında; ceza hukukunun son çare olma ilkesinin gözden kaçırılmaması gerektiği ifade edilmelidir. Derin sahte teknoloji, bazı suçların işlenmesinde araç olarak kullanılabileceği gibi insanlığa faydalı ve iyi amaçlar için de kullanılabilecek niteliktedir. Dolayısıyla derin sahte teknolojinin nötr bir araç olduğu düşünüldüğünde; söz konusu teknolojinin ceza hukukuyla korunması gereken hukuki değerleri zarara uğratması durumunda ceza hukukunun müdahale etmesi gerektiğini düşünüyoruz. Bu kapsamda, derin sahte teknolojinin araç olarak kullanılabileceği suç tiplerinde cezanın ağırlaştırılmasını gerektiren nitelikli unsur olarak **"teknolojinin sağladığı kolaylık ve yıkıcı etkiye"** yer verilmesi makul bir çözüm olabilir. Bu çözüm ile derin sahte teknoloji açıkça kanuni düzenlemede zikredilmeyerek her geçen gün gelişen teknolojinin diğer kötüye kullanım örneklerini de kapsaması hedeflenmektedir.

---

[216] Chipman, Ferraro, Preston, First Federal Legislation on Deepfakes Signed into Law.

[217] Anthony Failo, Stephanie Kirchner, "How do you stop fake news? In Germany, with a law", The Washington Post, 5 April 2017, https://www.washingtonpost.com/world/europe/how-do-you-stop-fake-news-in-germany-with-a-law/2017/04/05/e6834ad6-1a08-11e7-bcc2-7d1a0973e7b2_story.html, Erişim Tarihi: 07.12.2021.

Kaynakça

Abanoz Öztürk, B., "Deepfake İkilemi: Sadece Eğlence mi? Tehditler ve Hukuki Tartışmalar", Lexpera Blog, 07/04/2021, https://blog.lexpera.com.tr/deepfake-ikilemi-sadece-eglence-mi-tehditler-ve-hukuki-tartismalar/, Erişim Tarihi: 11.09.2021.

Ajder, H. & Patrini, G. & Cavalli, F. & Cullen, L., The State of Deepfakes, Landscape, Threats, and Impact, Deeptrace, September 2019, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf, Erişim Tarihi: 19.03.2021.

Akkır, A. & Yıldırım, G., Bir Bilişim Suçu "Deepfake", MGC Legal, 13.03.2018, (Çevrimiçi), https://www.mgc.com.tr/bir-bilisim-sucu-deepfake, Erişim Tarihi: 16.03.2021.

Aksoy Retornaz, E., Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etmei Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deepfake), On İki Levha Yayıncılık, Mayıs 2021.

Akyürek, G., Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Seçkin Yayınevi, Ankara, 2013.

Baker, J., "Deepfakes could break the ınternet", Cpo Magazine, https://www.cpomagazine.com/cyber-security/deepfakes-could-break-the-internet/, Erişim Tarihi: 21.10.2019.

Bellware, K., "Cheer mom used deepfake nudes and threats to harrass daughter's temmates, police say", The Washington Post, 13 March 2021 https://www.washingtonpost.com/nation/2021/03/13/cheer-mom-deepfake-teammates/, Erişim Tarihi: 30.09.2021.

Chipman, J., & Ferraro, M., & Preston, S., First Federal Legislation on Deepfakes Signed into Law, Jdsupra, 24 December 2019, https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/, Erişim Tarihi: 18.03.2021.

Ciancaglini, V. & Gibson, C. & Sancho, D., Malicious Uses and Abuses of Artificial Intelligence, Trend Micro Research, Trend Micro, EUROPOL, UNICRI, 2020, s. 53-54, https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf, Erişim Tarihi: 12.09.2021.

Cole, S., "We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now", https://www.vice.com/en/article/bjye8a/reddit-fake-porn-app-daisy-ridley, Erişim Tarihi: 24.01.2018.

Dupuy, B., "Not Real News: Altered video makes Pelosi seem to slur words", AP News, 24 May 2019, https://apnews.com/article/social-media-donald-trump-nancy-pelosi-ap-top-news-not-real-news-4841d0ebcc704524a38b1c8e213764d0, Erişim Tarihi: 30.09.2021.

"Dutch MPs in video conference with deep fake imitation of Navalny's Chief of Staff, NL Times, 24 April 2021, https://nltimes.nl/2021/04/24/dutch-mps-video-conference-deep-fake-imitation-navalnys-chief-staff, Erişim Tarihi: 30.09.2021.

Fagan, K., "A viral video that appeared to show Obama calling Trump a 'dips---' shows a disturbing new trend called 'deepfakes'", Business Insider, Erişim Tarihi 03.11.2020.

Failo, A., & Kirchner, S., "How do you stop fake news? In Germany, with a law", The Washington Post, 5 April 2017, https://www.washingtonpost.com/world/europe/how-do-you-stop-fake-news-in-germany-with-a-law/2017/04/05/e6834ad6-1a08-11e7-bcc2-7d1a0973e7b2_story.html, Erişim Tarihi: 07.12.2021.

Ker, N., "Is the political aide viral sex video confession real or a Deepfake?", Malay Mail, 12 Jun 2019, https://www.malaymail.com/news/malaysia/2019/06/12/is-the-political-aide-viral-sex-video-confession-real-or-a-deepfake/1761422, Erişim Tarihi: 30.09.2021.

Mohsin, K., "Yapay Zekanın Düzenlenmesi ve Yapay Zekâ Suçları", (Çev. Jülide Yaşar), Ceza Hukukunda Robot, Yapay Zekâ ve Yeni Teknolojiler, Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ed. Yener Ünver, Seçkin Yayıncılık, 2021, s. 229-245.

National Security Commission on Artificial Intelligence, Final Report, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf, Erişim Tarihi: 12.09.2021.

Öneren, Ç.E., "Deepfake İnterneti Yıkabilir", Sanal Hukuk, https://www.sanalhukuk.net/deepfake-interneti-yikabilir/, Erişim Tarihi: 16.03.2021.

Özbek, V. Ö., & Doğan, K. & Bacaksız, P., Türk Ceza Hukuku Özel Hükümler, 14. Baskı, Seçkin Yayıncılık, 2019.

Regulation of the European Parliament and of the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intellgence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD), (Çevrimiçi), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, Erişim Tarihi: 12.09. 2021.

Sabah Gazetesi, "CEO'nun Sesini Yapay Zekâ İle Taklit Ettiler 1,4 Milyon TL Çaldılar", 3 Eylül 2019, (Çevrimiçi), https://www.sabah.com.tr/ekonomi/2019/09/03/ceonun-sesini-yapay-zekayla-taklit-ettiler-14-milyon-tl-caldilar, Erişim Tarihi: 26.03.2021.

Young, Z., "French Parliament passes law against 'fake news'", Politico, 4 July 2018.

Ceza Muhakemesinde Yapay Zekâ Temelli Risk Değerlendirme Araçları ve Hukuki Etkileri

Av. Ozan Can Özbalçık

Giriş

Edebiyat ve sinemada bilimkurgu, çizgi roman, fantastik dünyaları seven kişiler, gündelik hayatlarında bu alanları derinden etkileyen eserlerde yer alan içeriklere rastlamaktan genellikle memnuniyet duyarlar. Bu eserlerin kendi ticari getirileri bir yana, bunlardan oluşturulan figür, poster, video oyunları vb. çeşitli ürünlerin yer aldığı ve ilgililerine hitap eden farklı piyasalar da mevcuttur. Peki bu dünyalarda yer alan çeşitli içeriklerin, yine ticari sahada, bu defa devletlerin kolluk kuvvetlerinin ve yargılama mercilerinin memnuniyet duyacağı biçimde geliştirilmesi ve pazarlanması karşısında birey olarak nasıl hissetmek gerekir? Örneğin; The Lord of The Rings (Yüzüklerin Efendisi) serisinin kötücül karakteri Sauron'un iletişimini ve zihinlere girmesini sağlayan büyülü küresi "Palantir"in, devletlerin istihbarat ve kolluk teşkilatlarına öngörücü polislik araçları pazarlayan bir teknoloji şirketinin adı olduğunu[218] veya Philip Dick'in sinemaya da uyarlanan Minority Report (Azınlık Raporu) öyküsündeki suçu ve failini önceden tahmin eden precogları (kahinler) gibi bu defa kolluk kuvvetlerinin suçu ve suçluları tahmin etmek için kullandığı yapay zekâ destekli teknolojilerin şirketler tarafından pazarlandığını bilmek karşısında aynı memnuniyeti yaşamak mümkün olabilir mi?

Hukuk perspektifinden bakıldığında, bu soruya olumlu yanıt vermenin güç olduğunu söylemek gerekir. Zira bu "ürünler", birçok karmaşık ve önemli meseleyi teknolojiyle kolaylaştırıyor gibi görünmekle birlikte, başta temel hak ve özgürlükler olmak üzere birçok hukuki kurumun yapısına uygun olmayan müdahalelere neden olmaktadır. Söz gelimi, sanığın yargılama süresince tutuklu kalıp kalmayacağı değerlendirmesinde, bu zaman zarfında yeni bir suç işleme riskini belirleyen bir karar destek algoritması kullanılması halinde, bu algoritmanın beslendiği veriler nedeniyle ırkçılığa dayanan ayrımcı bir sonucun ortaya çıkmasına ve algoritma içeriğinin sanık tarafından öğrenilememesi durumu da silahların

[218] Palantir'in ürünlerden biri olan küresel karar verme platformu Gotham, aynı zamanda DC çizgi roman dünyasının popüler karakterlerinden Batman'in yaşadığı ve türlü suçlarla savaştığı, genellikle sisli ve karanlık tasvir edilen kurgusal şehrin adıdır. Palantir (2021), https://www.palantir.com/platforms/gotham/, Erişim Tarihi: 16.09.2021. Amerika Birleşik Devletleri merkezli Palantir özellikle Avrupa'daki polis teşkilatlarının ilgisini cezbetmiş görünmektedir. Fransız Gizli Servisi, Danimarka Ulusal Polis Teşkilatı, kimi Alman eyaletleri ve Hollanda'da birçok yerel kolluk kuvvetinin Palantir'in veri analiz araçlarını satın aldığı bilinmektedir. Fieke Jansen, Data Driven Policing In The Context Of Europe, 2018, s.9, https://www.datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf, Erişim Tarihi: 01.10.2021.

eşitliği ilkesinin ihlaline neden olabilir. Başka bir örnek vermek gerekirse, belirli yerleşim alanlarında bulunanların suç işleme olasılıklarına göre tehlike puanlarıyla kategorilere ayrıldığı ve bu puanların niteliğine göre çeşitli kolluk müdahalelerine maruz kalma risklerinin arttığı bir veri tabanında yer almak, özel hayatın gizliliği başta olmak üzere birçok temek hakka müdahale teşkil edebilir. Bu çalışmada, ceza muhakemesinin çeşitli evrelerinde kullanılan yapay zekâ destekli araçların mevcut veya olası etkileri, bu perspektif bağlamında incelenmiş; giderek artış eğilimi gösteren algoritmik yaklaşımların, mevcut kazanımların yapısını bozmadan, verimli biçimde ceza adaleti sistemine entegre edilebilmesi imkânı ele alınmıştır.

1. Algoritmik Sistemlerin Ceza Muhakemesi Süreçlerinde Kullanımı

Gelecekteki suç faaliyeti riskini değerlendirme amaçlı işlemler, ceza adalet sistemlerinde uzun süredir uygulanmakla birlikte, "risk değerlendirmesi" terimi, genellikle gelecekteki suç olasılıklarını tahmin etmek için resmî, aktüeryal veya algoritmik yöntemlerin kullanımına atıfta bulunan bir içeriğe sahiptir. Bu amaçla kullanılan araçlar, kefalet veya salıverilme koşullarının, ceza süresinin veya denetimli serbestlikte denetim düzeyinin belirlenmesine, şartlı tahliye talebinin değerlendirilmesine ve çocuk suçlular için uygun rehabilitasyon programı veya özgürlükten yoksun bırakma seçimi gibi birçok önemli karar sürecinde destek araçları olarak kullanılmaktadır[219]. Klinik değerlendirmeler ve karar vericilerin deneyimlerine dayanan birinci nesilden suç geçmişi, yaş ve cinsiyet gibi statik faktörlere dayalı ikinci nesile; risk ve ihtiyaçlarla birlikte dinamik ve statik faktörlere dayanan üçüncü nesilden bu faktörleri birlikte değerlendirerek bireyselleştirilmiş planlara dayanan dördüncü nesile ve makine öğrenmesi tekniklerini kullanarak gerçek zamanlı olarak ve çok daha karmaşık tekniklerle mükerrer suçluluğu tahmin için kullanılabildiği beşinci nesile evrilmiştir[220]. Bugün algoritmik risk değerlendirme araçları ceza muhakemesinin birçok karar evresinde kullanılmakla birlikte, özellikle yargılama esnasında sanığın tutuklu kalmasına ve serbest kalırsa bu sürede yeniden suç işleyip işlemeyeceğine yönelik riskleri değerlendiren (pre-trial) araçlar, Amerika Birleşik Devletleri başta olmak üzere birçok ülkede oldukça popülerlik kazanmış görünmekte; makine öğrenimi ve yapay zekâ ile geliştirilmektedir. Avrupa ülkelerinin de "algoritmize etme eğiliminin" bir parçası olarak bütçeleri ve dava yüklerini azaltmak endişeleriyle bu araçları sistemlerine entegre etmeye başladığı görülmektedir[221].

Diğer taraftan algoritmik araçların kullanımı yalnızca yargılama evreleriyle sınırlı kalmamaktadır. Bir suçun ne zaman ve nerede meydana gelebileceği veya kimlerin suç faaliyetlerinin faili ya da mağduru olabileceği olasılıklarını tahmin etmek için geçmiş ve eş zamanlı verileri kullanan öngörücü polislik (predictive policing) teknolojileri de polis ve

[219] Megan Stevenson, Assessing Risk Assessment in Action, Minnesota Law Review, Sayı:103, 2018, s.314-315.
[220] John Villasenor/Virginia Foggo, Artificial Intelligence, Due Process and Criminal Sentencing, Michigan State Law Review, Cilt:2, 2020, s.307-309.
[221] Aleš Završnik, Algorithmic Justice: Algorithms and Big Data In Criminal Justice Settings, European Journal of Criminology**,** Cilt:18, Sayı:5, 2021, s.3.

istihbarat teşkilatları tarafından yaygın biçimde kullanılmaktadır[222]. Kişi bazlı yaklaşımlar (öngörücü profilleme), geçmişteki ve mevcuttaki davranış kalıplarının, bireysel özelliklerin ve sosyal ilişkilerdeki kimi özelliklerin, kişilerin gelecekteki eylemlerini tahmin etmek için göstergeler olarak kullanılabileceği varsayımına dayanmaktadır. Mekân bazlı yaklaşımlar (öngörücü haritalama) ise "hot spots" olarak da bilinen, geçmiş verilere göre çevrelerinden daha yüksek suç oranı gösteren coğrafi bölgelerde, benzer türde ve oranda suçların nispeten istikrarlı biçimde tekrarlanabileceği beklentisine yönelik olarak suçluluğun yönetilebileceği varsayımıyla hareket etmektedir[223]. Verilere erişim ve kapsamlı teknolojilerdeki artışın, Avrupa'da polis teşkilatlarını tepkisel polislikten öngörücü polisliğe ve suçları önleyip soruşturmak adına veriye dayalı karar alma entegrasyonlarına yönlendirdiği gözlemlenmektedir[224].

2. Algoritmik Sistemlerin Ceza Adaleti Süreçlerine Katkıları

Suçluluğa ilişkin çeşitli alanlarda kullanılan risk değerlendirme araçlarının, birçok faydası bulunması sebebiyle, yaygın biçimde kullanılmaya başlandığı ve bu eğilimin süreceği ifade edilmektedir. Ceza adalet sistemlerinin, odağını "anlatıcılardan" daha objektif ve ön yargısız olan bilgisayar veri tabanlarına yönlendirdiği ve buradan da algoritmik tabanlı karar vermeye doğru adım atmanın eşiğinde olduğu iddia edilmektedir. Bunun sonucu olarak, bir veri tabanında yer alan statik bilgilerden yararlanıyor da olsa karar vericilerin müdahalesine ihtiyaç duyan bir sistem yerine, otomatik araçlarla bağımsız kararların alınabileceği; yargıları genellikle olumsuz olarak görülen ve hatalarla ilişkilendirilen uygulamacıların takdir yetkisini kısıtlasa da bu araçların nihai karara nesnellik katabileceği ileri sürülmektedir[225]. Diğer yandan bu araçların hükümlerin tutarlılığını sağlayabilme, adalet sistemindeki sınırlı kaynakları verimli kullanabilme ve insan hataları ile ön yargı risklerini azaltma potansiyeline sahip olduğu da savunulmaktadır[226].

Bu teorik argümanların dışında sistemlerin başarılı olduğu iddiasını kuvvetlendirebilecek kimi çalışmalar da bulunmaktadır. Söz gelimi 1.36 milyon tutukluluk vakası üzerinde yapılan çalışmada, bir sistemin, şüphelinin kaçıp kaçmayacağını veya yeniden suç işleyip işlemeyeceğini bir insan yargıçtan daha iyi tahmin edebileceği gösterilmiştir[227]. Farklı bir çalışmada ise risk değerlendirme algoritmalarına dayanılarak yargılama öncesi gözetim kararlarının sonucu olarak suçta %25'e, hapis cezasına mahkumiyette %42'ye varan azalmalar gerçekleştirilebileceği iddia edilmiştir[228]. Birleşik Krallık'ta kullanılan Gang Matrix

---

[222] Jansen, s.7. Çok fazla verinin olduğu alanlarda insanların verilerden mümkün olduğunda çok yararlı bilgi sahibi olabilmek için yapay zekâ kullanma fırsatları arayacağı ve ceza adalet sistemlerinin bu alanlardan biri olduğu ifade edilmektedir. Bkz: Villasenor/Foggo, s.307.

[223] Simon Egbert/Matthias Leese, Criminal Futures Predictive Policing and Everyday Police Work, New York, Rooutledge, 2021, s.28-35.

[224] Jansen, s.1.

[225] Završnik, s.13.

[226] Villasenor/ Foggo, s.298.

[227] Završnik, s.3.

[228] Stevenson, **s.**305.

isimli risk değerlendirme aracının devreye girdikten sonra takip ettiği kişiler açısından suç işleme oranını ve şiddet olaylarından kaynaklı mağduriyetleri belirgin biçimde düşürdüğünü iddia eden sonuçlar açıklanmıştır[229]. Almanya'nın farklı eyaletlerinde kullanılan PreCobs (Bavaria / Baden-Württemberg), KrimPro (Berlin), PreMap (Aşağı Saksonya), KLB-operativ (Hessen) ve SKALA (Kuzey Ren-Westfalya) isimli yakın tekrar temelini esas alan ve özellikle konut içi hırsızlıklar ve araç hırsızlıklarını önlemek amaçlarıyla kullanılan teknolojilerle başarı gösterildiği belirtilmektedir[230].

3. Risk Değerlendirmenin Riskleri

Risk değerlendirme araçlarının yaygın kullanımının mevcut ve potansiyel faydalarının yanında hâlihazırda ön yargıları şiddetlendirmek ve adalet sisteminin merkezinde yer alan temel ilkeleri baltalamak gibi birçok etik ve hukuki riski bünyesinde barındırdığı yönünde önemli endişeler mevcuttur. Bu araçlardaki en temel sorunlardan biri, tahminin kendi doğasında bulunmaktadır. Zira geleceğe ilişkin tüm tahminler, esasen geçmişe bakılarak yapılacağından, geçmişin eşitsizliklerinin geleceğe yansıması riski oldukça yüksektir[231].

3.1. Ayrımcılık

Bu eşitsizlik ve endişelerin başında, algoritmaların yapısı gereği ırka ve etnik kökene dayalı ayrımcılık yapma ihtimali bulunmaktadır. Risk değerlendirme algoritması özellikle ırk, sosyoekonomik durum vb. faktörleri göz önünde bulundurmaktan kaçınmak için tasarlansa bile, değerlendirmeyi gerçekleştirmek için güvenilen veriler nedeniyle bu tür faktörler dolaylı olarak incelemeye dahil edilebilir. Örneğin, Iowa Risk Revize aracı, (diğer faktörlerin yanı sıra) sanığın istihdam ve ikamet durumu, mevcut mahkumiyeti ve önceki mahkumiyetleri ile ilgili girdileri de risk değerlendirmesinde kullanmaktadır. Değerlendirmede kullanılan bu faktörlerin tümü esasen tarihsel ve devam eden ırk ayrımcılığı modellerinden oldukça etkilenmektedir. Afrikalı-Amerikalıların hem kolluk kuvveti hem de ceza adaleti sisteminde orantısız bir şekilde hedef alındıkları bilinen bir olgudur. Dolayısıyla bu değerlendirmeden çıkacak sonuç; risk ölçme faktörlerinden biri olan geçmiş suç mahkumiyeti kaydının ırkla ilişkili olabileceği ve çıktının bu ön yargıdan beslenerek ayrımcılığa teknolojik bir form kazandırabileceğidir[232].

---

[229] Metropolitan Polis Teşikilatı tarafından çete şiddetlerini azaltmak, bu eylemlere karışan üyeleri belirlemek, çeteler tarafından sömürülenleri korumak ve riskleri değerlendirmek için kullanılan bir istihbarat aracıdır. Sistem bu kişilere risk puanlaması yapılması esasına dayanmaktadır. The Metropolitan Police Service, MPS Gang Violence Matrix Frequently Asked Questions, https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence-matrix/, Erişim Tarihi: 23.7.2021.

[230] Kai Seidensticker/Felix Bode/Florian Stoffel, Predictive Policing in Germany, 2018, http://kops.uni-konstanz.de/bitstream/handle/123456789/43114/Seidensticker_2-14sbvox1ik0z06.pdf?isAllowed=y&sequence=5, Erişim Tarihi: 29.8.2021.

[231] Villasenor/ Foggo, s.298.

[232] Villasenor/ Foggo, s.298.

2016 yılında, bu endişe verici ihtimalin gerçekleştiğine ilişkin bir çalışma sonucu kamuoyuyla paylaşılmıştır. ProPublica tarafından yayımlanan raporlara göre ABD'de Wisconsin ve bazı başka eyaletlerde mükerrer suç işleme risklerini tahmin etmek için kullanılan COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) algoritmasının, siyahilere daha yüksek risk puanları atayarak ayrımcılık yaptığı iddia edilmiştir. Algoritmada siyahilerin yüksek riskle puanlanmalarına karşın mükerrer suçluluğunun daha az olduğu, buna rağmen beyazların daha düşük riskle puanlanmalarına rağmen mükerrer suçluluğun daha yüksek olduğuna ilişkin bulgular ortaya konulmuştur[233]. COMPAS'ın geliştiricisi Northpointe (şu anda Equivant) ise bulguların gerçeği yansıtmadığını ve sonuçlara göre siyahilerle beyazların risk değerlendirmeleri arasında bazı küçük oransal farklılıklar olduğunu, tekrar suç işleyeceği öngörülen siyahilerin gerçekten de beyazlardan daha fazla suç işlediğini, suç işlenmeyeceği tahminin de aynı doğrultuda sonuçlandığını ve bulguları ile yöntemlerinin ırkçılığa işaret etmediğini savunmuştur[234]. Taraflar birbirinin zıttı argümanları ileri sürmeye devam etse de sistemlerin bahsedilen yapısı gereği bu endişelerin tamamen giderildiğinden veya giderilebileceğinden söz edebilmek mümkün değildir.

Ayrımcılığı önlemek için yapay zekâ kullanımının yeterince düzenlenememesinin tehlikelerine Avrupa'da da tanık olunmuştur. Hollanda genelinde kullanılan tahmine dayalı bir polislik yazılımı olan CAS (Crime Anticipation System) erken dönemlerinde, etnik kökeni, bir suçun işlenme olasılığını belirlemek için ilgili bir faktör olarak dikkate almak üzere tasarlanmıştır. CAS'ın belirli bir alandaki suçları tahmin etmek için kullandığı göstergeler arasında, "Batılı olmayanların sayısı" da bulunmaktaydı. Yazılım, yalnızca etnik köken ve suç arasında bir ilişkinin varlığını varsaymakla kalmamış, aynı zamanda özel bir etnik köken kategorisini de dikkate alarak oldukça şüpheli ve ön yargılı bir sistem oluşturmuştur[235].

Uluslararası Af Örgütü'nün yukarıda bahsi geçen Gang Matrix sistemine ilişkin yayımladığı raporda, az sayıda dahil olmalarına rağmen şiddet olaylarından siyahiler, Asyalılar ve etnik azınlıkların ezici oranda sorumlu tutuldukları ve bu gruplara kolaylıkla çete mensubu etiketinin yapıştırıldığına ilişkin veriler sunulmuştur[236].

---

[233] Julia Angwin/Jeff Larson/Surya Mattu/Lauren Kirchner, Machine Bias: There's Software Used Across the Country to Predict Future Criminals and It 's Biased Against Blacks, PROPUBLICA, 2016, https://www.propublica.org/article/machine-bias-risk-assessmentsin-criminal-sentencing, Erişim Tarihi: 20.7.2021.

[234] William Dieterich/Christina Mendoza/Tim Brennan, COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity, Northpointe, 2016, s.20-22, http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf, Erişim Tarihi: 22.7.2021.

[235] Fair Trials, Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU Policy Paper, s.17, https://www.fairtrials.org/sites/default/files/Regulating%20Artificial%20Intelligence%20for%20Use%20in%20Criminal%20Justice%20Systems%20-%20Fair%20Trials.pdf, Erişim Tarihi: 18.10.2021.

[236] Amnesty, Trapped In The Matrix, Secrecy, Stigma and Bias In The Met's Gangs Database, 2018, s.15-17, https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf, Erişim Tarihi: 24.7.2021.

Diğer taraftan özellikle polis uygulamalarının veri tabanları yine önceki uygulamalardan ve verilerden hareketle güncellemektedir. Polis aktivitesinin bölgesel olarak daha fazla suç işlendiği düşünülen yerlerde olacağı ve bu da bölgedeki polis ihtiyacını ve hareketliliğini de artıracağından, öngörücü yazılımların kullanılmasının kısır döngüye neden olabileceği dikkate alınmalıdır[237]. Ayrıca, aşırı polisliğin tersine, polisin belli alanları daha az incelediği yetersiz polislik sonucu, buralarda işlenen suçların sistemce göz ardı edilmesi, orantısız bir adalet duygusuyla beraber suça ilişkin verilerin de eksik olmasına ve öngörücü polisliğin sosyoekonomik açıdan dezavantajlı gruplar üzerinde uygulanmasına neden olacaktır[238]. Birleşik Krallık'ta yukarıda bahsedilen yanlış tespitler doğrultusunda ilgili grupların tutuklanma oranlarının ölçüsüz biçimde daha yüksek olduğu ve hatalı olarak sistemi, bu grupların yaşadıkları veya zaman geçirdikleri yerlerde daha fazla suç işlendiği varsayımına ittiği tespit edilmiştir[239].

Görüldüğü üzere algoritmik sistemlerin geçmişin ve günümüzün ön yargılarına dayanan ayrımcı çıktılarını veya başkaca hatalı uygulamalarını, görünüşte bilimsel olarak karar alıcıların önüne getirme ya da daha tehlikelisi bunların herhangi bir değerlendirme fırsatı bulunmadan doğrudan ayrımcı biçimde uygulanabilme tehlikesi mevcuttur.

3.2. Adil Yargılanma

COMPAS risk değerlendirme aracı, yine 2016 yılında, bu defa bir mahkeme huzurunda sanık hakları ekseninde tartışılmıştır. *Loomis v. Wisconsin* davasına konu olayda, COMPAS'ın kendisine ilişkin risk puanı da gözetilerek şartlı tahliye imkânı ortadan kaldırılan ve ceza alan sanık, COMPAS'ın bu süreçte kullanımının adil yargılanma hakkını ihlal ettiğini, algoritmanın resmî kullanımı gereği değerlendirmelerinin bilimsel geçerliliğine itiraz edemediğini ve değerlendirmesinde cinsiyeti dikkate aldığını ileri sürerek karara itiraz etmiştir[240]. Wisconsin Yüksek Mahkemesi ise COMPAS çıktılarının Loomis hakkında verilen kararda belirleyici bir faktör olmadığını, diğer faktörlerin yanında bir gözlem sağladığını değerlendirerek itirazları reddetmiştir[241].

COMPAS algoritmasının standart bir model kullanımı nedeniyle hükmün bireyselleştirilmesine aykırı olduğu iddialarına yönelik başka kararlarda da bu sonuçların hâkime suçlunun ıslahına yönelik bireyselleştirilmiş uygun programlar seçme imkânı vereceği

---

[237] Završnik, s.13.

[238] Završnik, s.14. Buket Abanoz Öztürk, Ceza Muhakemesinde Sanığın Mükerrer Suç İşleme Riskinin Hesaplanması: COMPAS Algoritması ve Adil Yargılanma Hakkı, Yapay Zekanın Cezai Sorumluluğu, Ankara, Adalet Yayınevi, 2021, s.93-94.

[239] Jansen, s.9.

[240] Villasenor/ Foggo, s.334.

[241] State of Wisconsin v. Loomis, 881 N.W.2d 749, 2016. Öte yandan mahkeme cinsiyetin bir faktör olarak kullanılmasına ilişkin itirazlara yönelik olarak risk puanlamasında bu uygulamanın olgusal bir temeli olduğunu, bu ayrımı yapmayan bir değerlendirmenin her iki cinsiyettekileri de hatalı sınıflandıracağı, mevcut durumun ayrımcılıktan ziyade bu kişilerin çıkarlarına hizmet ettiğini belirtmiştir. Zira istatistiksel olarak kadınların erkeklere göre daha düşük oranda mükerrer suçlu olduğu bilinmektedir.

[242], hükümde COMPAS'a yapılan atıfların rutin olarak alınan denetimli serbestlik görevlilerin hazırladığı raporlara atıf yapmaktan bir farkı bulunmadığı[243] gibi sebeplerle itirazlar yerinde bulunmamıştır.

Bu kararlar ve yargı süreçleri, yargılama aşamasında kullanılan risk değerlendirme araçlarının hukuki etkilerine yönelik bazı soruları da beraberinde getirmektedir. Örneğin Loomis kararında, mahkemenin algoritma sonucunun kararda belirleyici faktör olmadığı kabulü karşısında bu verilerin sanığın değerlendirilmesine ilişkin raporlarda neden yer aldığı sorusu her halükârda cevapsız kalmaktadır. Keza bu algoritmanın özel bir şirkete ait olması nedeniyle yazılımının sanık veya müdafi tarafından denetlenememesi, silahların eşitliği ilkesi bakımından tartışmalı görünmektedir. Risk değerlendirme yazılımı üreten şirketlerin, pazardaki rakiplerine karşı avantaj sağlamada kilit faktörler olabileceğinden, algoritmalarının ticari sır kapsamını koruma konusunda endişeleri makul sayılabilir[244]. Ancak bu ürünler bireylerin temel hak ve hürriyetlerine en ağır müdahalede bulunan kamusal bir sistem tarafından kullanıldığında, mülkiyete dayalı korumanın geri planda kalmasını beklemek veya en azından sanığın haklarını etkili kullanmasını engellemeyecek bir denge talep etmek oldukça doğaldır.

Şeffaflık, adil yargılanma hakkını destekleyen çelişmeli sürecin temel bir yönüdür ve insan hakları standartları, istisnalar haricinde genel bir kural olarak sanıklara, dava dosyalarına sınırsız erişim ile deliller hakkında yorum yapma fırsatı verilmesini gerektirir. Bu standartların özgürlükten yoksun bırakma kararları için, mahkeme öncesi karar verme süreçleri bağlamında da geçerli olduğuna şüphe yoktur. Sanık aleyhinde kullanılan delillerin kendisiyle paylaşılmaması için belirli gerekçeler kabul edilse dahi, bunlar sınırlı sayıda ve dar kısıtlamalar olup ticari çıkarlar, aksi yönde davranmak için geçerli bir gerekçe olarak kabul edilemeyecektir[245]. Dolayısıyla yargılamada kullanıldığı ve hâkimin kararının gerekçelerini oluşturduğu anlaşılan bir aracın çıktısının yerinde olup olmadığını denetlemeyi talep edebilme hakkı, silahların eşitliği ilkesinin zaruri bir sonucu olarak görülmektedir. Başkalarına ait geçmiş deneyimler ve kalıpların kullanıldığı bir çıktının kişinin geleceğine etki edip etmemesi gerektiği tartışması bir yana, sanığın yalnızca teoride değil; fiili olarak da maddi içeriği yanlış olmayan bilgiler uyarınca hüküm verilmesini denetleme imkânının ve hakkının mevcut olması gerekmedir[246]. Sonuç olarak, böyle bir uygulamanın, silahların eşitliği bağlamında adil yargılanma hakkına halel getirdiği görülmektedir[247].

---

[242] Malenchik v. State of Indiana, 928 N.E.2d 564, 2010, https://www.courts.ca.gov/documents/malenchik-decision.pdf, Erişim Tarihi: 10.10.2021.
[243] State of Michigan v. Younglove, No. 341901, 2019, https://casetext.com/case/people-v-er-in-re-younglove, Erişim Tarihi: 10.10.2021.
[244] Villasenor/ Foggo, s.343.
[245] Fair Trials, s.29.
[246] Villasenor/ Foggo, s.315.
[247] Abanoz-Öztürk, s.91-92.

Algoritmanın denetlenememesinin yanında yukarıda değinildiği üzere yadsınamayacak ve azımsanamayacak ölçüde hatalı, etik ya da hukuki açıdan geçerli olamayacak sonuçlar verme ihtimali karşısında, çıktıların adeta bir doğruluk karinesine yol açan bu uygulaması masumiyet karinesi çerçevesinde de tartışmalıdır. Teknik bilgi de gerektirdiğinden sanıktan başka kimsenin yanlışlama çabasına girmeyeceğini varsayabileceğimiz bu durum, adeta yanlışı kanıtlama yükümlülüğünün sanığın üzerinde kalmasına yol açmaktadır. Bu riske ilave olarak statik algoritma yerine, gelişimiyle paralel biçimde zamansal olarak değişikliğe uğrayan yapay zekâlı bir sistemin kullanılması durumunda, teorik olarak dahi yanlışı ispat imkânından söz edebilmek güç olacaktır[248].

Risk değerlendirme araçları ve masumiyet karinesi ilişkisi kapsamında gündeme gelebilecek bir diğer konu ise öngörücü polislik uygulamalarına maruz kalanların durumudur. Polisin suçu işlenmeden önce engelleme amacının yansıması olarak henüz suça ilişkin emarelerin olmadığı dilimlerde dahi kişilerin çeşitli sistemlerde risklilik değerlendirmelerine maruz kalmaları olasıdır. Kimi ülke örneklerinde (bkz: Gang Matrix) bu kişilerin risklilik durumları bazı kamu kurumlarına bildirilerek çeşitli sosyal imkânlarının kısıtlandığı da görülmüştür. Bu uygulamalar, suçluluk veya masumiyet meselesinin ancak adil ve hukuka uygun bir ceza adaleti süreciyle belirlenebileceği şeklindeki temel insan hakları ilkesine ciddi şekilde zarar vermektedir. Kimi öngörücü uygulamaların ahlaki ve etik açıdan masumiyet karinesini ihlal ettiği açık olsa da hukuki açıdan, özellikle Avrupa İnsan Hakları Mahkemesi içtihatları doğrultusunda, bu önleyici tedbirlerin masumiyet karinesi kapsamı dışında kalabileceği söylenebilir[249]. Ancak uygulamaların yapıları gereği insan hakları korumasının etkisinden azade olacağını söyleyebilmek pek mümkün değildir. Zira bu uygulamalar genellikle gözetlemeyi hedeflediklerinden özel hayatın gizliliğine dolaylı ya da doğrudan müdahalelerde bulunmaktadır[250].

3.3. Kişi Özgürlüğü ve Güvenliği

Karar destek aracı olarak kullanılan risk değerlendirme araçları aşırı tahminde bulundukları gerekçesiyle eleştirilmektedir. Yargılama öncesi tutukluluk durumuna ilişkin değerlendirme yapan araçlar tipik olarak yalnızca serbest bırakılan kişilerle ilgili yeniden suç işlenmesine ilişkin verilere dayanır, bu nedenle algoritmalar, geçmişte mahkemeler tarafından gözaltına alınan kişilerin haklı olarak özgürlüklerinden mahrum bırakıldığı varsayımına dayanmaktadır. Fakat geçmişte tutuklananların çeşitli hakları ihlal edilerek özgürlüklerinden yoksun bırakıldığı ihtimalinin göz ardı edilmesi ve kural olarak tutuksuz yargılamayı önceleyen bir

[248] Villasenor/ Foggo, s.322.
[249] Ceza yargılamasının başlangıcının belirsiz hale geldiği, bir kişinin ne zaman tüm ilgili haklara sahip bir şüpheliye dönüştüğünün artık net olmadığı ve yeni matematiksel dilin, ceza muhakemesi kurallarının şimdiye kadar saygı duyulan duvarlarını yıkmaya yardımcı olduğu yönünde eleştiriler için bkz: Završnik, s.6.
[250] Fair Trials, s.6.

tasarım olmadıkça araçların etkin kullanımıyla kişi özgürlüğü ve güvenliği hakkının ihlali gündeme gelebilir[251].

3.4. Mahkemenin Bağımsızlığı ve Tarafsızlığı

Risk değerlendirme araçlarının adil yargılanma çerçevesinde gündeme getirebileceği sorunlardan biri de hâkimin vicdani kanaatine dayanacak kararını, "bilimsel, tarafsız ve teknolojik bir çıktı" olarak kendisine sunulan veriler üzerinden değerlendirmesinin bağımsızlık ve tarafsızlığına etki edip etmeyeceği meselesidir. Yapılan araştırmalarda hâkimlerin bu çıktıları kabullendikleri, riskten kaçınma eğilimleriyle bu sistemlerin önerilerine ilişkin pasif bir kabulleniş hâlinde oldukları ifade edilmektedir[252]. Otomasyon ön yargısı olarak tarif edilen bu olgu, otomatik yardımlara diğer tavsiye kaynaklarından daha fazla güç ve yetki atfetme eğilimini ifade etmektedir. Araştırmalara göre insanların bilinçaltında zor olarak değerlendirdiği görevleri üstün analiz ve yeteneklere sahip güçlü ajanlar olarak gördüğü makinelere devretmeyi tercih etmeleri nedeniyle bu eğilime sahip olabileceği belirtilmektedir. Hâkimlerin de karar verirken hem otomasyon ön yargısı hem de beynin karmaşık zihinsel görevlerle uğraşırken buluşsal yöntemlere veya basit pratik kurallara güvenmeye yönelik doğal eğilimlerinden hareketle sistem kararlarını daha rahat benimseyeceği öngörülmektedir[253].

Esasen hâkimler de mükerrerlik durumunu değerlendirirken bizzat risk değerlendirmeleri yapmakta ve karar verme süreci şüphesiz insan deneyimini, kültürünü ve hatta ön yargıları içermektedir. Destek araçlarının hâkimlerin sübjektif hatalarını ortadan kaldırabileceği yönündeki beklentilere rağmen bireysel ve bağımsız karar verme süreçlerinin kişilerin ihtiyaçlarına ve beklentilerine daha uygun hale getirilebileceği, bu tür kişisel özelliklerle duygusal zekânın desteklenmesi gerektiği de ileri sürülmektedir[254]. Yaklaşımların yerindeliğine ilişkin somut veriler bulunmasa da birçok farklı sebepten ötürü hâkimlerin kararlarına yönelik teknolojik destekli bu çıktıları görmezden gelmelerinin zor olduğunu öngörebilmek mümkündür.

Yargılamanın yalnızca belirli kriminolojik sonuçları değil aynı zamanda tam anlamıyla adalet duygusunu yansıtması da oldukça önemlidir. Ceza adaleti sistemiyle doğrudan muhatap kalan kişilerin, kendileri hakkında "soğukkanlı" makineler yerine empati kurabilen hâkimler tarafından karar verilmesini istemesi doğaldır ve bunun sağlanması elzemdir[255].

---

[251] Fair Trials, s. 15.
[252] Abanoz-Öztürk, s. 97-98.
[253] Andrew Lee Park, Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing, 2019. https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/, Erişim Tarihi: 09.09.2021.
[254] Završnik, s. 12.
[255] Završnik, s. 16.

4. Çözüm Önerileri

Ceza yargılaması ve ceza muhakemesinin diğer evrelerinde kullanılan risk değerlendirme araçlarının etik ve hukuki açıdan sebep olduğu ya da olabileceği sorunların ortaya konulmasından sonra bunlara yönelik çözüm önerilerinin de değerlendirilmesi gerekmektedir.

Ayrımcılık riski bağlamında risk değerlendirme sistemlerinin ayrımcı olmayan sonuçlar üretecek, şüpheli ve sanıkların ırk veya etnik köken de dahil olmak üzere özellikleri nedeniyle doğrudan veya dolaylı olarak dezavantajlı olmamasını sağlayacak şekilde geliştirilmesi gerekmektedir. Bu sistemlerin, herhangi bir ayrımcı etkinin tanımlanıp ele alınabilmesi için dağıtımdan önce ve sonra zorunlu ve bağımsız testlere tabi tutulması ve yapay zekâ sisteminin ayrımcı sonuçlar üretmediği kanıtlanamadığında, kullanılmaması gerektiği önerilmektedir[256]. Avrupa Parlamentosu da Ceza Hukukunda Yapay Zekâ ve Bunun Cezai Konularda Polis ve Adli Makamlar Tarafından Kullanımına ilişkin 6 Ekim 2021 tarihli kararında bu tehlikelerin dikkate alınarak yapay zekâ teknolojilerinin bilim ve teknoloji çalışmaları, ırka dayalı çalışmalar, engellilik çalışmaları ve sosyal yaşamla uyumlu diğer disiplinler dahil olmak üzere disiplinler arası araştırma ve girdilerle oluşturulması gerektiği ve ayrıca kolluk kuvvetleri ve yargı mercileri için bu sistemlerini tasarlayan, geliştiren, test eden, bakımını yapan, dağıtan ve tedarik eden ekiplerin ayrımcılığı azaltmak için genel olarak toplumun çeşitliliğini, riskleri azaltmak için teknik olmayan bir araç olarak yansıtmalarının önemini vurgulamaktadır[257].

COMPAS gibi karar destek mekanizmalarının kullanımından doğan adil yargılanma çatısındaki sorunların başında ticari sır koruması nedeniyle sanığın, hatta görüş bildirecek savcı ve karar verecek hâkimin dahi denetleyemediği algoritmalara ilişkin silahların eşitliği meselesi gelmektir. Bu meselenin çözümüne yönelik olarak ise şeffaflık prensibinin hayata geçirilmesi gerekmektedir. Bu noktada ticari sır koruması ile bir denge kurulabilmesi adına sanık ve müdafinin algoritmaya ilişkin incelemelerini şirketin de gözetimde bulunabileceği, ortak ve yargı mercilerinin denetiminde korumalı sistemler üzerinden gerçekleştirebileceği, eksiklikleri olsa da bunun "algoritmik gizliliğe" yeğleneceği bir çözüm ileri sürülmektedir[258]. Ancak sanığın dezavantajlı konuma düşmemesini ifade eden silahların eşitliği kavramı etkin kullanılabildiğinde beklenen faydaları sağlayabilecektir. Bu bakımdan yapay zekâ sistemlerinin herhangi bir mülkiyet ve dolayısıyla erişim engeli olmadan birincil kullanıcıları, şüpheliler ve sanıklar ile genel halk tarafından anlaşılabilir ve incelenebilir olması gerekmektedir. Ayrıca sistemler, sanıkların kendilerine karşı verilen kararı anlamalarına ve itiraz etmelerine izin verecek şekilde anlaşılabilir tasarlanmalıdır[259]. Bu imkânlar risk puanlama metodolojisinin altında yatan kuralları inceleme hakkını da kapsayacak şekilde yorumlanmalıdır ve denetimli serbestlik prosedürlerinde hüküm giymiş bir kişinin,

[256] Fair Trials, s. 21-22.
[257] European Parliament, Artificial Intelligence In Criminal Law And Its Use By The Police And Judicial Authorities In Criminal Matters, 2021, para. 21. https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html, Erişim Tarihi: 08.10.2021.
[258] Villasenor/ Foggo, s. 343-347.
[259] Fair Trials, s. 26.

algoritmaya beslenen verilerden genel model tasarımına kadar uygulanan modellemeyi sorgulama olanağına sahip olmasını sağlamayı içermelidir[260].

Nitekim Avrupa Parlamentosu da yapay zekâ sistemlerinin eğitim verilerinin, bağlamının, amacının, doğruluğunun ve yan etkilerinin yanı sıra algoritmaların oluşturucuları ve geliştiricileri tarafından işlenmesinin ve temel haklara uygunluğunun tam dokümantasyonunu tutmanın öneminin altını çizerek bir yapay zekâ sisteminin hesaplamalarını insanların anlayabileceği bir forma indirmenin her zaman mümkün olması gerektiğini vurgulamaktadır [261].

Diğer taraftan böylesine önemli sonuçlara neden olan bir sistemin yalnızca muhataplarınca değil aynı zamanda kamusal denetiminin sağlanması da önem arz etmektedir. Avrupa Parlamentosu bu bağlamda da algoritmik sistemleri, bunların bağlamını, amacını, doğruluğunu, performansını ve bireylerin hayatlarını önemli ölçüde etkileme potansiyelinin bulunduğu durumlarda, kolluk kuvvetleri ve yargı tarafından kullanılan tüm yapay zekâ sistemlerinin bağımsız bir otorite tarafından periyodik olarak zorunlu denetlenmesi ve ceza adaleti alanında yapay zekanın gerekliliği ve orantılılığı hakkında tam olarak bilgilendirilmiş bir demokratik tartışmayı garanti etmek için uygun düzenleyici ve denetleyici gözetim dahil olmak üzere bu amaç için net bir kurumsal çerçeve çağrısında bulunmaktadır. Vatandaşların kullanılabilecek yapay zekâlı sistemleri ve bunların kullanımından doğabilecek herhangi bir temel hak ihlalini gidermek için hangi önlemlerin alındığını bilmeleri için bu denetimlerin sonuçlarının kamuya açık kayıtlarda bulunması gerektiğini ifade etmektedir[262].

Yapay zekâ sistemlerinin masumiyet karinesine saygı göstermesi bakımından, yargılamadan önce bir kişiyi suçlu olarak belirlemeyecek şekilde tasarlanması ve polisin makul şüphe olmaksızın bireylere karşı haksız, orantısız önlemler almasına izin vermemesi veya sistemlerin buna yardımcı olmaması önem arz etmektedir. Ceza adaleti sonuçlarını bildiren yapay zekâ sistemlerinin, kişi özgürlüğü ve güvenliği de göz önüne alınarak genel bir kural olarak, şüpheli ya da sanık lehine olan sonuçları tercih etmesi gerektiği önerilmektedir[263]. Bu yolla hâkimin tarafsızlığının etkilenmesinin de önüne geçilebilir ve bu araçlar iddia edildiği üzere haksız tutukluluk/denetim oranlarını düşürmek amacıyla etkili biçimde kullanılabilir.

Hâlihazırda çoğu AB ülkesi ve Türkiye'de de bulunan tutukluluk kararlarının yeterli gerekçeyi içermemesi sorunu yapay zekâ destekli araçların devreye girmesiyle kötüleşme riski taşımaktadır[264]. Bu kararlardaki gerekçe eksikliğinin kaynağı büyük ölçüde bireyselleştirme(me) olduğundan ve hakkın "önceden oluşturulan", "matbu" ifadelerle ihlal edildiği kabulü dikkate alındığında otomatik çıktıların buradaki sorunları derinleştireceğine ilişkin endişe de makul sayılabilir. Sistemlerin sanık dışındaki kişilere ilişkin geçmiş verilere

[260] Završnik, s. 14.
[261] European Parliament, para. 19.
[262] European Parliament, para. 21.
[263] Fair Trials, s. 14.
[264] Fair Trials, s. 27.

de dayanarak kişisel bir çıkarım yapamaması yöntemin bilimsel olarak isabetliliğine yönelik de önemli soru işaretleri doğurmaktadır. Bu açıdan hâkimin karar verirken yalnızca bu verileri dikkate almayarak hükmün bireyselleştirilmesine uygun ve sanığın durumunu gözetecek biçimde karar vermesi gerekmektedir[265].

Son olarak bu araçların ceza adaleti sistemindeki rolünün sınırlı olduğu gözetilmeli ve arzulanmayan sonuçlara neden olan sosyolojik, ekonomik, psikolojik vb. etkenlere daha fazla odaklanılmalıdır. Karar destekçisi risk değerlendirme araçları bakımından değerlendirilecek olursa mükerrer suç işleme riskini engellemenin hedeflerden yalnızca biri olduğu, geçmiş suç teşkil eden davranış için hesap verilebilirliği ve sonuç olarak adaletli bir yargı sürecini sağlamanın da eşit derecede önem arz ettiği göz ardı edilmemelidir. Cezaevinde olmanın çeşitli etkileriyle değerlendirildiğinde yeniden suç işleme riski olan kişiler için özgürlükten yoksun bırakmanın bu riski azaltması bir yana artmasına sebep olabileceği ve buna uygun alternatifler de düşünülmelidir[266]. Daha iyi algoritmalar oluşturmaya çalışarak problemleri dar bir çerçevede çözmeye çalışan indirgemeci bir yaklaşım yerine, sorunların çözümüne yönelik pratik katkılar daha önemlidir. Bir algoritma kişinin yargılama süresince mahkemeye gelip gelmeyeceğini öngörmekte başarılı olabilir ancak bunun nedenlerini araştırmak ve katılımı artıracak etkin müdahaleler tasarlamak ceza adalet sisteminin amaçları bakımından daha iyi sonuçlara yol açabilecektir[267].

Sonuç ve Değerlendirme

Risk değerlendirme araçları teknolojik gelişime paralel olarak yargı sistemlerine ve kolluk pratiklerine daha fazla dahil olmakta ve bu eğilimin yakın gelecekte de artarak devam edeceği anlaşılmaktadır. Bu araçların makine öğrenmesi ve yapay zekâ katkısıyla kullanıcılarının arzularına daha etkili çözümler sunduğu gözlemlenmektedir. Ancak kolaylaştırıcı görünümüne rağmen sistemlerin ceza adaletine etkileri yalnızca olumlu biçimde seyretmemektedir. Aksine bu uygulamalar birçok hukuki ve etik sorunu bünyelerinde barındırmaktadır. Her ne kadar gelinen aşamada geç bir sorgulama olarak görülebilirse de bu sistemlere ceza muhakemesinin çeşitli aşamalarında gerçekten ihtiyaç olup olmadığının etraflıca tartışılması hâlen önem arz etmektedir. Ceza muhakemesinin amaçları göz önüne alındığında bu araçların süreçlerde oynadığı sınırlı rol ve başarı sağlayıp sağlamadıkları noktasında tatmin edici sonuçların azlığı bu ihtiyaca dair soruların ve şüphelerin artmasına neden olmaktadır.

Öngörücü polislik uygulamalarının ceza muhakemesinin çeşitli kavramlarını bulanıklaştıracak ve başta özel hayatlarının gizliliğine yönelik müdahalede bulunan kişiler olmak üzere toplumun -genellikle sosyoekonomik açılardan dezavantajlı- bir bölümü üzerinde gözetimcilik yapacak denli yaygın ve hukuki güvencelerden yoksun kullanımı başka bir

[265] Abanoz-Öztürk, s. 95.
[266] Završnik, s. 5.
[267] Završnik, s. 9.

endişe kaynağıdır. Herhangi bir suç emaresinin bulunmadığı bir anda kişileri potansiyel suç failleri olarak izlemenin birçok farklı açıdan ayrımcılığı sürdürmesi ve bir kısır döngüye dönüşmesi mümkündür. Özellikle bu uygulamalar bakımından müdahalelere ilişkin çerçeveleri belirleyecek keskin hukuki düzenlemelerin yapılması gerektiği anlaşılmaktadır. Aksi takdirde ceza hukukunun yıllara ve önemli mücadelelere dayanan kazanımlarının "bilim ve teknoloji" etiketi altında örselenmesi oldukça kolaylaşacaktır.

Yargılamada kullanılan risk değerlendirme araçlarının adil yargılanma çerçevesinde birçok soruna yol açtığı henüz şimdiden anlaşılmaktadır. Bunların çalışma yöntemlerinin, çıktılarının denetlenememesi, karar vericiye yönelik kullanım mecburiyetinin otomasyon ön yargısı gibi sebeplerle onu psikolojik olarak da sonuca uyumlu davranmaya ittiği yönündeki tespitler göz önüne alındığında iddia ve savunma dengesinin önemli ölçüde bozulduğu gözlemlenmektedir. Keza geçmiş davranış kalıplarından hareketle kişinin henüz işlemediği fiillerden ötürü ve bir makinenin kendisi hakkındaki öngörüsüne dayanarak ceza hukuku müdahalesine maruz kalma riskinin artması ceza adalet sisteminin bireylere vereceği mesaj bakımından da tartışmalı görünmektedir. Bu noktada yargılamanın sanık açısından anlamlı olması için hâkim tarafından yapılacak bireyselleştirme daha da önem kazanmaktadır.

Şayet bu araçlar zorunlu olarak kullanılacaksa bağımsız denetimlerin sürdürülerek, kamusal tartışma ortamının yaratılması bu bağlamda ticari sır korumasının yerine sistemlerin şeffaf ve anlaşılabilir biçimde tarafların incelemesine sunulması gerekmektedir. Yine bu sistemlerin çıktılarını özgürlükten alıkoymayan çözümlere öncelemesi esas amaçlardan birisi haline gelmelidir.

Kaynakça

Abanoz-Öztürk, B., 2021, Ceza Muhakemesinde Sanığın Mükerrer Suç İşleme Riskinin Hesaplanması: COMPAS Algoritması ve Adil Yargılanma Hakkı, Yapay Zekanın Cezai Sorumluluğu, Adalet Yayınevi, s. 81-100.

Amnesty, 2018. Trapped In The Matrix, Secrecy, Stigma and Bias In The Met's Gangs Database. https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf, Erişim Tarihi: 24.07.2021.

Angwin, J. & Larson, J. & Mattu, S. & Kirchner, L. 2016. Machine Bias: There's Software Used Across the Country to Predict Future Criminals and It 's Biased Against Blacks, PROPUBLICA. https://www.propublica.org/article/machine-bias-risk-assessmentsin-criminal-sentencing, Erişim Tarihi: 20.07.2021.

Dieterich, W. & Mendoza, C. & Brennan, T. 2016. COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity, Northpointe. http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf, Erişim Tarihi: 22.07.2021.

Egbert, S. & Leese, M. 2021. Criminal Futures Predictive Policing and Everyday Police Work, New York, Rooutledge.

European Parliament 2021. Artificial Intelligence In Criminal Law And Its Use By The Police And Judicial Authorities In Criminal Matters. https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html, Erişim Tarihi: 08.10.2021.

Fair Trials, Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU Policy Paper**.** https://www.fairtrials.org/sites/default/files/Regulating%20Artificial%20Intelligence%20for%20Use%20in%20Criminal%20Justice%20Systems%20-%20Fair%20Trials.pdf, Erişim Tarihi: 18.10.2021.

Jansen, F. 2018. Data Driven Policing In The Context Of Europe. https://www.datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf, Erişim Tarihi: 01.10.2021.

Park, A. L. 2019. Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing. UCLA Law Review. https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/, Erişim Tarihi: 09.09.2021.

Seidensticker, K. & Bode, F. & Stoffel, F. (2018). Predictive Policing in Germany.

http://kops.uni-konstanz.de/bitstream/handle/123456789/43114/Seidensticker_2-14sbvox1ik0z06.pdf?isAllowed=y&sequence=5, Erişim Tarihi: 29.08.2021.

Stevenson, M. 2018. Assessing Risk Assessment in Action, Minnesota Law Review, Cilt:103, s.304-383.

The Metropolitan Police Service, MPS Gang Violence Matrix Frequently Asked Questions, https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence-matrix/, Erişim Tarihi: 23.07.2021.

Villasenor, J. & Foggo, V. 2020. Artificial Intelligence, Due Process and Criminal Sentencing, Michigan State Law Review, Sayı: 2, s.295-354.

Završnik, A. 2021. Algorithmic Justice: Algorithms and Big Data In Criminal Justice Settings, European Journal of Criminology**,** Cilt:18, Sayı:5, s.1-20.

Yapay Zekâ Kullanan Otonom Silah Sistemleri ve Savaş Suçları

Doktora Öğrencisi Ceren Özbek ve

Doktora Adayı Hilâl Nur Şarbak

Giriş

"Katil Robotlar" tabiri ilkin kulağa Ridley Scott'un 1979 tarihli kült bilim-kurgu filmi "Yaratık" (orijinal ismi ile *"Alien")* evrenine ait; gerçek dünyaya teşmil etmeyi düşünmenin dahi absürt olduğu bir kavram gibi gelebilir. Ancak, teknolojik gelişmelerin hayatın olağan akışını hızla değiştirdiği 21. yy. koşullarında, çok değil, yalnızca 40 sene önce sadece birer bilim-kurgu öğesi olarak hayal edilebilecek bilgisayar algoritmaları bugün üretimden lojistiğe, sağlıktan güvenlik sistemlerine kadar hayatın her alanında aktif biçimde kullanılmaktadır. Yapay zekâ (YZ) sistemlerinin günlük hayatın bütün yönlerine temas edecek biçimde yaygınlaşması, insanlığın kadim addedilebilecek faaliyetlerine ilişkin teknik bilgiyi hızla dönüştürmektedir. Bu anlamda, baştan aşağı dönüşüme uğrayacak alanlardan bir tanesi de silahlı çatışmalardır.

Dünyanın farklı yerlerinde devam eden silahlı çatışmalarda giderek artan biçimde kullanılan YZ ile bütünleşik askeri araçlar göstermektedir ki Türkiye'nin de içerisinde bulunduğu ve fakat başı özellikle Amerika Birleşik Devletleri (ABD) ve Çin'in çektiği bir grup devlet, YZ teknolojisi kullanan silahlı ve silahsız askeri donanımları hâlihazırda üretmekte ve geleceğe yönelik olarak da bu alanda araştırma-geliştirme çalışmaları için ciddi bütçeler ayırmaktadır[268] . Mevcut askeri konjonktürde, YZ'nin hâlihazırda kullanıldığı ve kullanım alanlarının bundan sonra da hızla genişleyeceği gözetildiğinde, YZ sistemlerinin silahlı çatışmalara dâhil edilmesi konusunda ne kinik olmak ne de buna tamamen karşı çıkmak gerçekçidir. Bu durumda esas odaklanılması gereken, YZ ile bütünleşik askeri araçların silahlı çatışmalar bakımından doğuracağı sonuçlara yönelik ihtiyatlı bir eleştirel bakış geliştirerek bunların hangi şartlar altında savaş hukukuna ve uluslararası insancıl hukuka uygun olarak kullanılabileceğini araştırmaktır.

[268] Çin hükümeti, 20 Haziran 2017'de yayınladığı raporda 2030'a kadar YZ alanında küresel öncü olmak yolundaki stratejik planını açıklamıştır. Raporun önemli bir kısmının YZ alanında asker-sivil entegrasyonun arttırılması hedefine ayrıldığı görülmektedir. Raporun İngilizce tercümesi için, bkz: (State Council of China, 2017); Benzer biçimde, Amerika Birleşik Devletleri de 2018 Ocak'ta yayınlanan Ulusal Savunma Stratejisi raporunda gelişmiş otonom sistemlerin askeri avantaj kazanmak bakımından kilit rolüne vurgu yaparak, otonomi, YZ'nin askeri uygulamasına önemli yatırımlar yapılacağını beyan etmiştir. Raporun tamamı için, bkz: Department of Defence Summary of the 2018 National Defense Strategy of United States of America, 14, 2018 https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, Erişim Tarihi: 26.12.2021

Bu bilgiler ışığında, bu çalışmanın amacı YZ'nin savaş suçları minvalinde ortaya çıkarabileceği temel hukuki meseleleri tartışmaktır. Bu bağlamda, çalışma üç temel kısımdan oluşmaktadır. Çalışmanın ilk kısmı, YZ sistemlerinin silahlı çatışmalarda kullanılmasının hangi hukuki sorunlara yol açabileceğini tespit edebilmek adına, YZ ve YZ'nin silahlı çatışmalar bağlamında tartışılmasının esas sebebi olan "otonom silah sistemleri" (OSS) kavramlarını açıklamaya ayrılmıştır. Çalışmanın ikinci kısmı, OSS aracılığı ile işlenebilecek savaş suçları kapsamında ortaya çıkabilecek sorumluluk hukuku problemlerine odaklanmaktadır. Çalışmanın üçüncü ve son kısmı ise, sorumluluk hukuku kapsamında çıkabilecek sorunlara ilişkin çözüm önerilerini incelemektedir.

1. YZ ve Otonom Silah Sistemlerinin Tanımlanması

YZ sistemlerinin silahlı çatışmalarda kullanılmasına ilişkin hukuki değerlendirmeye geçmeden önce, YZ ve OSS kavramlarını tanımlanmalıdır. Her iki tabir de ilk bakışta teknik ve açıklaması basit kavramlar gibi görünse de YZ ve OSS'yi kesin biçimde tanımlamak, bu teknolojilerin farklı seviyelerde "otonomi" ile çalışacak şekilde tasarlanabilir olması sebebiyle, kolay değildir. Zira, sistemlerin otonomi düzeyi farklılaştıkça, bunlar üzerindeki insan kontrolünün kademesi değişmekte; buna mukabilse, YZ ve OSS tarafından gerçekleştirilen (olası) hukuka aykırı davranışlardan "kimin" sorumlu olacağına ilişkin temel bir hukuki tartışma ortaya çıkmaktadır. İşte tam bu tartışma, bu çalışmada ele alınacak hukuki sorunların belkemiğini oluşturacaktır. Bu sebeple, YZ bağlamında otonomi ve OSS kavramlarına dair kapsamlı bir anlayışa sahip olabilmek bu çalışmanın amaçları bakımından elzemdir.

1.1. YZ Bağlamında Otonomi

Otonom kelimesi, Yunancada "öz" anlamına gelen "*autos*" ve "hukuk" anlamına gelen "*nomos*" kelimelerinden türetilmiştir. Kelimenin yalnızca kökeninden yola çıkıldığında, otonom bir varlığın, hukuk kurallarını kendisine icbar edebildiği; etme kapasitesini haiz olduğu söylenebilecektir[269]. Otonom kelimesinin basit semantik değerlendirilmesi ile bulunan bu anlam, otonomiyi "ahlak yasalarının rasyonel gereklerine uygun davranma" ile eş gören Kantçı bakış ile paraleldir[270]. Pratik akıl ve vicdana sahip olan insan, Kantçı bakış açısı ile yasalara uygun davranmak için aklı kullanacak; yani otonom biçimde hareket edecektir. Otonom biçimde hareket edebilen insan, eylemlerinin sorumluluğunu[271] üstlenme kapasitesini

[269]C. T. A. Schmidt &Felicitas Kraemer, Robots, Dennett and the Autonomous: A Terminological Investigation. Minds and Machines, 2006, 16(1), s.74.

[270]David J. Calverley, Imagining a Non-Biological Machine as a Legal Person. AI & SOCIETY, 2008, 16(1),s.532, . https://doi.org/10.1007/s00146-007-0092-7, Erişim Tarihi: 26.12.2021.

[271] Bu anlamda otonomi, cezai sorumluluk bakımından da kurucudur. Ceza hukuku bakımından, bir eylemin o eylemi gerçekleştirilen kişiye atfedilebilmesi için, eylemin kişi tarafından özgürce üstlenilmesi gerekir. Ceza hukukunda, eylemin sadece bir tesadüften ibaret olmadığı anlayışı esastır. Cezalandırma, kural olarak, ancak netice kast sonucu ortaya çıkmış ise gündeme gelebilecektir. Bkz: H. Roff, Killing in War: Responsibility,

de haizdir[272]. Başka bir ifadeyle, aydınlanmanın mirası ile şekillenen modern hukukta otonomi, birini eylemlerinden sorumlu tutabilmek (İng. *accountability*) için asli unsurdur[273].

YZ bakımından otonomi ise, münhasıran insana ait olduğu kabul edilen bu otonom bilinç düzeyine atıfla kullanılmamakta; teknik bir tabir olarak, insan kontrolü ve denetimi olmaksızın işlev göstermek üzere önceden programlanmış sistemleri ifade etmektedir[274]. Yani, YZ bağlamında "otonomi", makine sisteminin insan bir operatörden, programcıdan ya da sistemin eylemlerini herhangi başka bir biçimde kontrol edebilecek bir kullanıcıdan bağımsız hareket edebilme yetisi ile eşdeğerdir. İşte, YZ sistemlerinin kullanılması sonucunda ortaya çıkabilecek hukuka aykırılık hallerinde sorumluluk hukuku bakımından meseleyi sorunlu kılan tam da budur. YZ'nin eylemleri bir biçimde insan bir faile isnat edilebiliyorsa, yani YZ sistemi hala belirli bir seviyede insan operatörün kontrolünde ise, hukuken mutat olduğu üzere sorumluluk insan faile atfedilebilecektir[275]. Ancak, YZ'nin hareketi sonucu ortaya çıkan hukuka aykırılık ile insan bir fail arasında bağlantı kurulamadığında, bir sorumluluk boşluğu gündeme gelecektir[276]. Bu ikinci durumda bizzat YZ'nin bir ahlaki fail olarak kabul edilebileceği ve dolayısıyla sorumlu tutulabilirliği *de lege ferenda* bağlamında literatürde tartışılıyor olmakla birlikte[277], sorumluluk hukukunda *de lege lata* (felsefi anlamıyla) otonomi ile sorumluluk arasındaki bağıntı üzerine inşa edilmiş durumdadır. Dolayısıyla, mevcut hukuk insandan bağımsız hareket edebilen YZ sistemleri bakımından sorumluluğun tartışılabilmesi için gerekli araçlara sahip değildir. Bu sebeple, bu çalışma çerçevesinde de yalnızca *de lege lata* kapsamında YZ'nin bir hukuk kişiliğinin bulunmadığı kabulü ile sınırlı bir hukuki analiz yapılacaktır.

1.2. Otonom Silah Sistemleri (OSS)

"YZ bağlamında otonomi" kavramı tanımlandıktan sonra, OSS kavramını ve buna ilişkin tartışmaları anlamlandırmak bir nebze kolaylaşacaktır[278]. OSS'nin henüz üzerinde evrensel

---

Liability and Lethal Autonomous Robots, Routledge Handbook Of Ethics And War: Just War Theory In The 21st Century 14, (ed.) Fritz Allhoffvd, Routledge, 2013

[272]David J. Calverley, 2008. Imagining a Non-Biological Machine as a Legal Person. AI & SOCIETY, 22(4). https://doi.org/10.1007/s00146-007-0092-7, s.532., Erişim Tarihi: 26.12.2021.

[273]Christian Alwardt & Martin Krüger, Autonomy of Weapon Systems, Institute for Peace Research and Security Policy at theUniversity of Hamburg, 2009, s.1.

[274]John P. Sullins, When Is a Robot a Moral Agent? International Review of Information Ethics, 6(12), 2006, s.28.

[275]Joshua C. Gellers, Rights for Robots: Artificial Intelligence, Animal and Environmental Law (1. bs). Routledge, 2020, 142-143, https://doi.org/10.4324/9780429288159, Erişim Tarihi: 26.12.2021.

[276] M. Lotti, Killer Robots in the Battlefield and the Alleged Accountability Gap for War Crimes. Digital Watch, 2018, Nisan 17, https://dig.watch/resources/killer-robots-battlefield-and-alleged-accountability-gap-war-crimes, Erişim Tarihi: 26.12.2021.

[277]Daniel C. Dennett, "When Hal Kills, Who's to Blame? Computer Ethics." In Hal's Legacy: 2001's Computer as Dream and Reality, edited by D. Stork, 351-355 Cambridge, MA: The MIT Press, 1998, https://doi.org/10.7551/mitpress/3404.001.0001, Erişim Tarihi:26.12.2021.; Sullins, 2006; Calverley, 2008.

[278] Belirtmek gerekir ki, her OSS, YZ ile bütünleşik değildir. Örneğin, günümüzün silahlı çatışmalarında sıklıkla kullanılan insansız hava araçları gibi, önemli fonksiyonlarında otonomi kullanılan kimi askeri araçlar OSS olarak

konsensüs sağlanmış bir tanımı bulunmamaktadır. OSS'nin uluslararası hukukta düzenlenmesine ilişkin çalışmalar, 2013'ten bu yana "Aşırı Derecede Yaralayan ve Ayırım Gözetmeyen Etkileri Bulunan Belirli Konvansiyonel Silahların Kullanımının Yasaklanması veya Sınırlandırılması Sözleşmesi"[279] (BKSS) çerçevesinde devam etmektedir. 2016 yılında, BKSS kapsamında OSS[280] alanında ortaya çıkan yeni teknolojilerle ilgili sorunları değerlendirmek adına bir Hükümet Uzmanları Grubu (HUG; İng. *Group of Governmental Experts; "GGE"*) kurulmuştur. Geçtiğimiz beş yıl boyunca, düzenli olarak toplanmış olmasına rağmen HUG bünyesinde henüz bir OSS tanımı yapılamamıştır ve yeknesak bir tanım yapılmasının önündeki politik ve pratik engeller göz önünde bulundurulduğunda, yakın zamanda da yapılamayacak gibi görünmektedir[281].

OSS'nin tanımına ilişkin politik uyuşmazlık, Devletlerin yapılacak olan tanımın kapsamı üzerinde anlaşamamasından ileri gelmektedir. ABD'nin de içerisinde bulunduğu bir grup devlet; geniş bir tanımın sivil ve ekonomik amaçlar için geliştirilen YZ sistemlerindeki teknolojik gelişmeleri engelleyebileceği endişesiyle, OSS'nin dar tanımlanması gerektiğini savunmaktadır. Bu Devletlere göre, OSS yalnızca "tam" otonom, yani tamamen insan kontrolünden bağımsızlaşmış, silahları ifade etmektedir. Zira, OSS'nin silahlı çatışmalarda kullanılmasına ilişkin esas sorun, makine üzerinde insan operatörün kontrolünün tamamen ortadan kalması ve bunun yarattığı sorumluluk boşluğudur. "Tam" otonom silahlardan farklı olarak, yarı-otonom, yani üzerinde insan kontrolünün belli bir düzeyde devam ettiği, silahların kullanılması ise bu sorunu gündeme getirmemektedir. Dolayısıyla, bu Devletler BKSS çerçevesinde yapılacak düzenlemede yarı-otonom silahların OSS tanımının dışında bırakılması gerektiğini savunmaktadır[282].

---

sınıflandırılmakla birlikte, YZ ile değil; basit, kural tabanlı yazılımlar ile çalışmaktadır. Bkz: ("Artificial Intelligence and Machine Learning in Armed Conflict", 2020), s. 466

[279] 1980 tarihinde imzaya açılan ve 1983'te yürürlüğe giren BKSS'nin İngilizce dilindeki orijinal ismi *"Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects"*dir ve kısaca *"Certain Conventional Weapons"(CCW)* olarak anılmaktadır. Türkiye, BKSS'yi 1982 yılında imzalamış ve Sözleşme Türkiye bakımından 2005'te yürürlüğe girmiştir. (RG, No. 25690, 04.01.2005, 2004/8298)

[280] OSS, farklı uluslararası kuruluşlar ve Devletler tarafından farklı biçimlerde anılabilmektedir. Bunlardan en yaygın olanı "Ölümcül Otonom Silah Sistemleri" (ÖOSS); (İng. *Lethal Autonomous Weapons Systems, "LAWS"*) kavramıdır. BKSS çerçevesinde devam eden tartışmalarda ÖSSS kavramı kullanılmaya devam etse de bu çalışmada OSS tabiri tercih edilmiştir. Kanaatimizce, "ölümcül" ifadesi OSS'yi tanımlamak bakımından yanıltıcıdır. Zira, ölümcüllük bir silahın nasıl tasarlandığı ile değil, nasıl kullanıldığı ile ilgilidir. Ayrıca, OSS'yi ölümcül olarak betimlemek ölüm sonucunun gerçekleşmediği durumlarda da zararın ortaya çıkabileceği ihtimalini dışlayarak anlam daralmasına sebep olmaktadır. *Aynı yönde*, bkz: 20 Eylül 2020 tarihli, HUG toplantısında İsviçre, İrlanda ve Almanya'nın beyanları, UN Web Tv, 4th Meeting—1st Session Group of Governmental Experts on Lethal Autonomous Weapons Systems 2020, 22 Eylül 2020, https://media.un.org/en/asset/k1e/k1e117adw0, Erişim Tarihi: 26.12.2021.

[281]Austin Wyatt, So Just What Is a Killer Robot?: Detailing the Ongoing Debate around Defining Lethal Auton. Washington Headquarters Services, 2020, 20 Haziran, https://nsa-demo.dod.afpims.mil/News-Features/Stories/Article-View/Article/2210967/so-just-what-is-a-killer-robot-detailing-the-ongoing-debate-around-defining-let/, Erişim Tarihi :26.12.2021.

[282] Barbara Rosen Jacobson, Lethal Autonomous Weapons Systems: Mapping the GGE Debate. Diplo Foundation Policy Papers and Briefs, 8, 8, 2017, s.2.

Belirtmek gerekir ki, YZ ve buna bağlı olarak OSS'nin tanımına yönelik bu karmaşa, yalnızca global ölçekte, birbirinden farklı güvenlik ve ekonomi politikaları güden ve farklı öncelikleri olan Devletlerin ortak bir paydada buluşamamasından kaynaklanmaktadır. Bu teknolojilerin hem askeri hem de sivil amaçla daha geniş alanlarda kullanılmasının politik ve ekonomik sonuçları öylesine geniş bir yelpazede etki uyandırmaktadır ki teoride birbirleriyle uyumlu politikalar üretmek gayesinde olduğu varsayılan Avrupa Birliği (AB) ve Avrupa Konseyi (AK) Devletleri arasında dahi özellikle YZ'nin askeri amaçlarla kullanılmasına ilişkin net bir çerçeve henüz oluşturulamamıştır. 2021 yılının başında Avrupa Birliği Parlamentosu, YZ'nin askeri amaçlarla kullanılması konusunda bir düzenleme yapılması için Avrupa Birliği Komisyonu'na bir çağrıda bulunmuş ancak bu çağrının etkileri henüz Komisyon bünyesinde hayata geçmemiştir[283]. Yerel uluslararası örgütler bünyesinde de esas anlaşmazlık BKSS çerçevesindeki anlaşmazlıktan farklı değildir. "Tam" otonom olarak addedilen, insan kontrolünün tamamen devreden çıktığı silah sistemlerinin yasaklanması bakımından bir anlaşmazlık yoktur. Asıl anlaşmazlık, "yarı-otonom" silahların OSS tanımı içerisine alınıp alınmayacağından ileri gelmektedir[284].

Yarı-otonom silah sistemlerinin OSS tanımının dışında bırakılması yaklaşımı ilk kertede makul görülebilirse de YZ teknolojisinin son birkaç yıl içerisindeki gelişimi ve yakın gelecekte şüphesiz daha da hızla gelişeceği göz önünde bulundurulduğunda, oldukça sığ kalmaktadır. Zira, hayatın olağan akışı içerisinde, tam OSS bakımından dahi insan kontrolü, elbette, belirli bir biçimde devam edecektir. Bu silahların programlanmasına, çalışma prensiplerine ve askeri mevzilendirilmesine kuşkusuz, nihayet insanlar karar verecektir[285]. Ancak, insan kontrolünün teoride tesis edilebildiği kabul edilebilen durumlarda dahi belli insan-makine etkileşimi problemlerinden doğan hukuki sorunlar devam etmektedir[286]. Bu problemlerden başlıcaları, **otomasyon önyargısı** (İng. *automation bias*) olarak adlandırılan, insan operatörlerin otonom makinelerin doğru biçimde işleyeceğine—içgüdüleri aksini söylese dahi—kayıtsız şartsız güvenme temayülü[287]; **operatörün durumsal farkındalık**

[283]European Parliament Resolution of 20 January 2021 on Artificial Intelligence: Questions of Interpretation and Application of International Law in so Far as the EU Is Affected in the Areas of Civil and Military Uses and of State Authority Outside the Scope of Criminal Justice, 2021.

[284]Ulrike E. Franke, (2019). Not Smart Enough: The Poverty of European Military Thinking on Artificial Intelligence (ECFR/311). The European Council on Foreign Relations (ECFR), 2019, https://ecfr.eu/publication/not_smart_enough_poverty_european_military_thinking_artificial_intelligence/, Erişim Tarihi:26.12.2021.

[285]Robin, Geiß, The International Law Dimension of Autonomous Weapons Systems. Friedrich-Ebert-Stiftung, International Policy Analysis, 6, 2015, http://library.fes.de/pdf-files/id/ipa/11673.pdf, Erişim Tarihi:26.12.2021.

[286] The International Committee of the Red Cross, Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control, 2019, 9, https://www.icrc.org/en/document/autonomy-artificial-intelligence-and-robotics-technical-aspects-human-control , Erişim Tarihi: 26.12.2021.

[287] Kathleen L. Mosier, Linda J. Skitka, Susan Heers & Mark Burdick, Automation Bias: Decision Making and Performance in High-Tech Cockpits. The International Journal of Aviation Psychology, 1998, 8(1), 47-63, https://doi.org/10.1207/s15327108ijap0801_3, Erişim Tarihi:26.12.2021.; Linda J Skitka, Kathleen L. Mosier, Mark D. Burdick, Accountability and Automation Bias. International Journal of Human-Computer Studies,2000, 52(4), 701-717, https://doi.org/10.1006/ijhc.1999.0349, Erişim Tarihi:26.12.2021.; M.L. Cummings, Automation

eksikliği (İng. *lack of operator situational awareness*) olarak adlandırılan, insan operatörün farklı sebeplerle, OSS'ye müdahale etmek için yeterli zamana ya da kontrolü geri almak veya sistemi devre dışı bırakmak için müdahale edecek bir mekanizmaya (bir iletişim bağlantısı veya fiziksel kontrollere) sahip olamaması hali[288] ve **ahlaki bariyer** (İng. *moral buffer*) olarak adlandırılabilecek, insanın kendi eylemlerine etik olarak mesafelenmesine alan tanıyan psikolojik bir uzaklaşma şeması yaratması ihtimalidir[289]. İnsan-makine etkileşiminin karmaşık doğasından kaynaklanan bu üç durumda da insanın makine üzerinde kontrolü, kâğıt üzerinde devam ediyor olmakla birlikte, çalışmanın devamında daha detaylı üzerinde durulacağı üzere, bu durumların her biri ortaya çıkabilecek olası hukuka aykırı fiilin izlerini, insan operatöre kadar sürmeyi zorlaştırmakta ve bu da sorumluluk hukuku bakımından belirsizlik arz etmektedir[290].

OSS'yi "tam" veya "yarı" olarak sınıflandırmanın pratik yetersizliği karşısında, Uluslararası Kızılhaç Komitesi (İng. *International Committee of Red Cross; "ICRC*") OSS'yi "**önemli fonksiyonlarında otonomi sahibi olan**; yani, **insan müdahalesi olmaksızın** hedefleri **seçebilen** (arayabilen, tespit edebilen, tanımlayabilen veya takip edebilen) ve hedeflere **saldırabilen** kuvvet kullanabilen, etkisiz hale getirebilen, hasar verebilen veya yok edebilen) **silah sistemleri**"[291] olarak tanımlamıştır. ICRC'nin yaptığı bu görece geniş tanım, hem belli fonksiyonlarında otonomi kullanan her silah sisteminin hukuken sorunlu olmayabileceğini ortaya koyması[292] hem de—teknik ayrıntılarda kaybolmadan—bir silah sistemini OSS yapan esas unsurları insan kontrolü olmaksızın hedefi seçme ve hedefe saldırma olarak açıkça belirtmesi bakımından kullanışlıdır. Stockholm Uluslararası Barış Araştırmaları Enstitüsü (İng. *Stockholm International Peace Research Institute; "SIPRI"*) de, ICRC'nin tanımına benzer biçimde OSS'yi "bir kez etkinleştirildiği takdirde **insan müdahalesi olmaksızın**

Bias in Intelligent Time Critical Decision Support Systems. AIAA 1st Intelligent Systems Technical Conference. AIAA 1st Intelligent Systems Technical Conference, Chicago, Illinois., 20 Eylül 2004, https://doi.org/10.2514/6.2004-6313, Erişim Tarihi:26.12.2021.

[288] Durumsal farkındalık eksikliğinin sebeplerden bazıları stres, dikkat dağınıklığı gibi insan psikolojisine ilişkin olmakla birlikte; önemli bir kısmı, insanın fiziksel ve bilişsel sınırlarının makinelere kıyasla çok daha sınırlı olmasından kaynaklanmaktadır. Nitekim, OSS'nin nasıl işleyeceği konusunda çok iyi eğitilmiş bir kişi dahi makinenin çalışma hızına yetişememe ya da çalışma prensibi hakkında kolaylıkla yanılma riski ile karşı karşıyadır. Bkz: Vincent Boulanin, Neil Davison, Nettagoussac, Moa Peldán Carlsson, Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control, SIPRI (Stockholm International Peace Research Institute), 2020, s.53, 29, https://www.sipri.org/sites/default/files/2020-06/2006_limits_of_autonomy.pdf, Erişim Tarihi:26.12.2021.

[289] M.L. Cummings, Automation and Accountability in Decision Support System Interface Design The Journal of Technology Studies, 2006, 26, https://doi.org/10.21061/jots.v32i1.a.4, Erişim Tarihi: 26.12.2021.

[290]The International Committee of the Red Cross, Autonomy, ss. 9-10.

[291]The International Committee of the Red Cross, Autonomy, s.5. *(Tercüme yapılırken orijinal vurgular tekrarlanmıştır.)*

[292]Bu bakımdan, yalnızca gözetleme, seyir ve uçuş gibi "kontrol" fonksiyonlarında otonom olarak işlev gösteren ancak "hedefleme" fonksiyonlarının hâlâ insan eliyle manuel olarak gerçekleştirildiği askeri donanımlar ICRC'nin tanımı çerçevesinde OSS'nin doğurduğu hukuki sorunları gündeme getirmeyecektir. Geiß, s.7.

hedefleri **seçebilen**, **tanıyabilen** ve hedeflere karşı **kuvvet kullanabilen**"[293] sistemler olarak tanımlamıştır.

ICRC ve SIPRI tanımlarından farklı olarak İnsan Hakları İzleme Örgütü ise (İng. *Human Rights Watch, "HRW"*) OSS'yi üç aşamalı bir yaklaşım ile tanımlamaktadır. Buna göre, silah sistemlerinin yerine getireceği görevler üzerinde insan operatörün kontrolünün derecesine göre sistemler, insanın "döngünün parçası" olduğu; "döngüye dahil" olduğu ve "döngü dışı" olduğu[294] üç duruma göre sınıflandırmaktadır. HRW sınıflandırmasına göre insanın "döngünün parçası" olduğu silah sistemleri, hedefi belirleme ve vurma işlevlerinin münhasıran insan tarafından kontrol edildiği sistemlerdir[295] ve OSS kavramının dışındadır[296]. İnsanın "döngüye dahil" olduğu silah sistemleri, kural olarak, insan müdahalesi olmadan işlev gösterebilecektir. Ancak, bu sistemler üzerinde insan denetimi devam etmekte ve gerektiğinde insan operatör makinenin eylemlerini engelleyebilmektedir[297]. Nihayet, insanın "döngü dışı" olduğu sistemler ise, yukarıda anılan "tam" OSS tanımına benzer biçimde, hiçbir insan katkısı ve etkileşimi olmaksızın hedefleri seçebilen ve vurabilen silah sistemleridir[298]. HRW'nun üç aşamalı tanımında yalnızca insanın "döngüye dahil" ve "döngü dışı" olduğu silah sistemleri OSS tanımının içerisinde kabul edilmektedir[299].

HRW'nun literatürde de geniş biçimde benimsenen bu üç aşamalı yaklaşımı, ICRC ve SIPRI tanımlarına nazaran daha ayrıntılı gibi görünmekle birlikte, BKSS çerçevesinde yürütülen tartışmalarda olduğu gibi, bu yaklaşım da insan-makine etkileşiminden doğabilecek farklı ihtimalleri değerlendirmek bakımından yetersiz görünmektedir. Zira, insanın "döngünün parçası" olduğu sistemlerde dahi insan-makine etkileşiminden doğabilecek sorunlar ile karşılaşmak ihtimal dahilindedir. Bunun da ötesinde, yargısız, acele ve keyfi infazlar hakkında eski BM Özel Raportörü Heyns'in de 2013 raporunda belirttiği gibi, makinelerin karar alma mekanizmalarının kimi zaman nanosaniyeler içerisinde çalıştığı ve bu çalışma prensiplerinin her zaman insan operatörce denetlenemeyebileceği düşünüldüğünde, insanın "döngüye dahil"

---

[293] Vincent Boulanin, Laura Bruun, Netta Goussac, Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction (s. 72). SIPRI (Stockholm International Peace Research Institute), s.72, 2021, 2, https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf, Erişim Tarihi:26.12.2021. *(Vurgular yazarlar tarafından eklenmiştir.)*

[294]HRW'nun yayınladığı orijinal metinde bu kademelendirme için sırasıyla, "*human-**in**-theloop*"; "*human-**on**-the-loop*" ve "*human-**out-of**-the-loop*" terimleri kullanılmıştır. LosingHumanity: The Case Against Killer Robots, Human Rights Watch, 2012, 2, https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf, Erişim Tarihi:26.12.2021. *(Vurgular yazarlar tarafından eklenmiştir.)*

[295]A.e.

[296]Geiß, s. 7

[297]Losing Humanity, s. 2

[298]A.e.

[299]Alwardt&Krüger, s. 2

ve "döngü dışı" olduğu kabul edilen sistemler arasında pratik bir farklılık kalmamaktadır[300]. Bu durumda, bu iki kategoriyi birbirinden ayırmak hukuken anlamsızlaşmaktadır.

Bu anlatılanlar ışığında, ICRC ve SIPRI tarafından yapılan OSS tanımları, bir askeri donanımın ne zaman OSS olarak değerlendirilebileceği ve kullanılmasının hukuken hangi hallerde sorun teşkil edebileceği konusunda bağlama dayalı bir değerlendirme yapmaya daha elverişli görünmektedir. Silahın henüz üretim aşamasında teknik olarak nasıl tasarlandığından ziyade hangi görevleri gerçekleştirmek üzere ve nasıl kullanıldığına odaklanan bu tanımlar, özellikle insan-makine etkileşiminin karmaşık doğasından kaynaklanabilecek sorunlar konusunda, *ex ante* düzenleme yapabilmek ve nihayet, gerektiğinde, *ex post* değerlendirmelere olanak sağlamak bakımından daha kapsayıcıdır. Bu sebeple, bu çalışma bağlamında OSS'nin silahlı çatışmalarda kullanılmasına ilişkin yapılacak hukuki değerlendirmede, ICRC ve SIPRI tarafından yapılan tanımlar benimsenecektir.

2. OSS ve Savaş Suçları

OSS'nin yalnızca tanımından hareket ile, bu silahların silahlı çatışmalarda kullanılmasının doğurabileceği hukuki sorunlar hakkında genel bir fikre sahip olmak mümkündür. Bu sistemlerde kullanılan teknolojik donanımların otonomi seviyesine bağlı olarak karşılaşılabilecek (i) **sorumluluk boşluğu** ve karmaşık bilgisayar algoritmaları ve insan arasındaki etkileşimin öngörülemez doğasından kaynaklanan (ii) **hukuki belirsizlik,** OSS'nin silahlı çatışmalara dahil edilmesindeki temel iki temel sorunlu başlıktır. Çalışmanın bu kısmında, bu iki sorunlu başlık savaş suçlarından doğan sorumluluk özelinde incelenecektir. Bu bağlamda, çalışmanın sınırlarını çizebilmek adına, öncelikle savaş suçlarına ilişkin genel bir bilgi verilecek; daha sonra ise, OSS'nin silahlı çatışmalara dahil edilmesinin Devlet'in sorumluluğu ve bireylerin uluslararası ceza hukukundan doğan sorumluluğu bakımından doğurabileceği hukuki sorunlar ele alınacaktır[301].

2.1. Savaş Suçları

Uluslararası Ceza Divanı'nı kuran 17 Temmuz 1998 tarihli BM Uluslararası Ceza Divanı Roma Statüsü'nde (*buradan sonra:* "Roma Statüsü" veya "Statü") **soykırım**, **insanlığa karşı suçlar** ve **saldırı suçu** ile birlikte "uluslararası suçlar" kategorisi içerisinde sayılan "savaş suçları", kovuşturulması ve cezalandırılması bakımından Devletlerin ve bireylerin

[300]Christof Heyns, Report of the Special Rapporteur on Extrajudicial, Summaryor Arbitrary Executions (A/HRC/23/47), UN Human Rights Council, 2013, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/127/76/PDF/G1312776.pdf?OpenElement, Erişim Tarihi: 26.12.2021.

[301]OSS'nin silahlı çatışmalarda kullanılması bağlamında, Devletin ve bireyin ceza sorumluluğunun yanı sıra silah geliştiricisi/üreticisi şirketlerin sorumluluğu da söz konusu olabilecektir. Bu çalışmada, yalnızca anılan ilk iki sorumluluk tipi ile sınırlı bir değerlendirme yapılmıştır. Şirketlerin OSS bağlamında ortaya çıkabilecek sorumluluğuna ilişkin detaylı bir değerlendirme için, Bkz: R. G. Steinhardt, Weapons and the Human Rights Responsibilities of Multinational Corporations. İçinde S. Casey-Maslen (ed.), Weapons Under International Human Rights Law (ss. 507-541). Cambridge University Press. https://doi.org/10.1017/CBO9781139227148.023, 2014, Erişim Tarihi: 29.12.2021.

sorumluluğunun doğrudan uluslararası hukuktan ileri geldiği suç tiplerinin en klasik örneğidir. Savaş suçları, genel itibarıyla, uluslararası hukukun silahlı çatışmalarda uygulanacak kuralları olan "insancıl hukuk" kurallarının *ciddi ihlalleri* (İng. *"serious violations"*) sonucu oluşacaktır[302].Tek cümlelik bu genel tanım, elementlerine ayrıldığında, bir eylemin "savaş suçu" olarak nitelendirilebilir olup olmadığını tespit etmek için üç aşamalı bir değerlendirme yapılması gerektiği görülmektedir.

Her şeyden önce, insancıl hukuk kurallarının uygulama bulabilmesi için bir silahlı çatışmanın varlığı ön şarttır[303]. Dolayısıyla, bir eylemin "savaş suçu" olarak nitelendirilebilmesi için, ilk olarak, söz konusu eylem bir "silahlı çatışma" esnasında gerçekleşmiş olmalıdır[304]. Bir silahlı çatışmanın varlığı tespit edildikten sonra, ikinci aşamada eylemi insancıl hukukun "ciddi ihlali" olarak sınıflandıran bir "birincil kural" olup olmadığı araştırılacaktır[305]. Eylemi insancıl hukuk çerçevesinde ciddi ihlallerden biri olarak sınıflandıran bu "birincil" kural, antlaşmalardan ya da örf ve âdet hukukundan ileri gelebilecektir. Ancak, bir eylemin yalnızca insancıl hukukun ciddi ihlali olması da eylemi "savaş suçu" olarak tanımlamaya yeterli değildir. Zira, insancıl hukuk kurallarının asli muhatabı Devletler ve—belli koşullar altında—silahlı çatışmaya taraf olan Devlet dışı aktörlerdir ve bu kurallar, bir silahlı çatışma esnasında, çatışma taraflarının yapmaması gereken davranışları düzenlemektedir. Esasen, yalnızca ciddi ihlaller değil; bütün insancıl hukuk kurallarının ihlali kendi başına Devlet'in sorumluluğunu gündeme getirmek için yeterlidir[306]. Ancak, uluslararası ceza hukuku bakımından bir eylemi "savaş suçu" olarak tanımlamak ve dolayısıyla, bireylerin cezai sorumluluğunu tartışabilmek için insancıl hukukun ciddi ihlali olduğu tespit edilen eylemi, uluslararası hukuk çerçevesinde suç olarak düzenleyen "ikincil" bir kuralın varlığı aranacaktır [307].

Anlatılan bu üç aşamalı değerlendirmeyi sağlayarak bireysel cezai sorumluluk kapsamında savaş suçu teşkil eden insancıl hukuk ihlalleri, düzenlediği kaynağa göre, üç farklı grup halinde incelenebilecektir. Bunlardan ilki, genel antlaşmalar hukukundan ileri gelen savaş

---

[302] Eski Yugoslavya Uluslararası Ceza Mahkemesi, Tadić (Ara Temyiz), (IT-94-1-T), 17 Temmuz 1995, parag. 94.

[303]Kural olarak, uluslararası insancıl hukuk iç çatışmalarauygulanmayacaktır. Uluslararası hukuk bakımından bir "silahlı çatışma"nın hangi hallerde var olduğuna ilişkin kriterler hakkında detaylı bilgi için, bkz: Ricardo Garcia Vilanova, When does IHL apply? ICRC Blog, 13 Ağustos 2017, https://blogs.icrc.org/ilot/2017/08/13/when-does-ihl-apply/, Erişim Tarihi:26.12.2021.

[304] Savaş suçlarının teamülen yalnızca uluslararası nitelikteki silahlı çatışmalar esnasında işlenebileceği kabul edilmişse de bugün uluslararası nitelikte olmayan silahlı çatışmalardaki insancıl hukuk ihlallerinin de savaş suçu teşkil edebileceği kabul edilmektedir. Eski Yugoslavya Uluslararası Ceza Mahkemesi Statüsü, parag. 97; Roma Statüsü, madde 8(2)(c) ve (e)) Detaylı tartışma için ayrıca, bkz: La Haye, 2008, ss. 104-130.

[305] İnsancıl hukukun hangi ihlallerinin "ciddi" ihlaller olarak değerlendirileceğine ilişkin detaylı bilgi için, bkz: A. Schwarz, War Crimes. Max Planck Encyclopedias of International Law. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e431?rskey=1C6wQF&result=1&prd=MPIL#, 2014, Erişim Tarihi: 26.12.2021

[306] Bkz: aş. 2.3.

[307] A. Cassese, Cassese's International Criminal Law, (3. bs), Oxford University Press, 2013, ss. 65-70; Gerhard Werle, Florian Jeßberger, Principles of International Criminal Law (4. bs). Oxford University Press, 2020, 404, https://doi.org/10.1093/law/9780198826859.001.0001, Erişim Tarihi: 26.12.2021.

suçları, yani, Cenevre Sözleşmeleri ve Ek Protokollerinde düzenlenen insancıl hukukun "ağır ihlalleri" (İng. "*grave breaches*") rejimidir[308]. Cenevre Sözleşmeleri ve Sözleşmelere Ek Protokol (I)kapsamında, Sözleşmeler kapsamında korunan kişilere karşı işlenen kasten öldürme, işkence ve insanlık dışı muamele veya kasten gereksiz acılara sebep olma gibi suçlar, taraf Devletlerce cezalandırılması gereken "ağır ihlaller" olarak tespit edilmiş[309] ve savaş suçları olarak belirlenmiştir. İkinci grup, uluslararası ceza mahkemeleri tarafından suç haline getirilen insancıl hukuk ihlalleridir. Örneğin, Roma Statüsü m. 8(2) çerçevesinde, içerisinde Cenevre Sözleşmelerinin ağır ihlalleri hallerini de barındıran 51 adet tipik suç, mahkemenin yargı yetkisi kapsamındaki "savaş suçları" olarak tanımlanmıştır. Son grup ise, örf ve âdet hukuku bağlamında "savaş suçu" olarak tespit edilen, yani savaş suçları olarak kabul edilmeleri yönünde yaygın ve temsil edici Devlet uygulaması ve hukuk olduğu inancı *(opinio juris)* bulunan, insancıl hukuk ihlalleridir[310].

2.2. OSS ve Bireysel Cezai Sorumluluk

Ceza hukukunun evrensel prensipleri çerçevesinde uluslararası suçlardan dolayı kişisel ceza sorumluluğu, suçların şahsiliği ilkesine (İng. *"individual criminal responsibility"*)[311] dayanmaktadır. Buna göre, bireyin ceza hukuku sorumluluğundan bahsedebilmek için, failin eyleminin neticeye sebebiyet verdiğinin makul şüpheyi ortadan kaldıracak şekilde belirlenebilir olması gerektiği kabul edilmektedir.[312] OSS aracılığıyla bir savaş suçu işlenmesi halinde yapılacak sorumluluk değerlendirmesinde sorunlu olan kısım ise tam da budur. Bu bağlamda, sistemin insana ne ölçüde uyumlu tepki verdiği ve otonomi seviyesi, ceza hukuku sorumluluğunu belirleyecektir[313].

Bir suçu oluşturan iki ana unsur bulunmaktadır: maddi unsur (*actus reus*) ve manevi unsur (*mens rea*). Maddi unsur eylemin dışarıdan algılanma biçimini belirlerken, manevi unsur ise işlenen fiil sırasında kişinin zihnindeki hali ifade eder[314]. Kural olarak, fail yasaklanan

[308] Uluslararası insancıl hukuk kurallarının ağır ihlallerinin büyük bir kısmı 1949 Cenevre Sözleşmeleri ve Ek Protokol I çerçevesinde düzenlenmiş ve/veya kodifiye edilmiştir. Ağır ihlaller rejimi için, bkz: I. Cenevre Sözleşmesi, m. 49-50; II. Cenevre Sözleşmesi, m. 50-52; III. Cenevre Sözleşmesi, m. 129-131; IV. Cenevre Sözleşmesi, m. 146-148, Ek Protokol (I), m. 11 ve 85

[309] 4 Cenevre Sözleşmesi'ne, tüm Devletler taraftır ve bu sözleşmelerin, uluslararası örf ve âdet hukukunu yansıttığından şüphe yoktur. Ancak, ağır ihlaller tanımını genişleten Ek Protokol (I) için aynı tespiti yapmak mümkün değildir. Protokolün kimi maddelerinin hâlihazırda örf ve âdet hukukunu kodifiye ettiği kabul edilmekle birlikte,yalnızca ahdi yükümlükler doğuran hükümleri de bulunmaktadır. O'Connell, 2021, s. 37, para. 2.28

[310] Cassese, 2013, s. 68

[311] Roma Statüsü, m. 25

[312] Roma Statüsü, m. 66

[313] Marta Bo, Autonomous Weapons and the Responsibility Gap in light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute, Journal of International Criminal Justice 19/2, 2021, s. 25

[314] S. Casey-Maslen, Autonomous Weapons Systems and International Criminal Law, Bölüm 8, Drones and Other Unmanned Weapons Systems under International Law, Brill | Nijhoff, 2018, ss. 217-218

neticeyi gerçekleştirmiş olsa dahi buna kasten sebep olmadıkça—ve suç, istisnai olarak, kast olmaksızın da cezalandırılmıyorsa—cezai sorumluluk doğmayacaktır. OSS'nin insan müdahalesi olmadan alabileceği kararların öngörülemezliği, söz konusu hukuka aykırı neticeyi "kimin" gerçekleştirdiği ve hangi niyetle hareket edildiği hakkında varsayımsal bir çıkarım yapılmasını mecbur kılacaktır. Silahı kontrol eden kişi bakımından suçun manevi unsurunun, yani kastın varlığının, ortaya koyulamaması halinde OSS aracılığı ile işlenen suçlardan "kimin" sorumlu olacağı ceza hukuku çerçevesinde belirlenemeyebilecek[315]; bu durumda, OSS aracılığıyla işlenen suçlar cezasız kalabilecektir.

Yukarıdaki açıklamaya paralel olarak, Roma Statüsü m. 30 uyarınca da savaş suçlarının cezalandırılabilirliği bakımından kast esastır, yani bir fiilin savaş suçu teşkil edebilmesi için *bilerek* ve *istenerek* işlenmesi gereklidir. Kastın varlığının kanıtlanması için failin; (i) neticenin gerçekleşmesi için kasten hareket etmesi veya hareket etmemesi veya (ii) neticenin olayların olağan seyrinde gerçekleşeceğini bilmesi gereklidir[316]. Fletcher[317] tarafından yerinde bir şekilde ifade edildiği gibi failin riski öngörmesi ancak görmezden gelmesi halinde uluslararası ceza hukuku çerçevesinde *"öngörme ve kabul etme"* (Lt. *dolus eventualis*; İng. *recklessness*) söz konusu iken; failin olası riskler bakımından yeterince dikkatli davranmaması halinde *"özensiz davranışı"* (İng. *negligence*) söz konusudur[318]. Özensiz davranışta bulunulması Roma Statüsü de dahil olmak üzere uluslararası ceza hukuku çerçevesinde savaş suçlarının oluşumu için yeterli bir manevi unsur oluşturmamaktadır ve faile herhangi bir sorumluluk yüklenmesine izin vermemektedir. Bununla birlikte, önlem alma ve saldırının nesnesi hakkında gerekli bilgileri edinme görevinin yerine getirilmemesi kasıtlı bir ihmalden kaynaklanıyorsa, gerçek kişi operatör bu fiilden sorumlu tutulabilecektir. Ancak, OSS bakımından ortaya çıkması beklenen sorunlu durumlar genellikle kasten olmayan, hatalı tespit yapma, hedef alma veya ateş etme gibi riskleri barındıran eylemlerdir[319].

OSS aracılığı ile gerçekleşen netice bakımından herhangi bir suç işleme kastı bulunmaması halinde, OSS'yi kullanan kişilerin hataya düşmüş olabileceğinden bahsedilebilecektir. Örneğin, Roma Statüsü m. 8(2)(b) uyarınca, çatışmada doğrudan yer almayan sivillerin "kasten" hedef alınması, bir savaş suçu olarak kabul edilmiştir. Ancak, OSS'yi kullanan kişilerin, bilgisayar sisteminin hatalı şekilde hedefte bir düşmanın olduğunu göstermesi

---

[315] Mind the Gap: The Lack of Accountability for Killer Robots. (2015). Human Rights Watch. https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots, Erişim Tarihi: 26.12.2021.; Crootof, 2016, s. 1373; Cass, 2015, ss. 1049-1053

[316] Prosecutor v Katanga (UCM, II. Dava Dairesi, Dosya No ICC-01/04-01/07, 7 Mart 2014); İlgili karar çerçevesinde kabul edilen sorumluluk sadece OSS'yi kullanan operatör ve komutanın dışında üreticiler ve tedarikçileri de içine alan daha geniş bir sorumluluk alanı kabul edilebilecektir. Ancak bu çalışmanın kapsamında bu kişilerin sorumluluk alanlarına değinilmeyecektir.

[317] G. P. Fletcher, Rethinking Criminal Law, New York, Oxford University Press, 2000, s. 439 vd.

[318] Dikkat edilmelidir ki Türk ceza teorisi çerçevesinde ifade edilen ihmali hareket kasten ya da taksirle gerçekleştirilebilirken uluslararası ceza hukuku çerçevesinde ifade edilen ihmal (*negligence*) suçun manevi unsuruna ilişkin bir kavram olarak kabul edilmiştir. Uluslararası ceza hukuku sorumluluğun doğabilmesi için uluslar hukuk uyarınca en azından dolaylı kasta (*dolus eventualis*) denk gelen bir ağır kusur hali aranmaktadır.

[319] Bo, s. 17.

üzerine belli bir bölgede bulunan sivilleri hedef alması durumunda, "kast" değerlendirmesini yapmak mümkün olmayacaktır[320]. Nitekim, Statü'nün 32(1) maddesi de suçun maddi unsuruna ilişkin olarak kişinin açıkça hedefte hataya düşerek sivillere saldırması durumunda cezalandırılabilirliğin ortadan kalkacağını açıkça belirtmektedir[321]. Bu durumda sorumluk bağlantısını kurabilmek için kullanılabilecek bir diğer mevcut araç, silahlı çatışmalarda emir-komuta zinciri kapsamında doğan sorumluk olabilecektir.

2.2.1. Emir-Komuta Zinciri Kapsamında Doğan Sorumluluk *(Command Responsibility)*

Silahlı çatışmalar, kural olarak, askeri bir düzen içinde vücut bulmuş iki taraf arasında meydana geldiğinden emir komuta zincirinde gerçekleşir.[322] Roma Statüsü savaş suçlarından bireysel sorumluluğun yanı sıra, "komutanların ve diğer üstlerin sorumlulukları"nı da düzenlemektedir. Roma Statüsü'nün 28. Maddesi uyarınca kabul edilen komuta sorumluluğunun (İng. *command responsibility*) OSS'nin kullanımı bakımından uygulanabilecek bir sorumluluk rejimi olduğu tartışılabilecektir[323]. Komuta sorumluluğu, ast-üst ilişkisi içerisinde gerçekleştirilen eylemler sırasında komutana, astlarının herhangi bir savaş suçu işlemesini bilmeleri veya öngörmeleri halinde bunu engelleme ya da suçun işlenmesinden sonra ilgili astı cezalandırma sorumluluğu yüklemektedir[324].

OSS aracılığı ile gerçekleştirilen fiillerde amirin emri bakımından doğabilecek sorumluluk, ancak komutanın OSS'yi görevlendirmesi ve bu görevlendirmenin savaş suçu oluşturan bir saldırıya sebebiyet vermesi halinde doğacaktır. Komuta sorumluluğunun OSS bakımından kabulü varsayımında OSS'yi kullanan askerin savaş suçlarının işlenmekte veya işlenmek üzere olduğuna dair bilgisi varsa ve OSS üzerinde "*etkin komuta ve kontrol"*e[325] sahipse önleyici veya cezalandırıcı tedbirleri almadığı takdirde, kişisel olarak ceza sorumluluğu doğabilecektir[326]. Komuta sorumluluğunun bu takdirde OSS'nin kullanımı bakımından caydırıcılığı güçlendirmek ve cezasızlığı önlemek için bir araç olarak kullanılabileceği değerlendirilmelidir. Ancak komutanın OSS üzerindeki etkin komuta ve kontrolünün derecesi

---

320 A.e., s. 23 vd.

321 Ancak bu kişiler başka bir suçu planlayıp harekete geçtikten sonra beklenmedik şekilde başka bir suça sebebiyet verilmesi halinde sorumluluktan kaçamayacaklardır.

322 Komuta yetkisine sahip milli yetkililer, milli hedefler doğrultusunda harekatları icra etmelerini sağlamak maksadıyla, siyasi liderler, askeri planlayıcılar ve hukuk uzmanlarının formüle ettikleri ve askeri gücün ne şekilde kullanılabileceğini de içeren angajman kuralları askeri emir komuta zinciri şeklinde alt komutanlara aktarır. Ayrıntılı inceleme için bkz: (Lorenz, 1993), s. 29.

323 Bkz: Roff, 2013; C. Grut, The Challenge of Autonomous Lethal Robotics to International Humanitarian Law, Journal of Conflict & Security Law 2013(5)

324 T. Krupiy, Unravelling Power Dynamics in Organizations: An Accountability Framework For Crimes Triggered By Lethal Autonomous Weapons Systems, Loyola University Chicago International Law Review, 15(1), 2017, ss. 19-20

325 Roma Statüsü m. 28; Eski Yugoslavya Uluslararası Ceza Mahkemesi, Statü m. 7(2); Ruanda Uluslararası Ceza Mahkemesi, Statü m.6(2)

326Komutanın etkin kontrolünden ancak astının itaat etmesi gereken bağlayıcı emirler verebileceği hallerde bahsedilebileceği kabul edilmiştir: *Prosecutor v. Blaškić* (IT-95-14-A, Karar, f 69, 29 Temmuz 2004); Etkin komuta ve kontrol kavramının yaratıcı, tedarik eden ve kullanıcı bakımından hangi hallerde sorun yaratabileceğine ilişkin detaylı inceleme için, bkz: Krupiy, 2017, ss. 21-35

her sistem bakımından aynı olamayacağı için kontrol ve aşağıda değinilen sorunlu cezalandırma şartının OSS bakımından yeniden değerlendirilmesinin bir çözüm sunabileceği tartışmalıdır[327].

Emir komuta zincirinde ast-üst ilişkisinde, iki tarafın eylem bakımından iradesi ayrı şekilde değerlendirilmektedir. Bu bağlamda, eylemi gerçekleştiren astın, ne olursa olsun, kendi iradesi ile hareket ettiği kabul edilmekte ve ceza sorumluluğu bu eksende kurulmaktadır. Tam da bu sebeple, OSS ile onu kullanan insan arasında "emir komuta zincirindeki astlık-üstlük ilişkisi"ne benzer bir ilişki kurulması ilk kertede mümkün görünmekle beraber tartışmalıdır. Zira, ilgili sorumluluk rejiminde bahsi geçen asker ve komutanın, kural olarak, gerçek kişiler olduğu varsayılarak tasarlanmıştır[328]. OSS'nin otonomi seviyesi ne olursa olsun, mevcut konjonktürde, kendi iradesiyle hareket etmediği kabul edildiğinden; komuta sorumluluğunun yukarıda açıklanan şartlarının OSS bakımından kabulünün mümkün olmadığı söylenebilecektir[329].

2.3. OSS ve Devletin Savaş Suçlarından Sorumluluğu

Devletlerin savaş suçlarından doğan sorumluluğunun mahiyetine ilişkin tartışmalar uzunca bir süre uluslararası hukuk literatürünü meşgul etmiştir. Tartışmanın tamamına temas etmek, bu çalışmanın sınırları itibarıyla mümkün olmamakla birlikte[330], belirtmek gereken iki husus vardır. Bunlardan ilki, insancıl hukukun ihlallerinden doğan "ceza hukuku" sorumluluğunun yalnızca bireyler bakımından tartışılacak olmasıdır. Devletlerin uluslararası hukuktan doğan sorumluluğu yalnızca haksız fiil sorumluğu; yani hukuki sorumluluktur. Başka bir ifade ile, bir branş olarak uluslararası ceza hukuku, yalnızca bireylerin cezai sorumluluğu ile ilgilenmektedir[331]. Bu bağlamda, not edilmesi gereken ikinci önemli husus ise, Devletlerin savaş suçlarından sorumluluğunun, Devletlerin uluslararası haksız fiillerinden ileri gelen genel rejimin içerisinde, bireysel cezai sorumluluktan bağımsız bir kurum olmasıdır[332]. Bireyin savaş suçlarından sorumluluğu ile Devletin sorumluluğu—söz konusu bireyin

[327]İncelenen sorumluluk modelinin yaratıcılar ve tedarik edenlerin sorumluluğu çerçevesinde nasıl uyarlanabileceğine ilişkin bir analiz için, bkz: R. Buchan, N. Tsagourias, Autonomous Cyber Weapons and Command Responsibility, Autonomous Cyber Capabilities under International Law (ed. Rain Liivoja & Ann Väljataga), 2021

[328] Bu çerçevede uluslararası ceza hukuku ve Roma Statüsü kapsamında ancak gerçek kişilerin ceza hukuku soruşturulmasına ve yargılamasına tabi olabilecekleri vurgulanmıştır. Bkz: Smidt, 2000, s. 176

[329] J. S. V. Álvarez, Autonomous Weapons Systems: The Accountability Conundrum, <https://archivos.juridicas.unam.mx/www/bjv/libros/13/6467/7.pdf, 2021, Erişim Tarihi: 26.12.2021, s. 80

[330]Tartışmanın sebebi, Devletlerin "cezai" sorumluluğu olup olmayacağına ilişkin temel anlaşmazlıktan ileri gelmektedir. Tartışmanın kökenlerine ve gelişimine ilişkin detaylı bir inceleme için, bkz: Crawford, 2002, ss. 16-20

[331] van Sliedregt, 2012, ss. 5-7

[332] ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, para. 128

eylemleri Devlete atfedilebildiği ölçüde[333]—eşzamanlı olarak gündeme gelebilecek olsa da[334] Devletin sorumluluğu ne bireysel sorumluğa bağlıdır ne de bu iki tür sorumluluk türü birbirini dışlayacaktır. İki rejimin birbirinden bağımsız olarak var olduğu, Uluslararası Adalet Divanı (UAD) tarafından da *Soykırım* Davası'nda, "Devletin sorumluluğu ve bireysel ceza sorumluluk farklı hukuk rejimlerine tabidir ve farklı amaçlar güder. İlki, bir Devletin uluslararası hukuk tarafından kendisine yüklenen yükümlülüklerini ihlal etmesinin sonuçlarıyla ilgiliyken, ikincisi bir bireyin sorumluluğu [...] ve bunun sonucunda o kişiye uygulanacak yaptırımlarla ilgilidir"[335], denilerek açıklanmıştır[336]. Dolayısıyla, savaş suçu teşkil eden bir fiil ortaya çıktığında bireyin cezai sorumluluğunun yanı sıra, pekâlâ Devletin sorumluluğu da gündeme gelebilecektir.

Uluslararası hukukta Devletlerin haksız fiillerinden kaynaklanan sorumluluğu, Devlete atfedilebilen icrai veya ihmali bir eylemin (*subjektif unsur*); Devletin uluslararası hukuktan doğan bir sorumluluğunu ihlal etmesi (*objektif unsur*) ile doğacaktır[337].Başka bir ifade ile, Devletin uluslararası hukuktan doğan haksız fiil sorumluluğunun ortaya çıkması için Devletin "kusurunun" bulunması kurucu bir unsur değildir. Dolayısıyla, savaş suçları özelinde, teoride, savaş suçu teşkil eden ihlal Devlete atfedilebildiği her durumda Devletin haksız fiil sorumluluğu doğacaktır. Dahası, savaş suçları yasağı, uluslararası hukukun kendisinden sapma kabul edilmeyen *jus cogens* kuralları içerisinde yer almaktadır[338]. Bu sebeple, OSS aracılığı ile ihlal edilen tüm insancıl hukuk kuralları bakımından böyle bir analiz yapmak mümkün olmamakla birlikte, savaş suçları özelinde Devletin, kontrolü dışında gerçekleşen öngörülemez bir vaka sebebiyle sorumluluğunu yerine getiremediğini iddia edebileceği

---

[333] Devletlerin Uluslararası Haksız Fiillerinden Kaynaklanan Sorumluluğunu Düzenleyen Maddeler Metni (İng. *"Articles on Responsibility of States for Internationally Wrongful Acts"; ARSIWA*), Madde 2: Bir icrai ya da ihmali davranış: (a) uluslararası hukuka göre Devlete atfedilebiliyorsa; ve (b) Devletin uluslararası bir yükümlülüğünün ihlalini teşkil ediyorsa, Devletin uluslararası haksız fiili oluşacaktır.

[334] A. Nollkaemper, Concurrence between Individual Responsibility and State Responsibility in International Law. International and Comparative Law Quarterly, 52(3), ss. 615-640, 2003, https://doi.org/10.1093/iclq/52.3.615 , Erişim Tarihi: 29.12.2021.; A. Bianchi, State Responsibility and Criminal Liability of Individuals., (ed.) A. Cassese, The Oxford Companion to International Criminal Justice. Oxford University Press, 2009, ss. 16-24; B.I. Bonafè, Reassessing dual Responsibility for International Crimes. Seqüência: Estudos Jurídicos e Políticos, 37(73), ss. 19-36, 2016 https://doi.org/10.5007/2177-7055.2016v37n73p19 , Erişim Tarihi: 29.12.2021.

[335] ICJ, *Application of the Convention on the Preventionand Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, para. 182

[336] Devletlerin savaş suçlarından sorumluluğu, uluslararası hukukta Devletlerin*"ağırlaştırılmış sorumluluğu"* rejimi içerisinde değerlendirilecektir. Bkz: B. I. Bonafè, The Relationship between State and Individual Responsibility for International Crimes. Nijhoff, 2009; Devletlerin ağırlaştırılmış sorumluluğuna ilişkin ayrıntılı bir inceleme için ayrıca, bkz: C.Z. Pirim, Aggravated Responsibility Of States In International Law: A Theoretical Assessment. Public and Private International Law Bulletin, 32(2), ss. 147-182, 2012

[337] Devletlerin Uluslararası Haksız Fiillerinden Kaynaklanan Sorumluluğunu Düzenleyen Maddeler Metni, Madde 2

[338] Savaş suçlarına ilişkin yasağın *jus cogens* kurallar içerisinde yer aldığını gösteren detaylı bir inceleme için, bkz: T. Weatherall, Jus Cogens: International Law and Social Contract. Cambridge University Press, 2015, https://doi.org/10.1017/CBO9781139976664, ss. 213-219, Erişim Tarihi: 29.12.2021.

"mücbir sebep" (*force majeure*)[339] defisi de kullanılamayacaktır[340]. İnsan-makine etkileşiminin doğasından ileri gelen "öngörülemezlik" sebebi ile dahi olsa, OSS'nin bir savaş suçu teşkil edecek biçimde—örneğin, doğrudan sivilleri hedef alarak—kullanılması durumunda bir *jus cogens* norm ihlal edildiği için, Devletlerin Uluslararası Haksız Fiillerinden Kaynaklanan Sorumluluğunu Düzenleyen Maddeler Metni'nin 26. maddesi uyarınca[341] bu "öngörülemezlik" hukuka aykırılığı ortadan kaldıran bir mücbir sebep olarak ileri sürülemeyecek[342]; Devlet sorumluluktan kaçamayacaktır.

Tam da bu sebeplerle hem literatürde hem de BKSS çerçevesinde HUG tarafından yürütülen çalışmalarda, OSS'nin kullanılması sonucu ortaya çıkabilecek insancıl hukuk ihlalleri bakımından Devletlerin sorumluluğunun, bireyin cezai sorumluluğunda olduğu gibi, sorunlu olmadığı düşünülmüş ve uzun uzadıya tartışılmamıştır. HRW, 2015 yılında yayınladığı raporda, açıkça, OSS'nin kullanılması sonucu ortaya çıkabilecek hukuka aykırılıkların "kolaylıkla" kullanıcı Devlete atfedilebileceğini belirtmektedir[343]. HUG ise, 2019 yılında yayınladığı "rehber ilkeler"[344] çerçevesinde, insancıl hukukun OSS de dahil bütün silah sistemlerinin geliştirilmesine ve kullanılmasına uygulanacağını belirtmiş[345]ve Devletlerin, OSS'nin geliştirilmesi, edinilmesi ve nihayet kullanılması bakımından uluslararası yükümlülüklerine uygun davranma yükümlülüğü altında olduğunu vurgulamıştır[346]. Ancak, bu jenerik kabullerin ötesinde OSS'nin silahlı çatışmalarda kullanılmasının Devletlerin sorumluluğu bakımından doğuracağı sonuçlara HUG da özellikle değinmemiştir.

Bununla birlikte, OSS'nin Devletin savaş suçlarından sorumluluğunu sorunlu kılmadığı yönünde yapılan değerlendirme, aslında sığ bir çözümlemedir. Zira, kural olarak Devletin haksız fiil sorumluluğunun doğabilmesi için, bireysel cezai sorumlukta olduğu gibi, "kast" aranmayacak olsa da Devletin insancıl hukuk bakımından üstlendiği sorumluluğun kendisi, yani sorumluluğun *objektif* unsuru, belirli bir manevi unsuru barındırıyor olabilir. Söz gelimi, yukarıda da değinildiği üzere, ihlal edildiği takdirde savaş suçu teşkil edecek olan, bir silahlı çatışmada bireylerin doğrudan hedef alınması fiili[347], kendi içerisinde "hedef alma" halini,

---

[339] Devletlerin Uluslararası Haksız Fiillerinden Kaynaklanan Sorumluluğunu Düzenleyen Maddeler Metni, Madde 23

[340] İnsancıl hukukun savaş suçu teşkil etmeyen diğer ihlalleri bakımından bir değerlendirme için bkz: Boulanin vd., 2021, s. 42

[341] Devletlerin Uluslararası Haksız Fiillerinden Kaynaklanan Sorumluluğunu Düzenleyen Maddeler Metni, Madde 26: "Bu bölümde yer alan hiçbir durum, bir Devletin, uluslararası hukukun emredici bir normundan doğan bir yükümlülüğe uygun olmayan herhangi bir fiilinin haksızlığını engellemez." *(Tercüme yazarlara aittir.)*

[342] Amoroso, 2020, s. 147

[343] *Mind the Gap*, 2015, s. 13

[344] Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (CCW/GGE.1/2019/3) (2019). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/285/69/PDF/G1928569.pdf?OpenElement, ErişimTarihi: 26.12.2021.

[345] Rehber İlke #1

[346] Rehber İlke #5

[347]Ayrım gözetme ilkesine ilişkin ayrıntılı bilgi için, bkz: Rule 11. Indiscriminate Attacks, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule11 , Erişim Tarihi: 15.10.2021.

yani, saldırının sivillere—belli bir seviyede—*bilerek* yönetilmiş olmasını aramaktadır[348]. Benzer biçimde, bir saldırının edinilmek istenen askeri avantaj ile "orantılı" olmasını emreden [349] ve yine ihlal edildiği takdirde savaş suçu teşkil edecek orantılılık ilkesi, saldırı ile elde edinilmek istenen askeri avantajın Devlet ajanlarınca muhakeme edilmesini aramakta, dolayısıyla gerçekleşen saldırının orantılı olmadığına ilişkin bir ön bilincin varlığını —belli bir seviyede—gerektirmektedir[350].

Her iki örnekten de anlaşılabileceği gibi, insancıl hukukun OSS aracılığı ile ihlal edildiği bu hallerde Devletin daha ilk kertede objektif yükümlülüğünü ihlal etmediği ileri sürülebilecek; bu durumda mücbir sebep defisine dahi zaten ihtiyaç olmaksızın, Devlet sorumluluktan kurtulabilecektir. Dolayısıyla, OSS aracılığı ile gerçekleşecek savaş suçları bakımından Devletin sorumluluğunu tesis edebilmeyi güvence altına alabilmek için, OSS ve Devletin sorumluluğu bakımından da—tıpkı bireysel cezai sorumlukta olduğu gibi—özel düzenlemelerin yapılması gerektiği anlaşılmaktadır.

3. *De Lege Ferenda:* Önerilen Sorumluluk Modelleri

OSS'nin silahlı çatışmalarda kullanması, her durumda değilse bile, çalışmanın önceki bölümlerinde tartışılan belli koşullarda sorumluluk hukuku bakımından bir boşluk yaratabilecektir. Bunun engellenebilmesi amacıyla, uluslararası hukuk ya OSS'ye özgü bir savaş suçu tipi formüle ederek ya da "OSS-dostu" bir sorumluluk hali kabul ederek, operasyonel gerçekleri ve makine-insan etkileşimini göz önünde bulunduran yeni hukuki düzenlemelere yer açmalıdır. Bu, mevcut yasal çerçevenin araçları kullanılarak iki şekilde gerçekleşebilir: (i) mevcut düzenlemelerin, uygun olduğu ölçüde, analoji yoluyla OSS'ye uygulanması; (ii) OSS'ye has yeni düzenlemeler yapılması. Çalışmanın bu kısmında, sorumluluk boşluğunun çözümlenebilmesi için literatürde önerilen sorumluluk modelleri açıklanacak ve bu modellerin sorumluluk boşluğuna ne şekilde hizmet edebileceği değerlendirilecektir.

3.1. Dolaylı Faillik Kapsamında Doğan Sorumluluk

Bazı hukuk sistemlerinde[351] çocuk ya da akıl hastası gibi kusur yeteneğinden yoksun kişilerin suç işlemesi ya da bu kişilere suç işletilmesi durumlarında da *"dolaylı faillik"* (İng. "*the perpetrator-by-another*")[352] kurumu kabul edilmiştir[353]. Bu hallerde kusur yeteneğinden

[348]Amoroso, 2020, s. 147

[349] Orantılılık ilkesine ilişkin ayrıntılı bilgi için, bkz: Rule 14. Proportionality in Attack, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14, Erişim Tarihi: 15.10.2021.

[350]Amoroso, 2020, s. 148

[351]Detaylı bir inceleme için, bkz: Fletcher, 2000, s. 581 vd.

[352] Dikkat edilmelidir ki TCK m.37(2) kapsamında bir kişinin bir suçun işlenmesinde araç olarak kullanılması sadece kusur yeteneğinden yoksun kişiler bakımından kabul edilmemektedir. Ancak kusur yeteneği olmayan araç kişiye suç işletilmesi hali cezayı ağırlaştıran bir nitelikli hal olarak düzenlenmiştir. Kaldı ki TCK'nın lafzından anlaşıldığı üzere her kim bir başkasını (gerçek kişiyi) suç işlemede araç olarak kullanırsa dolaylı faillik kurumundan bahsedilebilecektir, aksi haller doğrudan faillik olarak değerlendirilmelidir.

[353] G. Hallevy, The Criminal Liability of Artificial Intelligence Entities—From Science Fiction to Legal Social Control. Akron Intellectual Property Journal, 4(2), ss. 171-199, 2016, s.179.

yoksun kişiyi yasaklanan neticeye yönlendiren failin cezalandırılması söz konusu olacaktır. Bu bağlamda, OSS ahlaki muhakeme yapma ve kusur yeteneğinden yoksun bir çocuk askere benzetilecek olursa, bu sorumluluk modelinin uyarlanarak OSS aracılığı ile işlenen filler bakımından kabul edilebileceği tartışılmaktadır.

Roma Statüsü m. 26 savaş suçlarına karışan 18 yaşının altındaki kişilerin yargılamaya tabi olmayacağını düzenlemiştir. Bu çerçevede, mevcut düzenlemenin OSS'ye uyarlanması önerilen sorumluluk modeline uygun bir zemin hazırladığı iddia edilebilecek olsa da bu iki farklı durumu birbirine eşitlemenin bazı sakıncaları da bulunmaktadır. Öncelikle, Roma Statüsü'ndeki çocuk askerlere ilişkin bu hüküm, silahlı çatışmalarda çocuk asker kullanılmasının engellenmesi ve çocukların korunmasına yöneliktir[354]. Dolayısıyla, mevcut düzenlemenin konu ve amacı, OSS'ye ilişkin çekincelerden tamamen farklıdır. İkinci olarak, OSS ile bütünleşik bir YZ sisteminin, "yarı masum" yani en azından kendi kendine öğrenebilen ve karar alabilen bir araç olarak değerlendirilmesi halinde, belli bir dereceye kadar özerk hareket edebileceği düşünülebilir. Ancak, bunun aksine, bir çocuğun sadece verilen komut doğrultusunda; herhangi başka bir muhakeme yapmadan ve suç işleme kastı olmadan hareket ettiği kabul edilir. Nitekim, bir çocuğu ya da kusur yeteneği olmayan bir kişiyi yönlendiren kişilerin ceza sorumluluğu gündeme getiren de budur[355]. OSS bakımındansa, sistemin otonomi seviyesinden bağımsız olarak, gerçekleştirilen fiil ile netice arasındaki nedensellik bağlantısı doğrudan onu kullanan kişinin hareketine atfedilemeyebilecektir ve halen bu kişilerin suç işleme kastının tespit edilemediği haller olabilecektir. İlgili model bu nedenselliğin tespiti bakımından bir çözüm önerisi getirmekle birlikte, OSS'yi kontrol eden kişinin her durum bakımından suç işleme kastı ispatlanamayacağı için yine yetersiz kalacaktır[356].

3.2. Olası Doğal Sonuç *(Natural Probable Consequence Liability*) Modeli

OSS'nin yaratıcıları ve/veya kullanıcıları OSS'nin işleyişine, genel kullanımına ve dağıtımına katkı sağlayacaklardır. Ancak, OSS aracılığıyla herhangi bir suç işlemeye niyetli olmadıkları göz önünde bulundurularak, bu kişilerin istenmeyen netice ortaya çıkana kadar suç işlendiğinden haberi olmayacaktır. Olası doğal sonuç modeline göre, bir kişinin davranışının doğal ve olası bir sonucu olduğu ölçüde, yani, ilk aşamada OSS'nin oluşturulması, kullanılması veya yetkilendirilmesi gibi fiiller sorumluluğun doğması için yeterli olacaktır. Geniş anlamda bu yaklaşım, suçun manevi unsuru çerçevesinde öngörülebilirlik veya dikkat

[354] R. Sparrow, Killer Robots, Journal of Applied Philosophy, 24, ss. 62-79, 2000, s. 73.

[355] Buna karşı çıkan bir görüşe göre çocuk askeri yönlendiren kişi gerçekleşen fiilden değil ancak bu kişilerin savaş alanlarında görevlendirilmesinden dolayı sorumlu tutulabileceğini savunulmaktadır. H. Liu, Refining Responsibility: Differentiating Two Types of Responsibility Issues Raised by Autonomous Weapons Systems, (ed.) Nehal Bhuta vd., Autonomous Weapons Systems: Law, Ethics, Policy, Cambridge University Press, 2016, s. 343.

[356] Álvarez, 2021, s. 93; G. R. Cross, C. G. Debessonet, An Artificial Intelligence Application in the Law: CCLIPS, A Computer Program that Processes Legal Information, HIGH TECH. Law Journal 1, ss. 329-336, s. 329.

ve özen yükümlülüğü bakımından bir değerlendirmeyi gerektirir. OSS'nin tasarlanması ve kullanımı esnasında herhangi bir riskin öngörülmesine rağmen görmezden gelinmesi ya da özensizlik hali ilgili model çerçevesinde doğrudan bireysel ceza sorumluluğun doğmasına sebebiyet verecektir[357]. Dikkat edilecek olursa, olası doğal sonuç modeli işlenen suçun manevi unsurunun tespitinde farklılık getirerek alternatif bir sorumluluk rejimi sunmaktadır. Diğer bir deyişle, OSS'nin bu araçları kullanan bakımından getirdiği avantajlar da göz önüne alındığında, uluslararası ceza hukuku çerçevesinde artık bilinçli taksire yakın bir ceza sorumluluğundan bahsedilebileceği düşünülmelidir.

Model, makul bir yaratıcının, tedarik edenin veya kullanıcının, suçun işlenebileceğini öngörmüş olabileceği ve/veya neticeyi engelleme fırsatına sahip olabileceği düşüncesine dayanmaktadır[358]. Bu bakımdan OSS'nin hedef aldığı kişi veya kişileri tespit ederken "hatalı pozitif" veya "hatalı negatif" seçimlerde bulunma oranının ayarlanmasında hata payının ne yönde kullanılacağı önem kazanmaktadır. Örneğin, çok acil terör saldırılarını bertaraf etmek üzere OSS'nin devreye girdiği varsayıldığında, hatalı pozitif, masum birinin hayatını kaybetmesi anlamına gelirken hatalı negatif ise terör saldırısının gerçekleşmesi ve birçok sivilin hayatını kaybetmesine sebebiyet verebilecektir. Ancak hedef hatalı negatiflerin engellenmesi olsa da hatalı pozitifin "doğal bir sonuç" olarak kabullenildiği varsayılabilir. Böylelikle bu sorumluluk modelinde, OSS'nin üretim ve kullanım aşamalarına dahil olan kişilerin sorumluluk alanı genişleyecek; buna mukabil, bu kişiler sistemi daha özenli tasarlamaya; kullanmaya teşvik edilebilecektir.

Bu anlatılanların ışığında, olası doğal sonuç modeli de ceza hukuku bakımından sorunsuz değildir. Model, bir kimsenin, fiili gerçekleştirdiği sıradaki neticeye yönelik niyetinin ötesindeki neticelerden de sorumlu tutulmasını öngörerek; sorumluluğun olması gerekenden daha fazla genişlemesine sebep olabilecektir[359]. Alternatif olarak uluslararası ceza hukuku bakımından ise bu durumun Anglosakson hukukunda bulunan "*due diligence*" (dikkat ve özen yükümlülüğü) defisi ile komuta sorumluluğunun bir kombinasyonu ile çözümlenmesi önerilebilecektir[360]. Ancak, OSS bakımından mevcut düzenlemelerin uyarlanması ile sorumluluk hukukundan doğan sorunlara her zaman yeterli ve etkili çözümler getirilemeyeceği anlaşılmaktadır. Bu şartlar altında, OSS'nin getirdiği sorunlar gözetilerek ve uluslararası ceza hukukunun ilkeleri ve ihtiyaçlarına uygun yeni bir sorumluluk rejimini tartışmak en makul çözüm gibi görünmektedir.

---

[357] Hallevy, 2016, s. 183
[358] Álvarez, 2021, s. 97
[359] **A.e.**
[360] İnsan hakları hukuku bağlamında *due diligence* definin değerlendirilmesine ilişkin detaylı inceleme için, Bkz: Sherman & Lehr, 2010

3.3. OSS Odaklı Bir Uluslararası Ceza Hukuku Sistemi

Çalışmanın önceki kısımlarında bahsedilen hukuki sorunların bertaraf edilebilmesi için OSS'nin silahlı çatışmalarda hangi şartlar altında kullanılabileceğinin özel olarak düzenlemesi gerektiği literatürde uzun süredir tartışılmaktadır. Bu çerçevede, kullanıcı bakımından bir sorumluluğun doğabilmesi için, kullanıcıya OSS aracılığı ile gerçekleşen fiil bakımından, mutlak bir karar alma yetkisinin tanınmış olması gerektiği ileri sürülmüştür.[361] Bu öneri, yukarıda bahsedilen "olası doğal sonuç" rejimine yaklaşsa da OSS'nin üretim ve tedarik aşamalarından öte; kullanılması bakımından yetkiyi elinde bulundurmayı esas almalıdır. Burada yetkinin çerçevesi bakımından belirleyici kriterin, OSS'yi kullanan askerin saldırıyı başlattığı ve bu çerçevede askerin OSS'yi ilgili saldırı bakımından görevlendirdiği an olması gerektiği kabulü önerilmiştir[362]. Bu da zorunlu olarak OSS'nin kontrolden çıkması riskini göz önünde bulundurularak; çalışma prensiplerinden emin olunarak kullanımının yaygınlaşmasına yol açacak ve böylelikle de beklenmedik neticelerin doğmasına engel olunacaktır.

Aynı doğrultuda, uluslararası hukuk çerçevesinde, silahlı çatışmalarda gerçekleşen her saldırı üzerinde **"anlamlı/kayda değer insan kontrolü"** (İng. *"meaningful human control"*) bulunması gerektiği kabul edilmiştir.[363] OSS üzerindeki insan kontrolünün ne zaman anlamlı olacağı bakımından üç aşamalı değerlendirme yapılmıştır. İlk olarak OSS kullanıldığı silahlı çatışmalarda adil savaş ilkelerine ve Uluslararası İnsancıl Hukuka uyma yükümlülüğü çerçevesinde gerçek kişi kullanıcılar **"arıza emniyeti rolünü"** oynamalıdır. Silahı kullanan askerin, arızalı ya da hatalı OSS'nin tespit edilmesi halinde doğrudan saldırılarda bulunmasını önlemesi gerekir. İkinci olarak, gelecekte uluslararası ceza hukuk çerçevesinde düzenlenecek olan OSS'nin fiillerinden doğacak cezai sorumluluğun çerçevesi çizilirken OSS'nin tasarlanması, üretimi, kullanımı ve tedariki bakımından anlamlı insan kontrolü kavramının ne anlama geleceği detaylıca açıklanmalıdır. Böylelikle bu kavramın "hesap verilebilirlik sibobu" olarak çalışması sağlanarak OSS'nin uluslararası hukuku ihlal eden bir fiil gerçekleştirmesi halinde bireysel cezai sorumluluk bakımından yasal koşullar güvence altına alınmış olacaktır[364]. Üçüncüsü, OSS üzerindeki insan denetimini insan onuruna saygının bir gerekliliği olduğunun altı çizilmelidir. Burada insan kontrolü "ahlaki bir fail" olarak işlev görür ve YZ tarafından silahlı çatışmalara katılan kişilerin beden bütünlüğü ve mülkiyet

[361] Krupiy, 2017, s. 61; Liu, 2016, s. 344

[362] Álvarez, 2021, s.100

[363] "Killer Robots: UK Government Policy on Fully Autonomous Weapons" 2013., https://article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf , Erişim Tarihi: 13.10.2021.; The Convention on Certain Conventional Weapons (CCW), Informal Meeting of Experts on Lethal Autonomous Weapons Systems (Ölümcül Otonom Silahlalar Hakkında Resmi Olmayan Uzman Toplantısı) 2014., UABD Delegasyonunun kapanış bildirisi, http://www.unog.ch/80256EDD006B8954/%28httpAssets%29/6D6B35C716AD388CC1257CEE004871E3/$file/1019.MP3, Erişim Tarihi: 18.10.2021.

[364] T. Chengeta, Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law, Denver Journal of International Law and Policy, 45/1 (3), 2020

hakkını etkileyen kararların alınmaması sağlanır[365]. Etik ve yasal olarak sağlam bir mekanizma kurulabilmesi için OSS'nin ödevleri ve yükümlülüklerini belirlemeye yönelik kuralların yukarıda bahsi geçen üç prensip ile beraber ve değişmez şekilde yerine getirileceği garanti edilmelidir[366].

Sonuç

YZ sistemleri ile geliştirilen silah sistemlerinin silahlı çatışmalarda kullanılması kimi çevrelerce hâlen "Yaratık" evrenine ait bir Hollywood kurgusu olarak telakki ediliyorsa da geçtiğimiz senelerde gerçekleşen silahlı çatışmalar YZ'nin silahlı çatışmalarda kullanılmasının olası sonuçları bakımından yeni bir fasıl açmış görünmektedir. Bu bağlamda, özellikle 2020 Eylül'de Azerbaycan ile Ermenistan arasında Dağlık Karabağ bölgesi üzerinde gerçekleşen bölgesel çatışma, güvenlik uzmanları tarafından "geleceğin silahlı çatışmalarının" bir fragmanı olarak yorumlanmıştır[367]. Azerbaycan'ın zaferi ile sonuçlanan ve Ermeni güçlerinin, yalnızca altı hafta içerisinde, askeri araçlarının %47'sini ve ağır silahlarının %93'ünü kaybettiği çatışmada[368], Ermeni askeri donanımını bu denli ciddi zarara uğratanın Azerbaycan tarafından yoğunluklu olarak kullanılan, Türkiye menşeli, Bayraktar TB2 model tanksavar füzeli insansız hava araçları olduğu belirtilmektedir[369].

Mevcut askeri konjonktürde, YZ sistemleri ile bütünleşik OSS'nin silahlı çatışmalarda kullanılmasının tamamen yasaklamasını düşünmek ne gerçekçi ne de gereklidir. Bu sistemlerin basiretli kullanımı gerçekten de silahlı çatışmalar esnasında daha az sivil ve çevresel kayıp yaşanmasını temin edebilecek; silahlı çatışmaların insancıl hukuka uygun olarak yürütülmesini kolaylaştırabilecektir. Ancak, insan-makine etkileşiminin karmaşık doğasından ve OSS'nin karar alma mekanizmalarına içkin öngörülemezlikten dolayı, bu sistemlerin silahlı çatışmalarda kullanılması aynı zamanda birçok hukuki sorunu da beraberinde getirmektedir. Özellikle, uluslararası insancıl hukuk ve ceza hukuku gibi bütün sistemin "insan" merkeze alınarak kurulduğu rejimler bakımından, mevcut hukuki araçlar

---

[365] C. Heyns, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions (A/HRC/23/47). UN Human Rights Council. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/127/76/PDF/G1312776.pdf?OpenElement, 2013, s. 80, Erişim Tarihi: 18.10.2021.

[366] Amoroso&Tamburrini, 2021, s. 258

[367] "The Azerbaijan-Armenia conflict hints at the future of war", 2020

[368] J. M. Rickli, Surrogate Warfare and the Transformation of War in the 2020s. ORF. https://www.orfonline.org/expert-speak/surrogate-warfare-transformation-war-2020s/, 2020, Erişim Tarihi: 26.12.2021.

[369] S. Gallagher, SITREP: Azerbaijan's Drone War Expands with Reaper-like TB2. Ars Technica. https://arstechnica.com/tech-policy/2020/11/sitrep-azerbaijans-drone-war-expands-with-reaper-like-tb2/, 2020, Erişim Tarihi:26.12.2021.; M. Boot, Warfare is evolving fast: We need a secretary of defense who is an agent of change. *Washington Post*. https://www.washingtonpost.com/opinions/2020/12/08/warfare-is-evolving-fast-we-need-secretary-defense-who-is-an-agent-change/, 2020, Erişim Tarihi: 26.12.2021; J. Marson & B. Forrest, Armed Low-Cost Drones, Made by Turkey, Reshape Battlefields and Geopolitics. Wall Street Journal. https://www.wsj.com/articles/armed-low-cost-drones-made-by-turkey-reshape-battlefields-and-geopolitics-11622727370, 2021, Erişim Trarihi: 26.12.2021

OSS aracılığı ile işlenebilecek olası savaş suçlarından doğacak hem bireysel sorumluluk hem de Devletin sorumluluğu hallerini düzenlemekte yetersiz kalmaktadır. Dolaylı faillik ve olası doğal sonuç modeli gibi mevcut hukuki kurumların OSS aracılığı ile işlenen savaş suçlarına analoji yoluyla uygulanabileceği ilk kertede düşünülebilse bile bunlara ilişkin detaylı incelemeler, bu tip önerilerin de uygulamada kadük kalabileceğini göstermektedir. Bu sebeple, OSS aracılığı ile işlenecek savaş suçları bakımından uluslararası hukukta yeni düzenlemeler yapılması mevcut konjonktürde bu silahların hızla yayıldığı göz önünde bulundurularak hem acil hem de elzem görünmektedir.

Kaynakça

AI HLEG. (2019). *A definition of AI: Main Capabilities and Scientific Disciplines*. European Commission.
https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Alwardt, C., & Krüger, M. (2019). Autonomy of Weapon Systems. *Institute for Peace Research and Security Policy at the University of Hamburg*, 9., Artificial intelligence and machine learning in armed conflict: A human-centred approach. *International Review of the Red Cross*, *102*(913) https://doi.org/10.1017/S1816383120000454

Álvarez, J. S. V. (2021). Autonomous Weapons Systems: The Accountability Conundrum, (Çevrimiçi)<https://archivos.juridicas.unam.mx/www/bjv/libros/13/6467/7.pdf (19.10.2021)

Amoroso, D. (2020). Autonomous weapons systems and international law: A study on human-machine interactions in ethically and legally sensitive domains. EdizioniScientificheItaliane.

Amoroso, D. &TamburriniG. (2021), Toward a Normative Model of Meaningful Human Control over Weapons Systems, Ethics & International Affairs, 35/3, 245
Artificial intelligence and machine learning in armed conflict: A human-centred approach. (2020). *International Review of the Red Cross*, *102*(913), 463-479. https://doi.org/10.1017/S1816383120000454

Bianchi, A. (2009). State Responsibility and Criminal Liability of Individuals., (ed.) A. Cassese, *The Oxford Companion to International Criminal Justice*. Oxford University Press.

Bo, M. (2021). Autonomous Weapons and the Responsibility Gap in Light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute, Journal of International Criminal Justice, (Çevrimiçi)<https://doi.org/10.1093/jicj/mqab005> (19.10.2021)

Bonafè, B. I. (2009). *The relationship between state and individual responsibility for international crimes*. Nijhoff.

Bonafè, B. I. (2016). Reassessing dual Responsibility for International Crimes. *Seqüência: EstudosJurídicos e Políticos*, *37*(73), 19-36. https://doi.org/10.5007/2177-7055.2016v37n73p19

Boot, M. (2020). Warfare is evolving fast. We need a secretary of defense who is an agent of change. *Washington Post*.

https://www.washingtonpost.com/opinions/2020/12/08/warfare-is-evolving-fast-we-need-secretary-defense-who-is-an-agent-change/,

Boulanin, V., Brunn, L., & Goussac, N. (2021). *Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction*. SIPRI (Stockholm International Peace Research Institute). https://www.sipri.org/sites/default/files/2021-06/2106_aws_and_ihl_0.pdf,

Boulanin, V., Davison, N., Goussac, N., & Carlsson, M. P. (2020). *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*. SIPRI (Stockholm International Peace Research Institute). https://www.sipri.org/sites/default/files/2020-06/2006_limits_of_autonomy.pdf,

Buchan, R. &Tsagourias, N. (2021) Autonomous Cyber Weapons and Command Responsibility, Autonomous Cyber Capabilities under International Law (ed. Rain Liivoja& Ann Väljataga),

Calverley, D. J. (2008). Imagining a Non-Biological Machine as a Legal Person. *AI & SOCIETY*, *22*(4). https://doi.org/10.1007/s00146-007-0092-7,

Casey-Maslen, S. (2018). *Autonomous Weapons Systems and International Criminal Law,*Bölüm 8, Drones and Other Unmanned Weapons Systems under International Law, Brill | Nijhoff

Cass, K. (2015). *Autonomous Weapons And Accountability: Seeking Solutions in The Law of War,* Loyola Of Los Angeles Law Review, 48(3) 1017

Cassese, A. (2013). *Cassese's international criminal law* (3rd ed). Oxford University Press.

Chengeta, T. (2020). *Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law*, Denver Journal of International Law and Policy, 45/1 (3)

Crawford, J. (2002). *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge Univ. Press.

Crootof, R. (2016). *War Torts: Accountability for Autonomous Weapons*, University Of Pennsylvania Law Review, 164(6) 1347

Cross, G. R. &Debessonet, C. G. (1986) *An Artificial Intelligence Application in the Law: CCLIPS*, *A Computer Program that Processes Legal Information*, HIGH TECH. Law Journal 1, 329.

Cummings, M. L. (2004). Automation Bias in Intelligent Time Critical Decision Support Systems. *AIAA 1st Intelligent Systems Technical Conference*. AIAA 1st Intelligent Systems Technical Conference, Chicago, Illinois. https://doi.org/10.2514/6.2004-6313,

Cummings, M. L. (2006). Automation and Accountability in Decision Support System Interface Design. *The Journal of Technology Studies*, *32*(1),. https://doi.org/10.21061/jots.v32i1.a.4,

Dennett, D. C. (1998). When Hal Kills, Who's to Blame? Computer Ethics. Içinde D. G. Stork (Ed.), *HAL's Legacy: 2001's Computer as Dream and Reality*. The MIT Press. https://doi.org/10.7551/mitpress/3404.001.0001,

Department of Defence. (2018). *Summary of the 2018 National Defense Strategy of United States of America*. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,

European Parliament resolution of 20 January 2021 on artificial intelligence: Questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice, P9 TA (2021)0009 2020/2013(INI) (2021). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html,

Franke, U. E. (2019). *Not Smart Enough: The Poverty of European Military Thinking on Artificial Intelligence* (ECFR/311). The European Council on Foreign Relations (ECFR). https://ecfr.eu/publication/not_smart_enough_poverty_european_military_thinking_artificial_intelligence/,

Fletcher, G.P. (2000). Rethinking Criminal Law, New York, Oxford University Press

Gallagher, S. (2020). *SITREP: Azerbaijan's Drone War Expands with Reaper-like TB2*. Ars Technica. https://arstechnica.com/tech-policy/2020/11/sitrep-azerbaijans-drone-war-expands-with-reaper-like-tb2/,

Garcia Vilanova, R. (2017). *When does IHL apply?* ICRC Blog. https://blogs.icrc.org/ilot/2017/08/13/when-does-ihl-apply/,

Geiß, R. (2015). *The International Law Dimension of Autonomous Weapons Systems*. Friedrich-Ebert-Stiftung, International Policy Analysis. http://library.fes.de/pdf-files/id/ipa/11673.pdf,

Gellers, J. C. (2020). *Rights for Robots: Artificial Intelligence, Animal and Environmental Law* (1. bs). Routledge. https://doi.org/10.4324/9780429288159,

Grut. C. (2013). *The Challenge of Autonomous Lethal Robotics to International Humanitarian Law*, Journal of Conflict & Security Law 5

Hallevy, G. (2016). The Criminal Liability of Artificial Intelligence Entities—From Science Fiction to Legal Social Control. *Akron Intellectual Property Journal*, *4*(2), 171-199.

Heyns, C. (2013). *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions* (A/HRC/23/47). UN Human Rights Council. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/127/76/PDF/G1312776.pdf?OpenElement,

ICRC. (2019). *Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control* (s. 28). https://www.icrc.org/en/document/autonomy-artificial-intelligence-and-robotics-technical-aspects-human-control,

Jacobson, B. R. (2017). Lethal Autonomous Weapons Systems: Mapping the GGE Debate. *DiploFoundation Policy Papers and Briefs*, *8*,

Krupiy, T. (2017). *Unravelling Power Dynamics in Organizations: An Accountability Framework for Crimes Triggered By Lethal Autonomous Weapons Systems*, Loyola University Chicago International Law Review, 15/1,

La Haye, E. (2008). *War Crimes in Internal Armed Conflicts*. Cambridge University Press. https://doi.org/10.1017/CBO9780511495151,

Liu, H. (2016) *Refining Responsibility: Differentiating Two Types of Responsibility Issues Raised by Autonomous Weapons Systems*, (ed.) Nehal Bhuta vd., Autonomous Weapons Systems: Law, Ethics, Policy, Cambridge University Press, 325

Lorenz, F. M. (1994). Law And Anarchy in Somalia, Parameters, Us Army War College Quarterly, Vol. 23, No. 4, (Çevrimiçi)<http://Strategicstudiesinstitute. Army.Mil/ Pubs/Parameters/Articles/1993/1993%20lorenz.Pdf > (19.10.2021),

Losing Humanity: The Case Against Killer Robots. (2012). Human Rights Watch. https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf,

Lotti, M. (2018). *Killer Robots in the Battlefield and the Alleged Accountability Gap for War Crimes*. Digital Watch. https://dig.watch/resources/killer-robots-battlefield-and-alleged-accountability-gap-war-crimes,

Marson, J., & Forrest, B. (2021). Armed Low-Cost Drones, Made by Turkey, Reshape Battlefields and Geopolitics. *Wall Street Journal*. https://www.wsj.com/articles/armed-low-cost-drones-made-by-turkey-reshape-battlefields-and-geopolitics-11622727370,

Mind the Gap: The Lack of Accountability for Killer Robots. (2015). Human Rights Watch. https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots,
Mosier, K. L., Skitka, L. J., Heers, S., & Burdick, M. (1998). Automation Bias: Decision Making and Performance in High-Tech Cockpits. *The International Journal of Aviation Psychology*, *8*(1), 47-63. https://doi.org/10.1207/s15327108ijap0801_3,

Nollkaemper, A. (2003). Concurrence between Individual Responsibility and State Responsibility in International Law. *International and Comparative Law Quarterly*, *52*(3), 615-640. https://doi.org/10.1093/iclq/52.3.615

O'Connell, M. E. (2021). Historical Development and Legal Basis. Içinde D. Fleck, M. Bothe, & K. Dörmann (Ed.), *The Handbook of International Humanitarian Law* (Fourth edition, ss. 10-50). Oxford University Press. https://doi.org/10.1093/law/9780198847960.001.0001

Pirim, C. Z. (2012). Aggravated Responsibility Of States In International Law: A Theoretical Assessment. *Public and Private International Law Bulletin*, *32*(2), 147-182.

Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (CCW/GGE.1/2019/3) (2019). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/285/69/PDF/G1928569.pdf?OpenElement,

Rickli, J.-M. (2020). *Surrogate Warfare and the Transformation of War in the 2020s*. ORF. https://www.orfonline.org/expert-speak/surrogate-warfare-transformation-war-2020s/,

Roff, H. (2013). Killing in War: Responsibility, Liability and Lethal Autonomous Robots, Routledge Handbook Of Ethics And War: Just War Theory In The 21st Century 14, (ed.) Fritz Allhoffvd., Routledge

Schmidt, C. T. A., & Kraemer, F. (2006). Robots, Dennett and the Autonomous: A Terminological Investigation. *Minds and Machines*, *16*(1). https://doi.org/10.1007/s11023-006-9014-6,

Schwarz, A. (2014). War Crimes. İçinde*Max Planck Encyclopedias of International Law*. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e431?rskey=1C6wQF&result=1&prd=MPIL#,

Sherman, J., & Lehr, A. (2010). Human Rights Due Diligence: Is It Too Risky? (Corporate Social Responsibility Initiative Working Paper No. 55). John F. Kennedy School of Government, Harvard University. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/workingpaper_55_shermanlehr.pdf,

Skitka, L. J., Mosier, K., & Burdick, M. D. (2000). Accountability and Automation Bias. *International Journal of Human-Computer Studies*,*52*(4). https://doi.org/10.1006/ijhc.1999.0349,

Smidt, M. L. (2000) *Yamashita, Medina, and Beyond; Command Responsibility in Contemporary Military Operations*, Military Law Review, 164, 176,

Sparrow, R. (2000). *Killer Robots*, Journal of Applied Philosophy, 24, 62,

State Council of China. (2017). *A Next Generation Artificial Intelligence Development Plan* (R. Creemers, G. Webster, P. Tsai, P. Triolo, & E. Kania, Çev.). https://d1y8sb8igg2f8e.cloudfront.net/documents/translation-fulltext-8.1.17.pdf,

Steinhardt, R. G. (2014). Weapons and the Human Rights Responsibilities of Multinational Corporations. İçinde S. Casey-Maslen (Ed.), *Weapons Under International Human Rights Law* (ss. 507-541). Cambridge University Press. https://doi.org/10.1017/CBO9781139227148.023,

Sullins, J. P. (2006). When Is a Robot a Moral Agent? *International Review of Information Ethics*, *6*(12),

The Azerbaijan-Armenia conflict hints at the future of war. (2020). *The Economist*. https://www.economist.com/europe/2020/10/08/the-azerbaijan-armenia-conflict-hints-at-the-future-of-war,

UN Web Tv. (2020). *4th Meeting—1st Session Group of Governmental Experts on Lethal Autonomous Weapons Systems 2020*. https://media.un.org/en/asset/k1e/k1e117adw0,

van Sliedregt, E. (2012). *Individual Criminal Responsibility in International Law* (C. 1). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199560363.001.0001

Weatherall, T. (2015). *Jus Cogens: International Law and Social Contract*. Cambridge University Press. https://doi.org/10.1017/CBO9781139976664

Werle, G., & Jeßberger, F. (2020). *Principles of International Criminal Law* (4. bs). Oxford University Press. https://doi.org/10.1093/law/9780198826859.001.0001,

Wyatt, A. (2020, Haziran 20). *So Just What Is a Killer Robot?: Detailing the Ongoing Debate around Defining Lethal Auton*. Washington Headquarters Services. https://nsa-demo.dod.afpims.mil/News-Features/Stories/Article-View/Article/2210967/so-just-what-is-a-killer-robot-detailing-the-ongoing-debate-around-defining-let/,

Mahkeme Kararları:

ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Karar, I.C.J. Reports 2007,

ICTY, *Tadić (Ara Temyiz)*, 17 Temmuz 1995, (IT-94-1-T),

ICC, *Prosecutor v Katanga*(ICC-01/04-01/07, 7 Mart 2014)

İSTANBUL BAROSU

•

Bilişim Hukuku Komisyonu

•

Yapay Zekâ Çalışma Grubu

Yapay Zekâ Çağında Hukuk

2021

Danışman
Dr. Barış Erman-*Yeditepe Üniversitesi Hukuk Fakültesi*

•

Editörler
Av. Selin Çetin
Av. Elif Baban
Av. C. Sümeyye Uçar
Av. Kübra İslamoğlu Bayer
Av. Zeynep Öğretmen Kotil
Av. Tarık T. Yazıcılar
Av. Damlanur İpek
Av. Benay Çaylak
Av. Nihan Üçer
Av. Pınar Saruhan
Av. Zeynep Cemre Demirtaş
Av. Mikal İpek
Av. Beyza Nur Gemci
Ayşegül Sivri