TERAZİ

HUKUK DERGİSİ • THD

Sayı **241** ▪ **Eylül 2026**

HAKEMLİ MAKALELER / Refereed Articles

Memet Erdem AYBAY : Anayasa Mahkemesi'nin Güncel Kararı Işığında Türkiye Futbol Federasyonu Tahkim Kurulu'nun Bağımsızlık ve Tarafsızlık Sorunu
The Issue of Independence and Impartiality of the TFF Arbitration Board in Light of Recent Constitutional Court Rulings

Hüseyin BİLGİN : Sermaye Piyasasında Kamunun Aydınlatılması İlkesi
The Principle of Public Disclosure in the Capital Markets

Anıl ÇAMYAMAÇ
Serkan ÇINARLI : FIFA Futbol Mahkemesine Dâir Bir İnceleme
An Analysis on FIFA Football Tribunal

Funda ÇEPNİ : Elektronik Haberleşme Hizmetinin Başkası Adına Sunulması veya Bu İzlenime Sebep Olunması Suretiyle Yetki Aşımı
Excess of Authorization by Providing Electronic Communications Service on Behalf of Others or Creating Such an Impression

Ali Fuat ÇİÇEKLİ : Ceza Muhakemesi Kanunu m.141/3 Hükmünün Hâkimin Hukukî Sorumluluğu Bakımından Kapsamı
The Scope of art.141/3 of the Criminal Procedure Code Regarding the Civil Liability of Judge

Yiğit Türker ÇOBAN : Türk Marka Hukukunda Kazanılmış (Müktesep) Haklar Teorisinin Gerekliliği Üzerine Düşünceler
Thoughts on the Necessity of Acquired (Vested) Rights Theory in Turkish Trademark Law

Cahit DAMAR : FSEK Kapsamında Açılabilecek Hukuk Davaları ve Taleplere İlişkin Değerlendirme
Evaluation of Civil Lawsuits and Claims That May Be Filed Under FSEK

Berker ÖZDEMİR : Estetik Cerrahide Beklenti Zararı
Expectation Damages in Aesthetic Surgery

Oğuz Kaan PEHLİVAN : "Trol Ağı"nda Takılan Haklar: Türkiye'de Önleyici Veri Madenciliğinin Eleştirel Analizi
Rights Caught in the "Dragnet": A Critical Analysis of Preventive Data Mining in Türkiye

Hediye BAHAR SAYIN : Anonim Şirketlerde Genel Kurula Yetkisiz Katılımın Genel Kurul Kararlarının Geçerliliğine Etkisi
The Effect of Unauthorized Participation in the General Meeting on the Validity of General Meeting Resolutions in Joint-Stock Companies

Macit ŞEFİK : Kuzey Kıbrıs Türk Cumhuriyeti Anayasası'nda Bireysel Başvuru Hakkının Olmaması Bir Eksiklik midir?
Is the Absence of the Right to Individual Application in the Constitution of the Turkish Republic of Northern Cyprus a Deficiency?

Hüseyin YALÇIN : Çerçeve Normlarda Kanunilik İlkesi
The Legality Principle of Framework Norms

HUKUK UYGULAMALARI / Law in Practice

Ersan ŞEN
Muhammed Enes EFE : Avukatın İddia ve Savunma Dokunulmazlığı Kapsamında Kişisel Verilerle İmtihanı

Mehmet Akif TUTUMLU : Tüketici Mahkemesinde Açılan Kısmî Davada (Görev Açısından) Dikkat Edilmesi Gereken Hususlar (Karar Tahlili)

Nurettin CEYLAN : Trafik Kazalarında Müterafik Kusurun Başlıca Görünüm Biçimleri ve Tespit Ölçütleri

ISSN 1306 - 9802

TÜBİTAK ULAKBİM Terazi Hukuk Dergisi TUBİTAK-ULAKBİM Türk Hukuk Dizininde Yer Almaktadır.

seçkin

TERAZİ

HUKUK DERGİSİ • THD

Sayı 241 • Eylül 2026

seçkin

Yayın Sahibi

Seçkin Yayıncılık A.Ş. Adına
Koray SEÇKİN

Yayıncısı

Seçkin Yayıncılık A.Ş. (Sertifika No: 45644)

İletişim

Mustafa Kemal Mah. 2158. Sk. No: 13
Çankaya/ANKARA
(0 312) 435 30 30 (Pbx)
terazi@seckin.com.tr
www.terazi.com.tr,
www.jurix.com.tr/dergi/terazi-hukuk-dergisi

Sorumlu Yazı İşleri Müdürü

Koray SEÇKİN
seckin@seckin.com.tr

Editörler

Prof. Dr. Alpay HEKİMLER
alpay.hekimler@ogu.edu.tr
Av. Mutlu DİNÇ
mdinc@seckin.com.tr

Editör Yardımcısı

Av. Çilem BAHADIR
cbahadir@seckin.com.tr

Dil Editörleri

Ahmet Berat BEGÜN / İngilizce
ahmetberat@gmail.com

Abone Sorumlusu

Meral HATIRLI
abone@seckin.com.tr

Kapak ve Sayfa Tasarımı

Emre KIZMAZ
ekizmaz@seckin.com.tr

ISSN 1306-9802

e-ISSN 2791-8432

Derginin Kısa Adı THD

Sayı 241 - Eylül 2026

Tarandığı Dizinler ULAKBİM

Yayın Dili Türkçe

Basım Tarihi/Yeri Eylül 2026/ANKARA

Yayın Türü Yaygın Süreli, Aylık

Matbaa

Vadi Grafik Ltd. Şti. (Sertifika No: 47479)
İvedik Organize Sanayi Bölgesi, 1420 Cad. No: 58/1
Yenimahalle/ANKARA
(0 312) 395 85 71

Yayın Kurulu

- Prof. Dr. Ayşe NUHOĞLU
  İstanbul Medipol Üniversitesi - İstanbul
- Prof. Dr. Murat TOPUZ
  Marmara Üniversitesi - İstanbul
- Prof. Dr. Müslüm AKINCI
  Kocaeli Üniversitesi - Kocaeli
- Prof. Dr. Ramazan ÇAĞLAYAN
  Ankara Hacı Bayram Veli Üniversitesi - Ankara
- Çilem BAHADIR
  Avukat, Ankara Barosu, Seçkin Yayıncılık - Ankara
- Galip DOĞAN
  Avukat, Ankara Barosu - Ankara
- Mehmet Akif TUTUMLU
  Tüketici Mahkemesi Hâkimi, Adalet Bakanlığı - Ankara
- Mutlu DİNÇ
  Avukat, İstanbul Barosu, Seçkin Yayıncılık - İstanbul

Danışma Kurulu

- Prof. Dr. Ahmet Mithat KILIÇOĞLU
  Atılım Üniversitesi - Ankara
- Prof. Dr. Ali Rıza ÇINAR
  Mef Üniversitesi - İstanbul
- Prof. Dr. Ayşe HAVUTÇU
  Yaşar Üniversitesi - İzmir
- Prof. Dr. Ayşe NUHOĞLU
  Medipol Üniversitesi - İstanbul
- Prof. Dr. Dr. h.c. Bahri ÖZTÜRK
  İstanbul Kültür Üniversitesi - İstanbul
- Prof. Dr. Binnur TULUKÇU
  Selçuk Üniversitesi - Konya
- Prof. Dr. Cemil KAYA
  İstanbul Üniversitesi - İstanbul
- Prof. Dr. Cumhur ŞAHİN
  Ankara Hacı Bayram Veli Üniversitesi - Ankara
- Prof. Dr. Çetin ARSLAN
  Hacettepe Üniversitesi - Ankara
- Prof. Dr. Durmuş TEZCAN
  İstanbul Kültür Üniversitesi - İstanbul
- Prof. Dr. Emel BADUR
  Çankaya Üniversitesi - Ankara
- Prof. Dr. Ender Ethem ATAY
  Başkent Üniversitesi - Ankara
- Prof. Dr. Ercan AKYİĞİT
  Mef Üniversitesi - İstanbul
- Prof. Dr. Faruk ACAR
  Marmara Üniversitesi - İstanbul
- Prof. Dr. Feridun YENİSEY
  Bahçeşehir Üniversitesi - İstanbul
- Prof. Dr. H. Tamer İNAL
  İstanbul Beykent Üniversitesi - İstanbul
- Prof. Dr. Dr. h.c. Hakan HAKERİ
- Prof. Dr. Halide Gökçe TÜRKOĞLU ÖZDEMİR
  Yaşar Üniversitesi - İzmir
- Prof. Dr. Halil KALABALIK
  Sakarya Üniversitesi - Sakarya
- Prof. Dr. Haluk Hadi SÜMER
  Selçuk Üniversitesi - Konya
- Prof. Dr. Hasan İŞGÜZAR
  Yozgat Bozok Üniversitesi - Yozgat
- Prof. Dr. Hayri BOZGEYİK
  Ankara Yıldırım Beyazıt Üniversitesi - Ankara
- Prof. Dr. Hayrunnisa ÖZDEMİR
  Ankara Sosyal Bilimler Üniversitesi - Ankara
- Prof. Dr. İ. Hamit HANCI
  İzmir Katip Çelebi Üniversitesi - İzmir
- Prof. Dr. İbrahim AŞIK
  Marmara Üniversitesi - İstanbul
- Prof. Dr. İbrahim KAYA
  İstanbul Üniversitesi - İstanbul
- Prof. Dr. İbrahim ÖZBAY
  Tokat Üniversitesi - Tokat
- Prof. Dr. İzzet ÖZGENÇ
  Ankara Hacı Bayram Veli Üniversitesi - Ankara
- Prof. Dr. Koray DOĞAN
  Dokuz Eylül Üniversitesi - İzmir
- Prof. Dr. M. Emin ARTUK
  İstanbul Medipol Üniversitesi - İstanbul
- Prof. Dr. M. Fatih USAN
  Ankara Medipol Üniversitesi - Ankara
- Prof. Dr. Muharrem ÖZEN
  Ankara Üniversitesi - Ankara
- Prof. Dr. Murat TOPUZ
  Marmara Üniversitesi - İstanbul
- Prof. Dr. Mustafa Ruhan ERDEM
  Yaşar Üniversitesi - İzmir
- Prof. Dr. Mustafa TOPALOĞLU
  Özyeğin Üniversitesi - İstanbul
- Prof. Dr. Müslüm AKINCI
  Kocaeli Üniversitesi - Kocaeli
- Prof. Dr. Nurettin BİLİCİ
  Çankaya Üniversitesi - Ankara
- Prof. Dr. Nuri ERİŞGİN
  Lefke Avrupa Üniversitesi - Lefke/KKTC
- Prof. Dr. Olgun DEĞİRMENCİ
  TOBB Üniversitesi - Ankara
- Prof. Dr. Ömer ANAYURT
  Ankara Hacı Bayram Veli Üniversitesi - Ankara
- Prof. Dr. Ömer KORKUT
  Çukurova Üniversitesi - Adana
- Prof. Dr. Ramazan ÇAĞLAYAN
  Ankara Hacı Bayram Veli Üniversitesi - Ankara
- Prof. Dr. Sabahattin YÜREKLİ
  Bursa Uludağ Üniversitesi - Bursa
- Prof. Dr. Sevtap YOKUŞ VEZNEDAROĞLU
  Altınbaş Üniversitesi - İstanbul
- Prof. Dr. Şaban KAYIHAN
  İstanbul Ticaret Üniversitesi - İstanbul
- Prof. Dr. Şafak NARBAY
  Sakarya Üniversitesi - Sakarya
- Prof. Dr. Tekin MEMİŞ
  Beykent Üniversitesi - İstanbul
- Prof. Dr. Timur DEMİRBAŞ
  Yaşar Üniversitesi - İzmir
- Prof. Dr. Veli Özer ÖZBEK
  İzmir Ekonomi Üniversitesi - İzmir
- Prof. Dr. Zühtü ARSLAN
  Ankara Üniversitesi - Ankara
- Doç. Dr. Cafer EMİNOĞLU
  Ankara Yıldırım Beyazıt Üniversitesi - Ankara
- Doç. Dr. H. Tahsin GÖKCAN
  Anayasa Mahkemesi Başkan Vekili - Ankara
- Doç. Dr. Mehmet ALTUNKAYA
  Akdeniz Üniversitesi - Antalya
- Doç. Dr. Pınar BACAKSIZ
  Dokuz Eylül Üniversitesi - İzmir
- Doç. Dr. Selin SERT SÜTÇÜ
  Akdeniz Üniversitesi - Antalya
- Doç. Dr. Seydi KAYMAZ
  Ufuk Üniversitesi - Ankara
- Doç. Dr. Sinan Sami AKKURT
  Selçuk Üniversitesi - Konya
- Doç. Dr. Şeref İBA
  Uluslararası Kıbrıs Üniversitesi - Lefkoşa/KKTC
- Dr. Öğr. Üyesi Ahmet Cemal RUHİ
  Hasan Kalyoncu Üniversitesi - Gaziantep
- Dr. Öğr. Üyesi Kumru KILIÇOĞLU YILMAZ
  Atılım Üniversitesi - Ankara
- Dr. Öğr. Üyesi Merve ACUN MEKENGEÇ
  Kocaeli Üniversitesi - Kocaeli
- Dr. Öğr. Üyesi Mustafa Aytaç ÖZELÇİ
  İstanbul Kültür Üniversitesi - İstanbul
- Dr. Öğr. Üyesi Oğuz CANER
  Bursa Uludağ Üniversitesi - Bursa
- Ali PARLAR
  İstanbul BAM Cumhuriyet Savcısı - İstanbul
- Aydın TEKDOĞAN
  Emekli Hâkim - Avukat
- Cengiz APAYDIN
  Kartal Adliyesi Cumhuriyet Savcısı - İstanbul
- Erhan GÜNAY
  Avukat, Muğla Barosu - Muğla
- Gönen ERİŞ
  Yargıtay Onursal Daire Başkanı - İstanbul
- İbrahim PINAR
  Avukat, Ankara Barosu - Ankara
- Mahir Ersin GERMEÇ
  Yargıtay Hukuk Dairesi Onursal Başkanı - Ankara
- Özgür SEMİZ
  Kültür İşleri ve Enformasyon Müsteşarı - Paris/Fransa
- Sadettin DOĞANYİĞİT
  E. Sayıştay Başdenetçisi - Ankara
- Serhat YENER
  Noter - Kırşehir 2. Noteri
- Y. Güngör ÖZDEN
  Anayasa Mahkemesi Onursal Başkanı - Ankara

TÜBİTAK ULAKBİM

Terazi Hukuk Dergisi
TUBİTAK-ULAKBİM
Türk Hukuk Dizininde
Yer Almaktadır.

İçindekiler

Yazım ve Atıf Kuralları 5

Editörden 7

Hakemli Makaleler 9

Memet Erdem AYBAY
Anayasa Mahkemesi'nin Güncel Kararı Işığında Türkiye Futbol Federasyonu Tahkim Kurulu'nun Bağımsızlık ve Tarafsızlık Sorunu
The Issue of Independence and Impartiality of the TFF Arbitration Board in Light of Recent Constitutional Court Rulings 10

Hüseyin BİLGİN
Sermaye Piyasasında Kamunun Aydınlatılması İlkesi
The Principle of Public Disclosure in the Capital Markets 26

Anıl ÇAMYAMAÇ
Serkan ÇINARLI
FIFA Futbol Mahkemesine Dâir Bir İnceleme
An Analysis on FIFA Football Tribunal 39

Funda ÇEPNİ
Elektronik Haberleşme Hizmetinin Başkası Adına Sunulması veya Bu İzlenime Sebep Olunması Suretiyle Yetki Aşımı
Excess of Authorization by Providing Electronic Communications Service on Behalf of Others or Creating Such an Impression 48

Ali Fuat ÇİÇEKLİ
Ceza Muhakemesi Kanunu m.141/3 Hükmünün Hâkimin Hukukî Sorumluluğu Bakımından Kapsamı
The Scope of art.141/3 of the Criminal Procedure Code Regarding the Civil Liability of Judge 63

Yiğit Türker ÇOBAN
Türk Marka Hukukunda Kazanılmış (Müktesep) Haklar Teorisinin Gerekliliği Üzerine Düşünceler
Thoughts on the Necessity of Acquired (Vested) Rights Theory in Turkish Trademark Law 79

Cahit DAMAR
FSEK Kapsamında Açılabilecek Hukuk Davaları ve Taleplere İlişkin Değerlendirme
Evaluation of Civil Lawsuits and Claims That May Be Filed Under FSEK 94

Berker ÖZDEMİR
Estetik Cerrahide Beklenti Zararı
Expectation Damages in Aesthetic Surgery 104

Oğuz Kaan PEHLİVAN
"Trol Ağı"nda Takılan Haklar: Türkiye'de Önleyici Veri Madenciliğinin Eleştirel Analizi
Rights Caught in the "Dragnet": A Critical Analysis of Preventive Data Mining in Türkiye 119

Hediye BAHAR SAYIN
Anonim Şirketlerde Genel Kurula Yetkisiz Katılımın Genel Kurul Kararlarının Geçerliliğine Etkisi
The Effect of Unauthorized Participation in the General Meeting on the Validity of General Meeting Resolutions in Joint-Stock Companies 141

Macit ŞEFİK
Kuzey Kıbrıs Türk Cumhuriyeti Anayasası'nda Bireysel Başvuru Hakkının Olmaması Bir Eksiklik midir?
Is the Absence of the Right to Individual Application in the Constitution of the Turkish Republic of Northern Cyprus a Deficiency? 160

Hüseyin YALÇIN
Çerçeve Normlarda Kanunilik İlkesi
The Legality Principle of Framework Norms 173

Hukuk Uygulamaları 187

Ersan ŞEN
Muhammed Enes EFE
Avukatın İddia ve Savunma Dokunulmazlığı Kapsamında Kişisel Verilerle İmtihanı 188

Mehmet Akif TUTUMLU
Tüketici Mahkemesinde Açılan Kısmî Davada (Görev Açısından) Dikkat Edilmesi Gereken Hususlar (Karar Tahlili) 191

Nurettin CEYLAN
Trafik Kazalarında Müterafik Kusurun Başlıca Görünüm Biçimleri ve Tespit Ölçütleri 197

Yüksek Yargı Kararları 209

Anayasa Mahkemesi Kararları 210

Yargıtay Kararları 222

Mevzuat Dizini 259

Kavram ve İçtihat Dizini 261

Kavramlar Dizini 262

İçtihat Başlık Dizini 263

İçtihat Dizini 264

"Trol Ağı"nda Takılan Haklar: Türkiye'de Önleyici Veri Madenciliğinin Eleştirel Analizi(*)

Rights Caught in the "Dragnet": A Critical Analysis of Preventive Data Mining in Türkiye

Oğuz Kaan PEHLİVAN(**)

Öz

Veri madenciliği uygulamaları, suçları tespit etmek ve önlemek için kolluk kuvvetleri tarafından giderek daha fazla kullanılmaktadır. Ancak, Almanya'da öncülüğü yapılan önleyici amaçlı veri madenciliği uygulaması, Türkiye'de sağlam bir yasal temele sahip değildir. Bu düzenleyici boşluk, özellikle özel veri tabanlarına erişimle ilgili olarak veri madenciliği uygulamalarını yöneten kapsamlı bir yasal çerçevenin oluşturulmasını gerektirir. Veri madenciliği suç önleme etkinliğini artırabilirken, aynı zamanda kişisel veri koruması için önemli riskler sunar. Bu makale, Anayasa Mahkemesi kararlarına ve Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarına atıfta bulunarak Türkiye'nin yasal ortamını eleştirel bir şekilde analiz eder ve Türkiye tarafından sıklıkla olarak ihlal edilen kişisel hak ve özgürlükleri korumak için açık yasal düzenlemelerin elzem olduğu sonucuna varır.

Anahtar Kelimeler

Veri Madenciliği, Trol Ağı Tarama Metodu, Adli Bilişim, Bilgisayarlı Eşleşme Metodu, Kişisel Verilerin Korunması, Ceza Adaleti.

Abstract

Data mining applications are increasingly employed by law enforcement agencies to detect and prevent crimes. Yet, the practice of data mining for preventive purposes, pioneered in Germany, lacks a robust legal foundation in Türkiye. This regulatory gap necessitates the establishment of a comprehensive legal framework governing data mining practices, particularly regarding access to private databases. While data mining can enhance crime prevention effectiveness, it simultaneously presents significant risks to personal data protection. This paper critically analyses Türkiye's legal environment, referencing Constitutional Court rulings and European Court of Human Rights (ECtHR) jurisprudence, and concludes that clear legal regulations are essential to safeguarding personal rights and freedoms which was and are continually being violated by Türkiye.

Keywords

Data Mining, Dragnet Surveillance Method, Digital Forensics, Computer Matching, Data Protection, Criminal Justice.

(*) Hakemli makale - *Peer reviewed article*
Makalenin geliş tarihi: 03.07.2026
Makalenin kabul tarihi: 05.08.2026
DOI: 10.67051/thd.241.09

(**) *Dr.*, Oslo Üniversitesi, Oslo - Norveç
E-posta: o.k.pehlivan@jus.uio.no; pehlivan.oguzkaan@gmail.com
Orcid: 0000-0003-0136-5389

Tüm Hakları Saklıdır / All rights reserved.

Extended Summary

The digitalisation of public administration and criminal justice has substantially expanded the capacity of public authorities to collect, combine and analyse personal data. Data mining techniques make it possible to identify patterns, correlations and relationships within large datasets and may thereby contribute to the prevention and detection of crime. The same techniques, however, may also allow public authorities to generate new information about individuals by combining data originally collected for entirely different purposes. This becomes particularly problematic when the persons whose data are processed are not themselves suspected of committing a criminal offence. The central question addressed in this article is therefore whether preventive data mining and dragnet-style screening practices in Türkiye are governed by a legal framework that is sufficiently clear, foreseeable, proportionate and subject to effective supervision.

The study employs a doctrinal and comparative legal method. It examines Turkish constitutional, criminal-procedural, policing and data-protection rules alongside the jurisprudence of the Turkish Constitutional Court and the Court of Cassation. These materials are compared with German constitutional jurisprudence, European Union law and relevant European human-rights standards. In addition, the article examines anonymised documents originating from criminal investigations in Türkiye. These documents are particularly important because they provide concrete evidence of the practical use of cross-database matching involving information obtained from both public and private databases. The study therefore combines normative legal analysis with an examination of actual investigative practices.

The German experience provides the principal comparative framework. Modern preventive data screening developed in Germany under the concepts of *Rasterfahndung* and *Schleppnetzfahndung*. These techniques were historically used to identify potential suspects by screening large datasets according to predetermined characteristics and by comparing information stored in different databases. Their effectiveness, however, is accompanied by an inherent fundamental-rights problem: a large number of persons who are not suspected of wrongdoing may nevertheless become objects of state analysis merely because their data correspond to particular patterns or profiles.

German constitutional jurisprudence has progressively developed safeguards against this risk. The Federal Constitutional Court's jurisprudence, beginning with the constitutional recognition of informational self-determination and continuing through its decisions of 2006, 2010, 2016, 2020 and 2023, has increasingly subjected large-scale data collection and automated analysis to requirements of proportionality, purpose limitation, legal certainty and sufficiently concrete danger. In its 2006 *Rasterfahndung* judgment, the Court considered the mass screening of data relating to persons who were not individually suspected of criminal conduct to constitute a serious interference with informational self-determination. A merely general terrorist threat was insufficient to justify such an intrusive measure. The Court's subsequent case law on telecommunications data retention, secret surveillance, subscriber information and automated data analysis further developed this approach by requiring stronger substantive thresholds and procedural safeguards as the intensity of the interference increases.

The Federal Constitutional Court's 2023 judgment concerning automated data analysis is particularly significant for the subject of this article. Modern analytical systems are capable not merely of retrieving existing information, but also of combining extensive datasets, identifying previously unknown relationships and generating new profiles or risk assessments. The constitutional problem thus concerns not only access to data, but also what public authorities are technically able to infer from those data. The German approach demonstrates that broad statutory powers to collect information cannot automatically be treated as authorisation for unlimited automated analysis. The greater the analytical capacity of the state, the more important become restrictions concerning the purposes of processing, categories of data, seriousness of the relevant danger, affected persons and independent supervision.

European law reflects a comparable tendency. In *SpaceNet AG and Telekom Deutschland*, the Court of Justice of the European Union rejected the general and indiscriminate retention of traffic and location data for ordinary crime-prevention purposes and instead emphasised more targeted forms of retention. The later *La Quadrature du Net II* judgment continued this proportionality-oriented approach. The Dutch SyRI litigation similarly demonstrates the legal problems created by automated risk profiling. In that case, the combination of data from different public databases for fraud-risk assessment was found incompatible with Article 8 of the European Convention on Human Rights because the system lacked sufficient transparency and proportionality safeguards. Taken together, these developments indicate that preventive data analysis requires more than a formal legal basis: necessity, proportionality, purpose limitation, transparency and meaningful independent review are equally essential.

The Turkish legal framework is considerably more fragmented. Numerous institutions participate directly or indirectly in the collection, processing and circulation of personal information, including law-enforcement authorities, intelligence services, the Information and Communication Technologies Authority, judicial authorities and the Cyber Security Presidency. Systems such as UYAP, POLNET, GBT, biometric databases and telecommunications records have produced an increasingly interconnected public-sector data environment. The integration of databases may improve administrative and investigative efficiency, but it simultaneously increases the capacity to reconstruct an individual's activities and relationships across different spheres of life.

The Personal Data Protection Law No.6698 provides an important general framework but contains broad exceptions for preventive, protective, intelligence and criminal-justice activities. These exceptions should not be interpreted as granting public authorities an unrestricted power to employ every technically available form of data analysis. There is an important legal distinction between obtaining a particular piece of information and systematically

combining multiple databases in order to identify patterns, construct profiles or generate predictions. The latter constitutes a qualitatively more intrusive form of personal-data processing. This problem becomes particularly acute with artificial intelligence, machine-learning-based profiling and predictive policing, because statistical correlations may increasingly substitute for individualised suspicion. False positives, discriminatory profiling and persistent digital suspicion may consequently affect individuals who have no actual connection with criminal activity.

Turkish constitutional jurisprudence contains both restrictive and permissive elements. In its 2020 judgment concerning the so-called "virtual patrol" power of the police, the Constitutional Court annulled a provision authorising online investigative activity because the limits of the interference were not defined with sufficient clarity. The decision is important because it confirms that digital policing powers must satisfy requirements of legality, foreseeability and proportionality. Likewise, the Court of Cassation has held that telecommunications measures cannot indiscriminately encompass persons who are neither suspects nor accused solely because they used the same base station, thereby limiting a classic form of dragnet investigation.

By contrast, the Constitutional Court's 2023 *Murat Albayrak* decision illustrates a more permissive approach. The case concerned historical telecommunications records obtained from public payphones and subsequently subjected to technical analysis by law-enforcement authorities in order to identify potentially suspicious individuals. The Court concluded that the relevant investigative practice could not be regarded as manifestly arbitrary and declared the application inadmissible. The decision is particularly significant because the investigative method starts with a broad population of communications data and progressively eliminates unrelated persons in order to identify potential suspects. Functionally, this resembles the logic of dragnet screening. Nevertheless, the method itself was not subjected to an intensive constitutional review based on concrete danger, foreseeability and proportionality comparable to that developed in German constitutional jurisprudence.

The article's principal empirical contribution lies in its examination of actual investigation documents reproduced in Figures 1-4. These documents show that telephone numbers attributed to target individuals were compared with information obtained from several public databases, including educational, health, utility, passport and driving-licence records. More significantly, the material also refers to information originating from private commercial databases. The documents therefore indicate that cross-database analysis involving both public and private data sources is not merely a theoretical possibility in Türkiye but an identifiable investigative practice. This finding raises an important legal question: even where an authority is entitled to request particular information, does that authority also possess a sufficiently specific statutory power to aggregate, systematically analyse and profile that information through dragnet-style techniques?

The article argues that the answer cannot automatically be affirmative. A judicial order or a general statutory power to obtain information does not necessarily provide an adequate legal basis for systematic data mining. Such techniques may affect large groups of individuals who are unrelated to the investigated offence and may generate new information that did not previously exist in any individual database. Accordingly, the legal regulation of data mining must address not only the collection of data but also its subsequent combination, analysis, retention, reuse and transformation into investigative profiles.

The study therefore proposes a specific safeguards-based regulatory framework for Türkiye. First, dragnet screening and automated data analysis should be governed by an explicit statutory basis that distinguishes preventive intelligence activities from criminal investigation and establishes appropriate thresholds, such as a concrete and sufficiently serious danger or an individualised degree of criminal suspicion. Second, data processing should be governed by necessity, proportionality, purpose limitation and data minimisation. Third, the legislation should clearly regulate the categories of data that may be processed, access to private databases, retention periods, deletion procedures, subsequent use and transfer of data, and the circumstances in which information relating to third parties may be analysed. Fourth, algorithmic and automated analytical methods must be sufficiently transparent and auditable to permit effective judicial or independent supervision. In this respect, Türkiye would benefit from a more specific regime comparable in function to the EU Law Enforcement Directive rather than relying predominantly on broad exceptions contained in general data-protection legislation.

In conclusion, preventive data mining should neither be prohibited categorically nor treated as an inherent extension of ordinary police powers. Properly regulated data analysis may increase investigative efficiency and assist public authorities in identifying genuine threats. The constitutional problem arises when technological capacity develops faster than the legal framework governing its use. Turkish law already contains important constitutional guarantees, data-protection principles and judicial decisions restricting certain forms of indiscriminate surveillance. Nevertheless, these rules do not yet form a coherent and comprehensive regime governing dragnet screening, cross-database analysis, algorithmic profiling and predictive policing. A clear, narrowly tailored and effectively supervised statutory framework would therefore protect both interests at stake: it would provide law-enforcement authorities with legitimate and predictable investigative powers while safeguarding individuals against arbitrary, disproportionate and opaque forms of digital surveillance.

Giriş

Bu makale, Türkiye'de adli soruşturma ve kovuşturmalar kapsamında kolluk kuvvetleri tarafından giderek daha fazla kullanılan bir veri madenciliği uygulamaları ve özellikle trol ağı tarama metodunu hukuki yönleriyle incelemektedir. Trol ağı tarama metodu, kolluk tarafından genellikle hedef kişiler hakkında herhangi bir suç şüphesi olmasa bile büyük ölçekli, ayrım gözetmeyen veri toplama çabalarını ifade eder. Bu tür uygulamalar, kolluk faaliyetlerinin hukukiliği, insan haklarına uyumu ve demokratik denetimi konusunda pek çok soru ortaya çıkarmaktadır. Veri madenciliği teknikleri kolluğun gelişmiş teknik imkanlarla suç önleme kapasitesini artırırken Türk anayasa hukuku ve Avrupa İnsan Hakları Sözleşmesi (8. maddesi) kapsamında güvence altına alınan özel hayatın gizliliği, kişisel verilerin korunması ve bireysel hakkı ve özgürlükler için önemli riskler içermektedir. Bu makale, gelişen gözetim uygulamalarını göz önünde bulundurarak Türkiye'de kolluk tarafından uygulandığı tespit edilen trol ağı tarama metodunun hukuki çerçevesinin eleştirel bir analizini sunmaktadır. Bilgi teknolojilerinin yaygınlaşmasıyla birlikte, bireylerin günlük yaşamlarında farklı cihazlar ve uygulamalar aracılığıyla çeşitli veriler toplanmaktadır. Bu durum, bireylerin gizlilik hakları ile kolluk kuvvetlerinin güvenlik amaçlı veri toplama faaliyetleri arasında bir denge kurma ihtiyacını ortaya koymaktadır. Veri madenciliği tekniklerinin yasal boyutlarının açıkça belirlenmesi, hukukun üstünlüğü açısından kritik öneme sahiptir.

Veri madenciliği, farklı veri tabanlarının kullanımını koordine ederek güncel sorunları ele almak için yenilikçi çözümler ve farklı bakış açıları kullanan bir tekniktir. Veri madenciliği, büyük miktarda bilgi içeren veri tabanlarından anlamlı verilere ulaşmaya amaçlar, bu da belirli hedeflerle uyumlu ilgili tahminlerin oluşturulmasını ve bu verilerin anlamlı bir şekilde sınıflandırılmasını sağlar.[1] Veri madenciliği, eğitim, ticaret, mühendislik, bankacılık, finans, tıp ve telekomünikasyon dahil olmak üzere birçok sektörde geniş bir uygulama alanına sahiptir. Kısacası, veri madenciliği, veri tabanlarından elde edilen verileri yapılandırarak bilgi üretmeyi sağlayan araçlar ve teknikler olarak nitelendirilebilir.[2]

Veri madenciliği tekniklerinin uygulanması; deprem verilerinin analiz edilmesine, çevrimiçi basın ve medya kaynaklarından görsel ve metinsel verilerin ayıklanmasına ve bunlardan öngörülebilir ve anlamlı sonuçların çıkarılmasına olanak tanır. Veri madenciliği örneğin kredi kartları kullanımı analiz edilerek, kullanıcıların tüketim alışkanlıklarını belirlemek için de kullanılabilir. Üniversite veritabanlarından profiller oluşturmak, öğrencilerin başarısını etkileyen faktörleri ve başarı seviyelerini belirlemek ve üniversite öğrenci portföylerini çıkarmak veya bir şirket veya markanın müşteri profilini belirlemek ve her grup için özelleştirilmiş reklam ve pazarlama stratejileri belirlemek için de uygulanabilmektedir.[3]

Şirketler, kendi müşterileri ya da müşterilerinin kullanıcıları hakkında; devletler ise egemen yargı yetkisi altındaki ülkelerdeki insanlar üzerinde veri madenciliği faaliyetleri yürütmektedirler.[4] Trol ağı taraması metoduyla Internet üzerinde ya da veritabanlarında daha önceden belirlenen Suç doğuran, suça neden olan özelliklere (kriminojen) sahip insanlar, fikirler, mallar ve hizmetler tespit edilmekte, bunlar arasındaki bağlantılar haritalandırılmakta ve olası tehditler belirlenmektedir. Amerika Birleşik Devletleri'nde (ABD) 2013 yılında patlak veren Ulusal Güvenlik Ajansı (NSA) faaliyetleri konusundaki tartışmalardan önce, dünya çapında internet ve veritabanlarında trol ağı metoduyla tarama yapmanın teknik olarak mümkün olamayacağı düşünülmekteydi. Öte yandan Internet trafiğinin yüzde 99'unun deniz altı kabloları üzerinden gerçekleştirildiği[5] ve bu trafiğin yüzde 30'unun ABD üzerinden geçtiği tahmin edilmektedir.[6] Dolayısıyla ABD ulusal güvenlik kurumları; potansiyel tehditleri ve teröristleri belirlemek, yerlerini tespit etmek amacıyla dünya çapında insan istihbaratı (*HUMINT*)[7] faaliyeti yürütmek yerine kendi topraklarından geçen Internet trafiğini izlemenin ve sinyal istihbaratı (*SIGINT*)[8] uygulamalarının fırsat maliyeti açısından oldukça avantajlı olduğunu düşünmekteydi. Edward Snowden'ın ifşaatlarından sonra, ABD'nin NSA aracılığıyla tüm internet trafiğinde trol ağı taraması (*Dragnet*) yaptığı açığa çıkmıştır.[9] Snowden, dünya çapındaki bu tür bir gözetlemenin NSA tarafından PRISM (*Protect, Respond, Inform, Secure and Monitor*) adı verilen bir programın parçası olarak Google, Facebook,

---

1 Serkan Savaş, Nurettin Topaloğlu ve Mithat Yılmaz, 'Veri Madenciliği ve Türkiye'deki Uygulama Örnekleri', *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi* C.11 S.21 (2012), s.2; Bu bağlamda veri madenciliği, çok katmanlı veri yığınları arasından 'ilgili görünen-görünmeyen' verileri işleyip aralarında bağlantı kurma faaliyeti olarak da tanımlanmaktadır bkz: Turan Atlı, 'Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi', *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* C.2 S.1 (2019), s.9; veri madenciliği, yapısal veri tabanlarında depolanmış büyük verilerden yeni ve yararlı örüntüler çıkarma şeklinde de tanımlanmaktadır bkz: Özgür Sağır ve Nur Banu Albayrak, 'Veri Madenciliğinin Siber Suçlarda Kötüye Kullanımı', *Journal of Kocaeli Health and Technology University* C.2 S.3 (Aralık 2024), s.69.

2 Dilek Yüksel Civelek, 'Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi', *Bilgi Toplumu Dairesi Başkanlığı, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı*, Uzmanlık Tezi (2011), s.42.

3 Savaş, Topaloğlu ve Yılmaz, s.9-17; Doğan, lisansüstü tezlerde en çok çalışılan uygulama konusunun "profil belirleme/kümeleme" olduğunu (20 tez) açıkça söylüyor, bkz: Onur Doğan, 'Türkiye'de Veri Madenciliği Konusunda Yapılan Lisansüstü Tezler Üzerine Bir Araştırma', *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* C.19 S.3 (2017), s.938-939.

4 Helena Miller, 'How Does Big Tech Use Data Mining?', *humanID*, 23 Haziran 2021, https://human-id.org/blog/how-does-big-tech-use-data-mining/ [Erişim 28 Aralık 2024].

5 Alan Mauldin, 'Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?', *Telegeography*, 04 Mayıs 2023, https://blog.telegeography.com/2023-mythbusting-part-3 [Erişim 20 Nisan 2024].

6 Tim Stronge, 'Does 70% of the World's Internet Traffic Flow Through Virginia?', *Telegeography*, 30 Mayıs 2019, https://blog.telegeography.com/does-70-of-the-worlds-internet-traffic-flow-through-virginia [Erişim 20 Nisan 2024].

7 HUMINT (Human Intelligence - İnsan İstihbaratı): İnsan kaynaklarından (ajanlar, muhbirler, esirler, yerel halk) elde edilen istihbarattır.

8 SIGINT (Signals Intelligence - Sinyal İstihbaratı): Elektronik sinyallerin (telefon görüşmeleri, e-postalar, radyo yayınları, radar sinyalleri) yakalanması ve analiz edilmesiyle elde edilen istihbarattır.

9 Jason Keiber, 'Surveillance Hegemony', *Surveillance & Society* Vol.13 No.2 (2015), s.168.

Skype, Yahoo ve diğer servis sağlayıcıları ve veritabanları kullanılarak yürütüldüğünü ortaya koymuştur.[10]

Bu çalışma, 'trol ağı' gibi önleyici veri madenciliği tekniklerini yalnızca ceza muhakemesi bağlamında değil; dijital gözetimin anayasal sınırlarını belirleyen kanunilik-meşru amaç-ölçülülük testinin bir alt başlığı olarak ele almaktadır. Dijital gözetim pratiklerinin büyük veri ve yapay zeka destekli biçimde sınıflandırma/öngörü üretmesi, müdahalenin kapsamını genişlettiği ölçüde hukuki belirlilik, bağımsız denetim ve etkili başvuru yolları gibi güvencelerin 'tamamlayıcı şart' haline geldiğini göstermektedir.

I. Adli Veri Madenciliği ve Adli Bilişim

Toplumdaki değişimlere ve yönelimlere kayıtsız kalamayacak olan hukuk da yaşanan gelişmelere kendisini adapte etmek durumundadır. Bu noktada hukuk, yeni sorunların çözümünde ya var olan usul ve araçlarını uyarlar ya da yeni usul ve araçlar geliştirir. Yeni delillerin elde edilmesi ve kabul edilebilir bir şekilde adli süreçlerde kullanabilmesi için yargılamanın dijitalleşmesi, veri tabanları (DNA veri tabanı, parmak izi, araç plakası, vb.) oluşturulması, otomatik plaka tanıma sisteminin geliştirilmesi yeni duruma uygun araçlar olarak gösterilebilir.[11] Ancak bilişim teknolojilerinin gelişmesine paralel olarak yaşanan adaptasyon yeterli olmamaktadır. Oluşturulan veri tabanlarını karşılaştırarak adli süreçlere faydalı bilgilerin üretilmesi sorunu yine karşımıza çıkmaktadır. Bu noktada veri madenciliğine istihbarat ve kolluk faaliyetleri kapsamında ceza adalet sisteminin verimliliğini artırma ve çeşitli verimlilik modellemeleri çıkarma çerçevesinde ihtiyaç duyulmaktadır.

A. Trol Ağı Tarama Metodu

Veri madenciliği, suçların ve suçluların tespit edilmesi ile önleyici amaçlarla, potansiyel tehdit unsurlarının açığa çıkarılması ya da potansiyel delillerin ele geçirilmesi amacıyla kolluk tarafından kullanılabilmekte çeşitli adli bilişim teknikleriyle şüpheli ve sanıklar tespit edilebilmektedir.[12] Adli süreçlerde elde edilen verinin tasnif edilerek anlamlı ve kullanılabilir bilgiye dönüştürülmesinde trol ağı tarama yöntemi en çok başvurulan yöntem olarak karşımıza çıkmaktadır.[13]

1972 Münih Olimpiyatlarında 11 İsrailli atletin rehin alınması ve öldürülmesi sonrasında "*bilgisayar destekli araştırma metodu*" kullanılmak üzere Almanya Federal Polis Bürosu'nda geniş bir veritabanı oluşturulmuştur.[14] 1978 yılına gelindiğinde, 37 veri bankasında 4,7 milyon isim, 3.100 kuruluş, 2,1 milyon parmak izi ve 1,9 milyon kişinin fotoğrafının depolandığı ve kolluk tarafından kullanıldığı tespit edilmiştir.[15] Alman hukukunda "*Rasterfahdung*"[16] ya da "*Schleppnetzfahndung*"[17] olarak adlandırılan bu kavram Türkçede "*Şüpheli Sayısını En Aza İndirmeye Yönelik Sistem Analizi*", "*Elektronik Veri İşleme*", "*Şema Soruşturması*", "*Trol Ağı Metodu*" olarak adlandırılmaktadır.[18] Bu metodun önleyici amaçlarla ve suçların aydınlatılmasına ilişkin olarak ilk olarak kullanılması 1970'ler Almanya'sında gerçekleştirilmiştir. Alman kolluk kuvvetleri, Alman Ceza Muhakemesi 163. bölümüne dayanarak "*trol ağı arama*" (*Schleppnetzfahndung*) (*trawl net search*) ya da "*tarama araması*" (*Rasterfahndung*) (*scanning search*) adıyla bu metodunu geliştirmiştir.[19] Bu yönteme öncelikle bir şüphelinin konumu belirlemek için, "*sıradan*" verileri analiz etmek ve bazı çıkarımlarda bulunmak için başvurulmuştur.[20] 1970 ve 1980'li yıllarda Rote Armee Fraktion (RAF) isimli terörist yapının unsurlarının tespit edilmesinde trol ağı tarama metodu kullanılmıştır.[21]

Trol ağı araştırma metodunun temel yapısı şöyledir:

> "*Belli kriminojen özellikler taşıyan bilgiler, kimliklerin bilgisayar tarafından otomatik bir şekilde okunması sırasında hafızaya kaydedilmekte ve bu bilgiler uzmanlar tarafından değerlendirilmektedir. Kriminojen özelliğe sahip olan ve ağa takılan herkes hakkında araştırma yapılır. Trol ağı metodunu düzenleyen StPO 163d maddesi, kişisel verilerin bilgisayara kaydedilmesi yasağı açısından genel bir hukuka uygunluk sebebidir. Ancak Alman hukukunda trol ağı metodu sadece ceza muhakemesi hukuku amaçlarına uygun olarak düzenlenmiştir. Önleme amaçlı veri toplama bu kapsama girmez.*"[22]

Trol ağı arama metodu ilk olarak Alman iş adamı Hanns-Martin Schleyer'in RAF tarafından kaçırılması sonrasında, 1979 yılında Frankfurt'ta RAF üyesi teröristlerin

---

[10] Lonneke van der Velden, 'Leaky Apps and Data Shots: Technologies of Leakage and Insertion in NSA-Surveillance', *Surveillance & Society* Vol.13 No.2 (2015), s.184; David Murakami Wood and Steve Wright, 'Before and After Snowden', *Surveillance & Society* Vol.13, No.2 (2015), s.136; Oğuz Kaan Pehlivan, 'Amerika'da Paradigma Değişimi: NSA ve İstihbaratın Denetimi', *Özgürlük ve Güvenlik Dengesinde Siber Dünya* (2024), s.7-9; Oğuz Kaan Pehlivan, 'İpin Ucunu Kaçırmak: NSA', *Özgürlük ve Güvenlik Dengesinde Siber Dünya* (2024), s.10-13.

[11] Johannes F. Nijboer, 'Section 3: Concept Paper and Questionnaire- Information Society (Including Information Technology) and Criminal Justice', *Combatting Cybercrime*, 2013, https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/preparatory-colloquium-section-iii-concept-paper-and-questionnaire.pdf [Erişim 15 Nisan 2024].

[12] Leyla Keser Berber, *Adli Bilişim (Computer Forensic)* (2004), s.39, Sağır ve Albayrak, s.77.

[13] Yener Ünver, 'Federal Almanya'da Terör ve Organize Suçluluk ile İlgili Düzenlemeler', *Nurullah Kunter'e Armağan* (1998), s.408-409.

[14] A. Aslıhan Erbaşı, 'Avrupa Birliği Terör Politikası Işığında Almanya Örneği', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2009), s.142.

[15] Ari Weil, 'The Red Army Faction: Understanding a Measured Government Response to an Adaptive Terrorist Threat', *Cornell International Affairs Review* Vol.10, No.2 (2017), s.145.

[16] Erbaşı, s.142.

[17] Baran Kızılırmak, 'Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2018), s.157.

[18] Ayşe Nuhoğlu, 'Trol Ağı Araştırma Metoduna İlişkin Alman Anayasa Mahkemesi Kararı', *Hukuk ve Adalet* S.10 (2007), s.201.

[19] Yonah Alexander, *Counterterrorism Strategies: Successes and Failures of Six Nations* (Potomac Books, 2006), s.83-84.

[20] Iain Cameron, *National Security and the European Convention on Human Rights* (The Hague, 2021), s.182.

[21] Erbaşı, s.143 vd.

[22] Feridun Yenisey, *Kolluk Hukuku* (2023), s.204.

kullandıkları bir evin tespit edilmesinde kullanılmıştır. Kolluk kuvvetleri aradıkları şüphelileri tespit edebilmek için öncelikle hedef şahısların isim ve soy isimleriyle telefon faturası sorgusu yapmışlardır. Ancak hedef kişilerin elektrik faturasını sahte bir isimle nakit olarak ödemesinin muhtemel olduğunu düşünerek, ilk olarak elektrik idaresine nakit olarak ödeme yapan tüm kişilerin ismini sorgulamışlar ve yaklaşık 18.000 potansiyel isim çıkmıştır. Sonraki aşamada ise bu isimleri farklı veritabanlarında eşleştirerek gerçek olup olmadıklarını tespit etmeye çalışmışlardır. Tapu kayıtları, sağlık sigortası, yangın sigortası, devlet ödenekleri ve kurumsal kayıtlarda yer alana isim listeleri çapraz kontrol edilerek sadece iki ismin hatalı olduğu ortaya çıkmıştır. Birisi uyuşturucu satıcısı bir suçlu, diğeri ise Schleyer'i kaçıran Rolf Heissler.[23]

Trol ağı metoduyla yapılan geniş tarama ve eşleştirmelerde sadece kriminojen özellikleri benzeyen kişilerin trol ağına takılmamakta, şüpheli olmayan pek çok masum kişilerin de verilerine erişilebilmektedir. Zira profilleme istatistiksel çıkarımlara dayandığından kesinlikten ziyade olasılık üretir; bu da yanlış bir özelliğin kişiye atfedilmesi (false positive) veya gerçekten ilgili kişinin dışarıda kalması (false negative) riskini yapısal hale getirir.[24] Bu bağlamda trol ağı tekniği, yalnızca veri toplama değil; verilerin algoritmik olarak sınıflandırılması, risk kategorilerine ayrılması ve sonraki kolluk/istihbarat kararlarına girdi üretilmesi bakımından, literatürde dijital gözetimin tipik işleyiş döngüsüyle örtüşmektedir.[25] Dolayısıyla bu metodun sınırlarının çizilmesine ihtiyacı duyulmuştur. Almanya'da Kişisel Verilerin Korunması Kanunu 1977 yılında çıkarılmıştır. 1981 yılında Federal Meclis sosyal planlama (barınma, eğitim vb.) yapmak amacıyla kişisel veriler toplanmasına izin vermiştir. Ancak Almanya Federal Anayasa Mahkemesi (BVerfG), bu hükmün anayasaya aykırılığına hükmetmesine rağmen trol ağı ve tarama araması prosedürlerinin kullanılmasını yasaklamamıştır.[26] 1983'te Federal Anayasa Mahkemesi'nin "*nüfus sayımı*" (*Volkszählunsurteil*) kararına göre:

> "*Modern veri işleme koşulları altında, kişiliğin özgürce gelişimi, bireyin kişisel verilerinin sınırsız toplanmasına, depolanmasına, kullanılmasına ve ifşa edilmesine karşı korunmasını gerektirir. Bu nedenle bu koruma, insan onuruyla birlikte kişiliğin özgürce gelişimi temel hakkı tarafından kapsanmaktadır. Bu bağlamda, temel haklar, bireyin kişisel verilerinin ifşasını ve kullanımını kendisi belirleme gücünü garanti eder.*"[27]

1986 yılında ise polise, eğer suçlunun tutuklanması ve suçun çözülmesinde haklı neden oluşturuyorsa -tükürük ve parmak izi gibi benzersiz olan DNA molekülü içeren diğer vücut sıvıları da dâhil- kişisel veri toplayabilmesi, bunları depolayabilmesi ve analiz edebilmesi yetkisi verilmiştir.[28] Alman Ceza Muhakemesi Kanununa göre trol ağı metodu ile araştırma; diğer yollarla maddi gerçeğe ulaşma ve faili tespit etmenin daha az başarı şansı olacağı ve daha zor olacağı durumlarda sınırlı sayıda belirtilen terör suçları, silahlı soygun, ateşli silahlar ile uyuşturucu madde suçları kapsamında uygulanabilir.[29] Ayrıca, bu metoda sadece ağır cezalık suçların adli soruşturmalarında başvurulabilir ve önleyici amaçlar için kullanılması mümkün değildir.[30]

Teknik kabiliyetlerin oldukça ilerlemesine paralel olarak 2000'li yıllarda Almanya Federal Anayasa Mahkemesi (BVerfG), veri madenciliğine elverişli büyük veri toplama/erişim yetkilerini orantılılık, amaçla bağlılık ve somut tehlike/şüphe eşiği üzerinden sıkılaştıran bir hat kurmuştur:

4 Nisan 2006 tarihli *Rasterfahndung / elektronik profil çıkarma* kararında Mahkeme, 11 Eylül saldırıları sonrası "uyuyan teröristleri" tespit etmek amacıyla uygulanan ve "trol ağı" (Rasterfahndung) olarak bilinen yöntemin anayasaya uygunluğunu denetlemektedir. Mahkeme, masumiyet karinesine sahip çok sayıda kişinin verisinin suç şüphesi olmaksızın taranmasının ve toplanmasının bireyin "*bilgi edinmeye dair kendi kaderini tayin hakkına*" yönelik ağır bir müdahale olduğuna hükmetmiş ve genel bir terör tehdidinin (örneğin 11 Eylül sonrası oluşan durumun) bu tedbir için tek başına yeterli olamayacağını belirtmiştir. Karara göre, bu tür önleyici veri tarama faaliyetlerinin hukuka uygun sayılabilmesi için yüksek dereceli hukuki menfaatlere (yaşam hakkı, devletin varlığı gibi) yönelik "*somut bir tehlikenin*" (*konkrete Gefahr*) varlığı şarttır ve somut olgulara dayanmayan, tamamen ihtiyati nitelikteki taramalar anayasaya aykırıdır. Bu kararında mahkeme ters orantılılık olarak adlandırılan bir ilkeyi açıklamıştır:

> "*Olası veya fiili hukuki menfaat ihlallerinin ağırlığı ne kadar büyük ve söz konusu temel hak müdahalesinin ağırlığı ne kadar az ise, ilgili hukuki menfaatin ihlal edildiğini (veya risk altında olduğunu) ortaya koymak için gereken olasılık derecesini ve şüphenin dayandığı olguları belirlemek için gereken kesinlik derecesini düşürmek o kadar kabul edilebilir hale gelir.*"[31]

---

23 Richard Clutterbuck, *Terrorism, Drugs & Crime in Europe after 1992* (Routledge, 2013), s.60; Nurullah Özgül, 'İnsan Haklarının Korunması ve Geliştirilmesinde Yeni Bir Sorun Alanı: Algoritmik Profilleme', *TİHEK Akademik Dergisi* Y.5 S.9 (2022), s.102-103: Karşılaştırmalı olarak, Hollanda'daki SyRI (Risk Gösterge Sistemi) örneğinde de farklı kurumların elindeki ikametgâh, banka hesabı ve taşınmaz kayıtları gibi verilerin tek bir algoritmik risk sisteminde birleştirilmesi; kullanılan model/algoritmaların gizliliği nedeniyle 'şeffaflık eksikliği' tartışmalarını doğurmuş, Lahey Yerel Mahkemesi de mahremiyet hakkı ile teknolojiden yararlanma arasında kurulması gereken dengenin sağlanamadığını vurgulamıştır.

24 Özgül, s.91.

25 Murat Uzunparmak, 'Dijital Gözetimin Kavramsal ve Hukuki Çerçevesi: Yapay Zeka Destekli Gözetim Sistemlerinin Anayasal Sınırları', *Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* C.27 S.3 (2025), s.1089-1116.

26 Clutterbuck, s.60.

27 EFDPO - European Federation of Data Protection Officers, 'A Landmark Judgment Turns 40: The German Census Judgment of 1983', 14.12.2023, https://www.efdpo.eu/a-landmark-judgment-turns-40-the-german-census-judgment-of-1983/ [Erişim 28 Aralık 2024].

28 Clutterbuck, s.59.

29 Yenisey, s.205.

30 Kızılırmak, s.157.

31 BVerfG (1. Senat), 1 BvR 518/02, 4 Nisan 2006, BVerfGE 115,320,360 ff. "Je gewichtiger die drohende oder erfolgte Rechtsgutbeeinträchtigung und je weniger gewichtig der Grundrechtseingriff ist,

Mahkeme bu formülü, özellikle terörle mücadele gibi yüksek hukuki menfaatlerin söz konusu olduğu durumlarda, somut tehlike eşiğinin veya şüphe derecesinin, daha az yoğun müdahaleler için aşağı çekilebileceğini belirtmek için kullanmıştır. Ancak mahkeme, trol ağı taraması gibi masumiyet karinesini zedeleyen ağır müdahalelerde, tehlike sadece genel düzeyde ise bu eşiğin düşürülmesine izin vermemektedir.

2 Mart 2010 tarihli *trafik verilerinin toplu/saklama* (*data retention*) kararında ise Mahkeme, telekomünikasyon trafik verilerinin (kimin, kiminle, ne zaman görüştüğü, konum bilgisi vb.) somut bir şüphe olmaksızın altı ay süreyle önleyici olarak saklanmasını (*Vorratsdatenspeicherung*) düzenleyen yasayı incelemektedir. Mahkeme, bu uygulamanın vatandaşların iletişim mahremiyetine (Any. m.10) çok ağır bir müdahale oluşturduğunu ve nüfusun tamamını kapsayan bu tür bir gözetimin toplumda "*diffüz bir tehdit hissi*" yaratarak özgürlüklerin kullanımını engelleyebileceğini belirtmiştir. Kararda, veri saklamanın kategorik olarak imkânsız olmadığı, ancak söz konusu yasanın veri güvenliği standartları, verinin kullanım amacı, şeffaflık ve hukuki denetim mekanizmaları açısından yetersiz olduğu için anayasaya aykırı olduğu sonucuna varılmış ve toplanan verilerin derhal silinmesine hükmedilmiştir.[32]

20 Nisan 2016 tarihli *BKA Yasası / terörle mücadelede gizli gözetim* kararında Mahkeme, Federal Kriminal Dairesi'ne (BKA) uluslararası terörle mücadele kapsamında verilen konut gözetimi, bilgisayar sistemlerine gizli erişim (uzaktan arama) ve iletişim denetimi gibi geniş yetkileri anayasal denetimden geçirmektedir. Mahkeme, bu yetkilerin "*özel hayatın çekirdek alanını*" (insan onurunun dokunulmaz parçası) ihlal etmemesi gerektiğini vurgulayarak, mevcut düzenlemelerin çoğunun orantısız olduğuna ve özellikle verilerin silinmesi, şeffaflık ve yargısal denetim gibi koruma mekanizmalarını yeterince içermediğine karar vermiştir. Ayrıca karar, toplanan verilerin başka amaçlarla kullanılması veya paylaşılmasının (örneğin yabancı istihbarat servisleriyle), verinin ilk toplandığı andaki amaçla uyumlu olması veya varsayımsal olarak yeniden toplanmasını haklı kılacak ağırlıkta bir gerekçeye dayanması gerektiği ilkesini (*amaç değişikliği / hypothetische Datenneuerhebung*) detaylandırmıştır. Bu kararında Mahkeme uluslararası terör tehlikesine karşı konut içi gözetim, IT sistemine uzaktan erişim, iletişimin denetlenmesi gibi derin müdahaleleri ilkesel olarak dışlamaz; fakat çekirdek özel hayatın korunması, mesleki sır (avukat, gazeteci vb.) korumaları, üçüncü kişilere sirayet için çok dar koşullar, bildirim-denetim-silme yükümlülükleri ve özellikle veri kullanımı/aktarımı bakımından amaçla bağlılık ile "*amaç değişikliğinde hipotetik yeniden-toplama*" (*hypothetical recollection*) ölçütünü merkezî bir sınır olarak kurar (yurtdışına veri aktarımı dâhil).[33]

27 Mayıs 2020 tarihli kullanıcı verisi (*Bestandsdaten*) / dinamik IP eşleştirme kararında Mahkeme, güvenlik birimlerinin telekomünikasyon hizmet sağlayıcılarından abone bilgilerini (özellikle dinamik IP adreslerinin kime ait olduğu bilgisini) talep etme yetkilerini düzenleyen yasaları incelemektedir. Mahkeme, dinamik IP adreslerinin eşleştirilmesinin basit bir kimlik tespiti olmadığını, kişinin iletişim davranışlarını ve internet kullanımını ifşa etmesi nedeniyle telekomünikasyon gizliliğine (Any. m.10) yönelik daha derin bir müdahale olduğunu saptamıştır. Kararda, bu tür verilere erişimin, genel bir idari işlem gibi sınırsız olamayacağı; kamu güvenliği için somut bir tehlike veya suç takibi için en azından başlangıç şüphesinin bulunması gerektiği belirtilerek, yasal düzenlemelerin kullanım amacını ve eşiklerini yeterince sınırlamadığı gerekçesiyle orantısızlık ve anayasaya aykırılık kararı verilmiştir. Bir diğer deyişle, Mahkeme abone verisine erişimi düzenleyen hükümleri büyük ölçüde yetersiz amaç sınırlaması ve düşük eşikler nedeniyle anayasaya aykırı bularak; en azından kamu güvenliği için somut tehlike veya cezai soruşturma için başlangıç şüphesi, dinamik IP üzerinden kimlik tespitinde ise daha ağır menfaat/ihlâl eşiği, ayrıca belgelendirme, bildirim ve yargısal denetim gibi güvenceleri zorunlu kılar (geçiş dönemi için sınırlı uygulamaya izin vererek).[34]

Son olarak Alman hukukunda veri madenciliği tekniklerinin hukuki sınırları, 16 Şubat 2023 tarihli Federal Anayasa Mahkemesi kararıyla daha da netleşmiştir. Mahkeme, "otomatik veri analizi"ne (*automatisierte Datenanalyse*) dair kolluk yetkilerini düzenleyen Hessen Emniyet Teşkilatı Kanunu'ndaki hükümleri iptal ederek, bireylerin mahremiyet haklarının ancak ciddi ve somut bir tehlike söz konusu olduğunda sınırlandırılabileceğini vurgulamıştır. Kararda özellikle şu ifadeye yer verilmesi oldukça dikkat çekicidir:

> "*Otomatik veri analizi önceden veri biriktirme (stoklama) amacıyla yapılamaz; yalnızca somut bir tehlike temelinde ve yeterli yasal güvencelerle yürütülebilir.*"[35]

Mahkeme, ayrıca "*hedef gözetmeyen büyük veri analizlerinin*" bireylerin temel haklarını orantısız biçimde ihlal edebileceğine dikkat çekerek, bilgiye dayalı kişisel karar alma özgürlüğünün (*informationelle Selbstbestimmung*) anayasal güvence altında olduğunu açıkça belirtmiştir. Bu karar, Türkiye'de halen hukuki temeli belirsiz biçimde uygulandığı görülen trol ağı tarama gibi geniş kapsamlı analiz pratikleri açısından da önemli bir karşılaştırmalı hukuki referans sunmakta; somut tehdit koşulunun ve yasal güvencelerin yokluğu durumunda yapılan veri analizlerinin açık bir temel hak ihlali teşkil edeceğine işaret etmektedir.

um den es sich handelt, desto geringer darf die Wahrscheinlichkeit sein, mit der auf eine drohende oder erfolgte Verletzung des Rechtsguts geschlossen werden kann, und desto weniger fundierend dürfen gegebenenfalls die Tatsachen sein, die dem Verdacht zugrunde liegen."

32 BVerfG (1. Senat), 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08, 2 Mart 2010.

33 BVerfG (1. Senat), 1 BvR 966/09, 1 BvR 1140/09, 20 Nisan 2016.

34 BVerfG (1. Senat), 1 BvR 1873/13, 1 BvR 2618/13, 27 Mayıs 2020.

35 BVerfG, 1 BvR 1547/19, Rn. 1, 16 Şubat 2023. Eine automatisierte Datenanalyse darf nicht auf Vorrat erfolgen, sondern nur auf der Grundlage einer konkreten Gefahr und mit hinreichenden gesetzlichen Schutzvorkehrungen.

Alman anayasa yargısının ulusal düzeyde geliştirdiği bu ölçütler -somut tehlike eşiği, amaçla sınırlılık ve orantılılık- yalnızca ulusal hukukla sınırlı kalmamış; kişisel verilerin önleyici amaçla toplu biçimde saklanması sorunu, Avrupa Birliği hukukunda da benzer bir ölçülülük ekseninde ele alınmıştır.

Avrupa Birliği Adalet Divanı'nın (ABAD) 20 Eylül 2022 tarihli *SpaceNet v. Telekom Deutschland* (C-793/19 ve C-794/19) birleştirilmiş davalarına ilişkin kararı da oldukça önemlidir. Alman Federal İdare Mahkemesi (*Bundesverwaltungsgericht*), Almanya'daki Telekomünikasyon Yasası'nın (TKG), telekomünikasyon hizmet sağlayıcılarına (SpaceNet ve Telekom Deutschland gibi) müşterilerinin trafik ve konum verilerini (kimin, kiminle, ne zaman görüştüğü, IP adresleri vb.) suçla mücadele ve kamu güvenliği amacıyla genel ve ayrım gözetmeksizin (*indiscriminate*) saklama zorunluluğu getirmesinin AB hukukuna uygunluğunu sormuştur. ABAD, bu tür bir "genel ve ayrım gözetmeyen" veri saklama yükümlülüğünün, AB Temel Haklar Şartı'nın özel hayata saygı (m.7), kişisel verilerin korunması (m.8) ve ifade özgürlüğü (m.11) maddelerine aykırı olduğuna hükmetmiştir. Mahkeme, bu tür bir uygulamanın ancak casusluk ve terör gibi *ulusal güvenliğe yönelik ciddi bir tehdit* durumunda ve bu tehdidin *somut, gerçek ve öngörülebilir olması* şartıyla, sınırlı bir süre için uygulanabileceğini belirtmiştir.[36]

Karar, ciddi suçlarla mücadele amacının bile, tüm nüfusun trafik ve konum verilerinin toptan saklanmasını haklı çıkaramayacağını, ulusal güvenlik tehdidi ile adi suçlar arasında bir hiyerarşi olduğunu vurgulamıştır. Bununla birlikte Mahkeme, ciddi suçlarla mücadele için şu yöntemlerin hukuka uygun olabileceğini belirtmiştir:

1. **Hedefli Saklama (Targeted Retention):** Belirli kişi kategorileri veya coğrafi bölgelerle sınırlı saklama.
2. **IP Adreslerinin Saklanması:** İnternet bağlantısının kaynağına atanan IP adreslerinin genel ve ayrım gözetmeksizin (ancak sınırlı bir süre için) saklanması.
3. **Kimlik Verilerinin Saklanması:** Kullanıcıların sivil kimlik bilgilerinin genel saklanması.
4. **Hızlı Dondurma (Quick Freeze):** Somut bir suç şüphesi üzerine, halihazırda mevcut verilerin silinmesini önlemek için yetkili makam kararıyla anlık olarak dondurulması.

Sonuç olarak ABAD, Alman yasasının öngördüğü şekliyle, herhangi bir somut şüphe veya tehdit olmaksızın önleyici amaçla yapılan genel veri toplanmasının ve saklamanın AB hukukuna aykırı olduğuna karar vermiştir.

ABAD, IP adreslerinin genel ve ayrımsız saklanmasına ilişkin sonraki La Quadrature du Net II kararında da (C-470/21, 30 Nisan 2024) SpaceNet'te çizdiği sınırı esas olarak sürdürmüştür. Avrupa hukukunda önleyici veri madenciliğinin sınırlarını gösteren bir başka gelişme ise, yüksek mahkeme içtihadının ötesinde idari düzeyde kurulan risk analizi sistemlerine ilişkindir. Hollanda'da sosyal yardım dolandırıcılığını önlemek amacıyla kurulan SyRI (Systeem Risico Indicatie) sistemi, farklı kamu veri tabanlarını birleştirerek vatandaşları risk profillerine göre işaretlemekteydi. Lahey Bölge Mahkemesi, 5 Şubat 2020 tarihli kararında SyRI mevzuatının, öngördüğü veri işlemenin şeffaflıktan yoksun olması ve ölçülülük testini karşılamaması nedeniyle Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesindeki özel hayata saygı hakkına aykırı olduğuna hükmetmiştir. SyRI kararı, Almanya'daki Rasterfahndung ve 2023 tarihli otomatik veri analizi kararlarının doğal bir karşılaştırmalı eşi olarak; devletin refah ve güvenlik amacıyla kurduğu otomatik profilleme sistemlerinin, açık yasal dayanak, şeffaflık ve bağımsız denetim güvenceleri olmaksızın temel haklarla bağdaşmayacağını ortaya koymaktadır.[37]

B. Bilgisayarlı Eşleme Metodu (Computer Matching)

Bir başka veri madenciliği metodu olarak bilgisayar eşleştirmesi gösterilebilir. Bu metot, şüpheli kişi ve yaşamı hakkında bilgi toplamak amacıyla kamu ve özel kurumların bilgisayar sistemlerinde depolanan verilerin karşılaştırılmasını ve toplanan verilerden şüphelinin kimliğinin tespit edilmeye çalışılmasını içerir.[38] Bilgisayar eşleştirmesi, bilgisayara belirli kalıpları (örneğin sosyal güvenlik numaralarının kopyaları, eşleşen isimler, adresler) araması için talimat vermek üzere tasarlanmış bir yazılım kullanarak veri tabanlarının birbiriyle karşılaştırılmasını gerektirir. Trol ağı tarama metoduna benzer şekilde, veri tabanları belirli bir veri öğesi, yani bir tanımlayıcı (*identifier*) kullanılarak karşılaştırılır. ABD'de sosyal güvenlik numaraları kullanılabilirken, Türkiye'de kimlik numaraları veya ad ve soyadların ilk birkaç harfi kullanılabilmektedir. Amaç, vergi daireleri, hastaneler, yurtlar gibi kamu kurumlarına ait bilgisayar sistemlerinde depolanan verilerle şüpheli kişinin kişisel verilerini karşılaştırarak gerçeği ortaya çıkarmak olduğundan, doğru ve iyi sınıflandırılmış kayıtların tutulması büyük önem taşımaktadır.[39]

ABD'de daha çok mükerrer sosyal yardım alan mükerrer kesilen faturalarla dolandırıcılık suçlarına ilişkin olarak bu yöntem kullanılmaktadır. 1988 tarihli Bilgisayarlı Eşleme ve Mahremiyetin Korunması Yasası (*The Computer Matching and Privacy Protection Act of 1988*) eşleme programları kullanımda kişisel verilere ilişkin güvenceler getirmekte, federal kurumların veri

[36] ABAD, Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH, Joined Cases C-793/19 and C-794/19, 20 Eylül 2022.

[37] Marvin van Bekkum and Frederik Zuiderveen Borgesius, 'Digital Welfare Fraud Detection and the Dutch SyRI Judgment', *European Journal of Social Security* Vol.23 No.4 (2021), s.323-340. Kararın insan hakları boyutu için ayrıca bkz. Adamantia Rachovitsa and Niclas Johann, 'The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case', *Human Rights Law Review* Vol.22 No.2 (2022), s.1-15.

[38] Nihal Temizsoy Bayram, 'Ceza Muhakemesi Hukukunda Moleküler Genetik İnceleme ve Elde Edilen Verilerin Delil Olarak Kullanılması', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2018), s.60.

[39] Ünver, s.407.

sorgulama işlemlerini hangi şartlar altında yapacağını belirlemektedir.[40]

II. Türkiye'de Adli Veri Madenciliği

Almanya ve Avrupa Birliği hukukunda kanunilik-meşru amaç-ölçülülük ekseninde biçimlenen bu güvence rejimi, Türk hukuku bakımından bir karşılaştırma zemini sunmaktadır. Zira aşağıda görüleceği üzere, Türkiye'de trol ağı tarama ve benzeri veri madenciliği tekniklerinin fiilî uygulaması yaygınlaşmış olmakla birlikte, bu teknikleri kuşatan öngörülebilir ve denetlenebilir bir hukuki çerçeve henüz oluşmamıştır.

Türkiye bağlamında konuya iki açıdan yaklaşılabilir. İlk olarak Türkiye'de veri madenciliğinin verimlilik artırımı[41] ve kamu hizmetlerinin kolaylaştırılması[42] amacıyla kullanılmasına ilişkin bazı adımlar atıldığı söylenebilir. Veri madenciliği metotlarını kullanarak verimliliğin artırılması mümkün olan adli bilişim uygulamalarımızdan bazıları şöyledir: UYAP Bilişim Sistemi, SEGBİS, POLNET, Jandarma Entegre Muhabere ve Bilgi Sistemi (*JEMUS*), balistik iz ve görüntü analizi (*Balistika)*, Otomatik Parmak İzi Tanıma Sistemi (*AFIS*). 2006 yılında TÜBİTAK ve Adalet Bakanlığı tarafından öncelikli birtakım araştırma alanları belirlenmiş ve "*Adli Veri Madenciliği*" araştırma alanları arasında sayılmıştır.[43] Yürütülecek araştırmalar sonucunda yargı sisteminde, suçla mücadelede ve karar alma süreçlerinde verimlilik artışına dair hedeflere ulaşılması öngörülmüştür. Örneğin, adli veri madenciliğinin suçla mücadele politikalarının formüle edilmesini, oluşturulmasını ve uygulanmasını, suç haritasının çıkarılmasını ve verilere dayalı idari kararların alınmasını kolaylaştıracağı ifade edilmiştir. Elde edilen çıktılar, gelecekteki karar alma süreçlerinde kullanılmak üzere izlenecek ve değerlendirilecektir. Hâkim ve savcılara yönelik eğitim programı, izleme ve değerlendirme sürecinin bulgularına uygun olarak geliştirilecek ve uygulanacaktır. Kurulacak yeni mahkemelerin sayısı, oluşturulacak uzmanlık alanları ve hakimler, savcılar ve personel için belirlenecek kalite standartları da belirlenecektir.

Adalet Bakanlığı'nın 2010-2014 Stratejik Planında ise "*2014 yılı sonuna kadar adli istatistik çalışmalarının geliştirilmesi ve UYAP'ın adli veri madenciliği alanında etkin kullanılmasının sağlanması*" bir hedef olarak belirlenmiştir.[44] Ayrıca bu çerçevede veri havuzu (*Data Warehouse*) yapısı ve veri madenciliği (*Data Mining*) sistemlerinin kurulması amaçlanmaktadır. Bunun bir sonucu olarak 17 Mayıs 2024 tarihinde Ulusal Biyometrik Veri Yönetim Sistemi, Emniyet Genel Müdürlüğü tarafından tüm Türkiye'de kullanılmaya başlandı. Şu an için sadece parmak izi tanıma sistemi kullanılan Ulusal Biyometrik Veri Yönetim Sisteminde Gelecek dönemde avuç içi, damar, yüz, iris, retina, ses gibi diğer biyometrik teknolojilerin de millileştirilmesi ve Ulusal Biyometrik Veri Ailesi'nin elde edilmesi hedeflenmektedir.[45]

İkinci olarak ise veri madenciliğinin suçla mücadele de etkinliğin artırılması noktasında bir teknik olarak kullanılması söz konusudur. "*Suç veri madenciliği*" giderek gelişen bir alandır. Türk literatüründe, konunun kişisel verilerin güvenliği çerçevesinde çok sınırlı bir şekilde ele alındığı görülmektedir. Türkiye'de, veri madenciliği için temel bir girdi oluşturan kişisel verilerin korunması, kaydedilmesi ve paylaşılması konusunda tartışmalar devam etmektedir. Bu bağlamda, suçla mücadele, önleyici/teşhis edici veya cezai kovuşturma amacıyla veri madenciliğine olanak sağlayan yasal düzenlemelere bakmakta fayda vardır.

A. Türkiye'de Trol Ağı Tarama ve Bilgisayarlı Eşleme Metodu

Veri madenciliği tekniklerinin uygulayıcıları yalnızca güvenlik kurumları (MİT, emniyet) ile sınırlı değildir. Türkiye'de Bilişim Teknolojileri ve İletişim Kurumu (BTK), Siber Güvenlik Başkanlığı, KVKK, Adalet Bakanlığı, Savcılıklar ve *Historical Traffic Search*-Arama Trafiği Geçmişi (HTS) toplanmasına ilişkin kararları yoluyla Ceza Hakimlikleri gibi çok sayıda kurum doğrudan ya da dolaylı biçimde bu süreçlerde rol almaktadır. Bu aktörlerin bazıları doğrudan veri toplayıcı, bazıları işleyici, bazıları da denetleyici pozisyonda bulunmaktadır.

Özellikle UYAP, POLNET, SEGBİS, GBT gibi sistemler yalnızca emniyet birimleriyle sınırlı değil, aynı zamanda savcılık makamları ve mahkemeler tarafından da aktif biçimde kullanılmakta; böylece çok kurumlu bir dijital yargı ekosistemi oluşmaktadır. Dolayısıyla, devletin yalnızca "gizli servis/kolluk" değil, aynı zamanda sivil kamu yönetimi aygıtları eliyle de dijital gözetim kapasitesine ulaştığı söylenebilir. Dijital gözetimin kamu yönetiminde normalleşmesi, yetki sınırlarının belirsizleşmesi halinde hukuki belirlilik ve hesap verebilirlik ilkelerini aşındırmakta; bu da çok-aktörlü veri ekosistemlerinde denetim boşluklarını daha görünür kılmaktadır.[46]

BTK'nın erişim ve denetim yetkileri ile Siber Güvenlik Başkanlığı'nın yasal konumu, veri madenciliği uygulamalarının yönlendirilmesi ve uygulanması bakımından kritik önemdedir. Özellikle 177 no.lu Cumhur-

---

[40] U.S. Department of the Treasury, 'Computer Matching Programs', 19.03.2024, https://home.treasury.gov/footer/privacy-act/computer-matching-programs [Erişim 20 Nisan 2024].

[41] Neslihan Can, 'Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2020), s.195-198.

[42] Yılmaz Demirci, 'Kamu Hizmetlerinde Veri Madenciliği: Çözüm Masası Verileri Temelinde Bir Araştırma', Yayınlanmamış Doktora Tezi, *Sakarya Üniversitesi* (2018); Doğan, s.934,940.

[43] Adalet Bakanlığı, *Türkiye Hukuk Kamu Araştırmaları Programı* (TÜBİTAK, 2006) http://www.tubitak.gov.tr/tubitak_content_files/ARDEB/kamag/Turkiye_Hukuk_Kamu_Arastirma_Programi.pdf [Erişim 28 Aralık 2024].

[44] Adalet Bakanlığı, *Adalet Bakanlığı Stratejik Planı (2010-2014)*, https://sgb.adalet.gov.tr/Resimler/SayfaDokuman/24122019093355stratejikplan.pdf [Erişim 28 Aralık 2024].

[45] ODATV, 'Emniyet verileri milli yazılıma emanet: BİYOTEKSAN kuruldu', *Odatv.com*, 17.05.2024, https://www.odatv.com/guncel/emniyetteki-biyometrik-veriler-milli-yazilima-emanet-biyoteksan-kuruldu-120044143 [Erişim 24 Ağustos 2024].

[46] Uzunparmak, s.1102.

başkanlığı Kararnamesi'nin 3. maddesine göre Cumhurbaşkanlığına bağlı ve kamu tüzel kişiliğini haiz bir kurum olan Siber Güvenlik Başkanlığı'na, kamu ve özel sektör altyapılarına müdahale, veri akışını denetleme ve önleyici güvenlik tedbirleri alma yetkisi tanınmıştır. Bu yetkiler, özellikle "kritik altyapılara siber saldırı ihtimali" gibi soyut gerekçelerle geniş yorumlara açık olup, veri güvenliği ve kişisel mahremiyet açısından hukuki denetim mekanizmalarının zayıflığıyla dikkat çekmektedir.

Nitekim Siber Güvenlik Başkanlığı'nın, kamu kurumlarına "anlık veri iletim yükümlülüğü"[47] getirebilmesi, veri madenciliği tekniklerinin kurumsal düzeyde sistematik kullanılmasına olanak tanımaktadır. Bu kurumların, sadece teknik birimler olarak değil, aynı zamanda "önleyici dijital istihbarat aktörleri" olarak konumlandırılması, makalenin temel iddialarını destekler niteliktedir. Kamu bilgi sistemleri arasındaki entegrasyon (ör. UYAP'ın MERNİS ve POL-NET ile birlikte çalışması), farklı amaçlarla toplanan kişisel verilerin tek bir akışta erişilebilir hale gelmesini sağlayarak profil çıkarma kapasitesini artırmaktadır. Bu nedenle, her bir sistem ve alt uygulama bakımından müstakil düzenleme, erişim yetkilerinin sınırlandırılması ve düzenli denetim mekanizmaları veri koruma rejiminin merkezine yerleştirilmelidir.[48]

Öte yandan Siber Güvenlik Kanunu[49] 6(2) maddesi ile getirilen kişisel verilerin "hukuka ve dürüstlük kurallarına uygun şekilde, doğru ve gerektiğinde güncel olmak kaydıyla, belirli, açık ve meşru amaçlarla, işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmak kaydıyla ve işlendiği amaç için gerekli olan süre kadar muhafaza edilmek üzere işlenir" hükmü, kişisel verilerin korunması açısından oldukça önemli ama yetersiz bir gelişmedir.

İstihbarat birimleri, yetki alanlarına giren iç ve dış tehditlerle ilgili olarak toplanılması gereken verilere ulaşabilmektedir. İstihbarat faaliyetleri kapsamında veri madenciliğine ilişkin ayrıntılı bir düzenleme bulunmaması olağandır. Zira Millî İstihbarat Teşkilatı (MİT) Kanunu 6(b) maddesi uyarınca MİT, "*Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir.*" Benzer şekilde 6(g) madde uyarınca, MİT, telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir. Dolayısıyla toplanılan bu veriler ile potansiyel tehditlerin belirlenmesi ve profilleme yapılması amacıyla çeşitli veri madenciliği tekniklerinin kullanılmasına ilişkin bir sınırlama söz konusu olmayacaktır. Benzer şekilde, Europol Tüzüğü[50] ve Kolluk-Ceza Adaleti Direktifi,[51] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR)[52] 23. maddesi ile Kişisel Verilerin Korunması Kanunu (KVKK)[53] istihbarat faaliyetlerini kapsam dışında bırakmıştır.[54]

2010 yılında Anayasanın 20. maddesine yapılan bir ekleme ile kişisel verilerin korunmasına ilişkin bir hüküm getirilmiştir: "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" Bu çerçevede Kişisel Verilerin Korunması Kanunu tasarısı hazırlanmış ve 2016 yılında kabul edilmiştir.[55] KVKK, "*İstisnalar*" kenar başlıklı 28. maddesinin (ç) ve (d) bentleri, önleyici, koruyucu ve istihbari faaliyetler kapsamında veri madenciliği uygulamalarına izin vermektedir. Maddenin (ç) bendi uyarınca "*kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi*" hukuka uygundur. Ayrıca (d) bendi uyarınca "*kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi*" yine hukuka uygun olacaktır. Bu madde çerçevesinde kolluğun, önleyici faaliyetler kapsamında trol ağı metodu kullanması hukuka uygun mudur?

Bu tartışma, doktrinde ön alan evresi olarak adlandırılan; suçun önlenmesi ile ceza muhakemesi soruşturması arasında kalan gri alana temas etmektedir. Ön alan evresinde somut tehlike bulunmasa dahi kolluğun veri toplama, işleme ve analiz etme pratiklerinin istihbari nitelik taşıdığı kabul edildiğinden, trol ağı taraması gibi yöntemlerin hukuki sınırı özellikle kanunilik, ölçülülük ve denetlenebilirlik ekseninde ayrıksı biçimde tartışılmalıdır.[56]

---

47 7545 sayılı Siber Güvenlik Kanunu, RG: T.19.03.2025, S.32846.

48 Ömer Özkaya ve İbrahim Toprak, 'Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi', *Manas Sosyal Araştırmalar Dergisi* C.11 S.3 (2022), s.1300-1301.

49 7545 sayılı Siber Güvenlik Kanunu, RG: T.19.03.2025, S.32846.

50 2016/794 sayılı Europol Tüzüğü, OJ L 135, 24.05.2016.

51 2016/680 sayılı Kolluk-Ceza Adaleti Direktifi, OJ L 119, 04.05.2016.

52 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), OJ L 119, 04.05.2016.

53 6698 sayılı Kişisel Verilerin Korunması Kanunu, RG: T.07.04.2016, S.29677.

54 Europol Tüzüğü ve Kolluk Ceza Adaleti Direktifi ile KVKK hükümleri arasında benzerlik ve farklar için bk. Enver Kaşli, 'Kolluk Faaliyetlerinde Kişisel Verilerin Korunması: Avrupa Birliği 2016/794 Sayılı Europol Tüzüğü ve 2016/680 Sayılı Kolluk-Ceza Adaleti Direktifi Işığında Bir İnceleme', *Ankara Avrupa Çalışmaları Dergisi* C.22 S.1 (2023), s.111.

55 Oğuz Kaan Pehlivan, 'Kişisel Verilerin Korunması Kanunu ne vadediyor?', *Al Jazeera Turk*, 03 Mayıs 2017, https://www.aljazeera.com.tr/gorus/kisisel-verilerin-korunmasi-kanunu-ne-vadediyor [Erişim 25 Nisan 2024].

56 Özkaya ve Toprak, s.1296.

Kolluk güçlerinin genel olarak tehlikeyi önleme ve suç soruşturma görevi vardır. Bu bakımından *"kolluğun kollama denilen görevi suç-öncesi ve suç-sonrası olarak ikiye ayrılır. Suç-öncesi görev de a) koruma, b) önleme, c) yardım olmak üzere üçe ayrılır."*[57] Ceza muhakemesi kapsamında suç soruşturması ve cezalandırma amaçlanır. Ancak bunun yanında kolluk ileride meydana gelmesi muhtemel *"somut tehlikelerin"* önlenmekle de görevli ve yetkilidir, *"Prensip olarak tehlikenin önlenmesi bakımından genel anlamda hâkim kararı olmaksızın, polisin harekete geçmesi ve tedbir alma yönünde yetkisi vardır."*[58]

Kolluğun, tehlikeyi önleme yetkisi kişilerle ilgili veri toplamasını gerektirir. Bu bağlamda kolluğun birtakım metotlar kullanarak henüz şüpheli olmayan kişilere ilişkin toplanan verileri incelemesi ve analiz etmesi yeni bir yetki olarak karşımıza çıkar. Özellikle öngörücü (predictive) nitelik kazanan gözetim pratikleri, gerçekleşmemiş eylemler üzerinden risk üretmeye yöneldiğinde, masumiyet karinesi ile ifade ve örgütlenme özgürlükleri üzerinde doğrudan baskı yaratabilmektedir.[59] Özellikle yapay zekanın gelişmesi neticesinde günümüzde daha derin bir tehdit söz konusudur. Yapay zeka destekli profilleme, yalnızca daha hızlı tarama anlamına gelmemekte; aynı zamanda bireylerin dijital ayak izlerinden hareketle potansiyel suçlu etiketlemesi üreterek masumiyet karinesini aşındırma, kitlesel gözetim yoğunluğunu artırma ve kara kutu karar süreçleri nedeniyle hukuksal denetlenebilirliği zayıflatma riski taşımaktadır. Bu nedenle, trol ağı benzeri geniş tarama-eşleştirme mekanizmalarında ölçek büyüdükçe, hatanın ve haksız hedeflemenin maliyeti de büyür.[60]

Önleyici kolluk faaliyetlerinde veri toplama ve işleme, pratikte kimlik tespiti, parmak izi, yüz tanıma, elektronik gözetim ve telekomünikasyon yoluyla iletişimin denetlenmesi gibi yöntemlerle somutlaşmaktadır. Veri madenciliği ise bu yöntemlerden gelen çoklu veri akışını eşleştirerek 'risk profili' üretme kapasitesi nedeniyle müdahalenin kapsamını genişletebilmektedir.

Bir başka açıdan kolluk, *"tekrar tanımaya yarayan önleme ve koruma tedbirlerine"* başvurabilir.[61] Bu taktirde ceza adalet sistemine bir şekilde temas eden kişilerden toplanan veriler ileride işlenecek suçların tespitinde kullanılmak üzere önleme amaçlı olarak kayıt altına alınırlar.[62] Genel ifadelerle verilen yetkilerin dışında böylesi özel bir yetkinin kanunla açıkça ve ayrıntılı bir şekilde düzenlenmiş olması gerekmektedir.

Polisin veri toplama ve depolama yetkisine ilişkin olarak Polis Vazife ve Salahiyet Kanunu'na (PVSK)[63] bakmak gerekmektedir. PVSK'nın 5. maddesi, parmak izi ve fotoğrafların kayda alınması, kişisel verilerin toplanması yetkilerini düzenlemektedir. 5. maddede kişisel verilerin parmak izi ve resim şeklinde önleyici hizmet olarak sistematik bir şekilde buna ayrılmış bilgisayar programına kaydedilmesi kabul edilmiştir.[64] Fotoğraf ve parmak izi bilgisayarlarda saklanabilmek ve AFIS adı verilen otomatik parmak izi sorgulamaya imkân veren sistemde parmak izleri kayıtları tutularak buradan veri eşleştirme yapılabilmektedir.[65] PVSK 4(A/1) maddesi ise polise önleme amaçlı kimlik sorma yetkisi verilmiştir. Farklı bir veri toplama yöntemi olan kimlik tespiti ise "kanunlarda sınırlı bir şekilde düzenlenmektedir."[66]

Kolluğa yetki veren bir diğer norm PVSK Ek 7. maddedir. Bu madde ile kolluğa genel yetki kapsamında istihbarat toplama yetkisi verilmiştir. Ayrıca İçişleri Bakanlığına bağlı Kaçakçılık İstihbarat, Harekât ve Bilgi Toplama Dairesi Başkanlığı da kaçakçılıkla mücadele kapsamında veri toplamak ve tasnif etmekle yetkilendirilmiş ve Genel Bilgi Tarama (GBT) uygulaması halini almıştır.

Kolluğa ilişkin yetkilerin farklı metinlere dağılması, veri işleme yöntemleri bakımından öngörülebilirliği zayıflatmakta ve uygulamada sınırların belirsizleşmesine yol açabilmektedir. Bu nedenle görev-yetki-yöntem ilişkisinin kodifiye edilerek daha bütüncül bir kolluk mevzuatı içinde gösterilmesi, kişisel verilerin korunması hakkının güvencesi bakımından da işlevseldir.

Trol ağı metoduyla toplanan verilerden profilleme yapılarak suç delili ya da şüpheliler arasından suçluya ulaşmak mümkün olabilmektedir. Buna göre hedef şahıslar hakkında kamu kurum ve kuruluşlarının veritabanlarından elde edilen veriler, üzerinde çeşitli analiz programlarının çalıştırılabileceği bir veritabanına aktarılmakta, daha sonra bu özel yazılımlar aracılığıyla veriler tasnif edilerek şüpheli profilleri oluşturulmaktadır.[67] Bu süreç literatürde; (i) sayısallaştırılmış gözlemlerin toplanması ve depolanması, (ii) verilerin analiz edilerek farklı davranış/özellikler arasındaki korelasyonların belirlenmesi (veri madenciliği), (iii) farklı zaman dilimlerinde davranış değişkenlerinin çıkarımı şeklinde üç aşamalı bir profilleme mantığıyla açıklanmaktadır.[68] Yapa zekanın gelişmesiyle bu profilleme pratikleri, uygulamada yalnızca basit veri eşleştirme ile sınırlı olmayıp; makine öğrenimi/derin öğrenme (sınıflandırma-regresyon, CNN/RNN), metin tabanlı veriler için doğal dil işleme (NLP), suç örgütleri için sosyal ağ analizi (ör. GNN) ve GIS destekli mekânsal-zamansal modelleme üzerinden tahminsel

---

57 Nurullah Kunter, Feridun Yenisey ve Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı olarak Ceza Muhakemesi Hukuku* (2008), s.445.

58 Yenisey, s.14.

59 Uzunparmak, s.1092.

60 Orkun Konak ve C. Gazi Uçkun, 'Yapay Zekânın Suçla Mücadelede Kişi Profili Oluşturulmasında Kullanımı: Kısa Bir Değerlendirme ve Etik Analiz', *TURAN-SAM Uluslararası Bilimsel Hakemli Dergisi* C.17 S.68 (2025), s.49.

61 Yenisey, s.15; Niyazi Umut Akıncıoğlu, 'Yapay Zekâ Destekli Suç Tahmin Sistemleri: Uygulamadaki Sorunlar ve Hukuki Boyut', *Liberal Düşünce Dergisi* Y.30 S.120 (Güz 2025), s.88.

62 Kunter, Yenisey ve Nuhoğlu, s.958.

63 2559 sayılı Polis Vazife ve Salahiyet Kanunu, RG: T.14.07.1934, S.2751.

64 Yenisey, s.27.

65 Yenisey, s.37.

66 Kunter, Yenisey ve Nuhoğlu, s.966.

67 Ünver, s.408.

68 Özgül, s.90.

polislik çıktıları üretebilecek şekilde de kurgulanabilmektedir.[69,70]

Avrupa Birliği 2016/680 sayılı Kolluk-Ceza Adaleti Direktifi 3(4) maddesi ile GDPR 4(4) maddesi profilleme kavramına yer vermektedir.[71] "*Profil oluşturma*" terimi, bir bireye ait kişisel verilerin otomatik olarak işlenmesini ifade etmektedir. Bu veriler, örneğin çalışanların iş yerindeki performansları, kişilerin ekonomik durumları, sağlıkları, kişisel tercihleri, ilgi alanları, güvenilirlikleri, davranışları, konumları, hareketleri ve daha fazlası dahil olmak üzere söz konusu bireye ilişkin bir dizi faktörü analiz etmek ve/veya tahmin etmek için kullanılabilir.[72] Otomatik bireysel karar verme (*automated individiaul decision-making*) kenar başlıklı 2016/680 sayılı Kolluk-Ceza Adaleti Direktifi 11(1) maddesine göre "*Üye devletler, profil oluşturma da dahil olmak üzere, veri sahibi ile ilgili olumsuz bir hukuki etki doğuran veya veri sahibini önemli ölçüde etkileyen, yalnızca otomatik işleme faaliyetine dayalı bir kararın, kontrolörün tabi olduğu Birlik veya üye devlet hukuku tarafından yetkilendirilmediği ve veri sahibinin hakları ve özgürlükleri için, en azından kontrolörün insan müdahalesi elde etme hakkı olmak üzere, uygun güvenceler sağlamadığı sürece yasaklanmasını sağlar.*" Dolayısıyla, AB hukuku uygun güvenceler ve buna ilişkin somut hukuki yetkiler sağlanmadan, en azından profilleme ve tespit edilen kriminojen niteliklere sahip hedef şahısların gerçekten tehdit olup olmadıkları kararının alınmasını yasaklamıştır.[73] Bu tartışma, profillemenin tahmin boyutu güçlendikçe şüphenin somut olgudan ziyade istatistiksel korelasyonlara kayması riskini de gündeme getirir. Öngörücü sistemlerde birey, fiilî davranışından bağımsız biçimde yaşadığı yer veya ait olduğu grubun istatistiksel özellikleri üzerinden sürekli "şüpheli" konumuna itilebilir; bu da dijital damgalama ve "*digital redlining*" benzeri dışlayıcı etkiler doğurabilir. Avrupa Birliği, bu tür riskleri GDPR'daki otomatik kararlara ilişkin güvenceler (m.22 ve m.15), kolluk bağlamına uyarlanmış Kolluk-Ceza Adaleti Direktifi rejimi ve 12 Temmuz 2024 tarihli Avrupa Birliği Yapay Zeka Yasası'nın (EU AI Act)[74] risk-temelli yaklaşımıyla (insan gözetimi, şeffaflık, denetlenebilirlik vb.) sınırlamaya çalışmaktadır.[75] KVKK kapsamında kolluk bağlamında getirilen istisnaları tam anlamıyla bu maddede açıklanan güvence ve yetkiler kapsamında değerlendirmek oldukça geniş bir yorum olacaktır. Bu çerçevede 7545 sayılı Siber Güvenlik Kanununun kişisel veri işleme yetkilerinin genişliği ve bazı müdahale araçlarında yargısal güvence tartışması, KVKK'nın veri minimizasyonu ve amaca bağlılık ilkeleriyle birlikte okunduğunda uygulamada uyumsuzluk riski doğurabilmektedir.[76]

Bununla birlikte, güvenlik faaliyeti istisnaları veri işlemeyi otomatik olarak meşrulaştıran bir serbestiyet alanı değildir; veri işlemenin meşru bir amaca dayanması ve kullanılan her yöntemin açık bir hukuki dayanağının bulunması gerekir. Bu nedenle, güvenlik faaliyetleri bağlamında kişisel veri işleme yöntemlerini müstakil ve öngörülebilir bir yasal çerçevede toplayan bir düzenleme ihtiyacı devam etmektedir. Dolayısıyla, Türkiye'de KVKK sınırlı bir koruma sağlamaktadır, bunun yerine Kolluk ve Ceza Direktifi benzeri spesifik bir düzenleme yapılması gerekmektedir.

B. Trol Ağı Tarama Metodunun Hukukiliği

1999 tarih ve 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu[77] (mülga) 4. maddesi uyarınca "*Bu Kanunda öngörülen suçların veya delillerinin ortaya çıkarılması için, suçların işleniş biçimlerine benzer tutum ve davranışlarda bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumdaki, Devletin ulusal güvenliği bakımından gizli kalması zorunlu olanlar hariç her türlü resmî ve özel kayıtlarla bilgisayar verileri incelenebilir.*" Yenisey'e göre bu madde "*trol ağı metoduyla veri araştırma*" metodunu göstermektedir: "*Fakat yeni Ceza Muhakemesi Kanunu'nda bu metot düzenlenmemiştir. Bunun için polisin trol ağı gibi bir metotla veri taraması yapması, alması ve kullanma-*

69 Konak ve Uçkun, s.48.

70 Türk hukukunda yapay zekâ destekli kolluk, profilleme ve öngörücü polislik uygulamalarının hukuki boyutu için ayrıca bkz. Aytaç Çetinkaya, 'Yapay Zekâ Destekli Kolluk Uygulamalarında İdarenin Hukuki Sorumluluğu', *Bilişim Hukuku Dergisi* C.6 S.2 (2024), s.508-548; Onur Kaplan, 'İdari Kolluk Faaliyetlerinde Dijital Dönüşümün Etkileri ve Sınırları: İki Artı İki Beş Eder Mi?', *Bilişim Hukuku Dergisi* C.7 S.1 (2025), s.46-78; Zafer İçer, 'Yapay Zekâ Temelli Önleyici Hukuk Mekanizmaları-Öngörücü Polislik', *Yapay Zekâ Çağında Hukuk* (İstanbul Barosu, 2021), s.30-48; Rifat Karatay, 'Kolluğun Önleyici Faaliyetler Kapsamında Kişisel Veri İşlemesi', ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, *Kişisel Verilerin Korunmasına Uzman Bakış* (KVKK, 2023), s.329-361. Profilleme ve otomatik karar alma bakımından bkz. Irmak Erdoğan, *Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri* (Seçkin, 2022); Neslihan Kavak Güven, *Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Profilleme ve Otomatik Karar Alma* (On İki Levha, 2022).

71 GDPR ve Ceza Adaleti Direktifi aynı tanımı kullanmaktadır: "profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;" "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA," 119 Official Journal of the European Union (2016); "Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," L 119/1 Official Journal of the European Union (2016); Oliver Radley-Gardner, Hugh Beale and Reinhard Zimmermann (eds), *Fundamental Texts on European Private Law* (Hart Publishing, 2016).

72 Can, s.129; çevrimiçi davranışlardan profil çıkarma ve bunun hedefleme/ayrımcılık/manipülasyon riski doğurabileceğini dair bkz: Sağır ve Albayrak, s.78.

73 ABAD'ın 20 Eylül 2022 tarihli *SpaceNet ve Telekom Deutschland* kararı, supra dn.34.

74 2024/1689 sayılı Avrupa Birliği Yapay Zeka Yasası, OJ L, 2024/1689, 12.07.2024. Polis Vazife ve Salahiyet.

75 Akıncıoğlu, s.88,92,97.

76 Uzunparmak, s.1104.

77 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, RG: T.01.08.1999, S.23773.

sı hukuken mümkün değildir. Fakat gerçekte bu konu yapılıyor mu yapılmıyor mu, bu konuda bir açıklık bulunmamaktadır."[78]

Gerçekten de bu düzenlemeye göre dar kapsamlı bir şekilde profilleme olan PVSK Ek 7. maddesi uyarınca "*Polis; Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere; ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar.*" Ayrıca "*kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşların ihtiyaç duyulan bilgi ve belgelerinden yararlanabilmek için gerekçesini de göstermek suretiyle yazılı talepte bulunulabilir.*"

Öte yandan 2018 yılında PVSK 26. maddesine getirilen ek düzenleme kolluk kuvvetlerine sanal devriye yetkisi getirilmiştir; "*Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir.*" Ancak Anayasa Mahkemesi 19.02.2020 tarihli (E.2018/91, K.2020/10) kararıyla, polise sanal ortamda gözetim ve denetim yetkisi tanıyan bu düzenlemeyi iptal etmiştir. Mahkeme, söz konusu hükmün bireylerin özel hayatına müdahale niteliğinde olduğunu ve "*müdahalenin sınırlarını belirleyen açık ve net yasal düzenlemelerin bulunmadığını*" vurgulamıştır.[79] Gözetim altında olma hissinin bireyleri oto-sansüre yöneltebildiği ve bu nedenle ifade özgürlüğünün kullanımını pratikte daraltabildiği dikkate alındığında, dijital gözetim yetkilerinin ancak açık/öngörülebilir sınırlar ve ölçülülük güvenceleriyle kurgulanması gerekir.

Bu karar, kolluk güçlerinin önleme amacıyla dijital gözetim yaparken sahip olması gereken *yasal yetki, amaç-açıklık, ölçülülük ve denetim ilkeleri* açısından temel bir içtihat niteliğindedir. AYM'nin sanal devriye kararında vurguladığı açıklık ve öngörülebilirlik ihtiyacı, dijital gözetim literatüründe kanunilik ilkesinin tek başına yasal dayanakla sınırlı görülmeyip, erişilebilir-öngörülebilir çerçeve, bağımsız denetim ve etkili başvuru güvenceleriyle birlikte ele alınması gerektiği yaklaşımıyla paraleldir.[80] Türkiye'de veri madenciliği temelli uygulamalarda olduğu gibi, sanal devriye yetkisi de hedef gözetmeksizin veri toplama ve izleme riskini barındırdığı için, söz konusu iptal kararı, makalede savunulan "*öngörülebilir ve denetlenebilir bir yasal çerçevenin zorunluluğu*" görüşünü pekiştirir niteliktedir.

Öte yandan 6698 Sayılı Kişisel Verilerin Korunması Kanununun "*önleyici, koruyucu ve istihbari faaliyetler*" kapsamında getirdiği istisnalar, 28/ç ve 28/d maddelerinde düzenlenmiştir. Buna göre, millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenlik amaçlarıyla yetkilendirilmiş kamu kurum ve kuruluşları tarafından yapılan veri işleme faaliyetleri hukuka uygundur. Benzer şekilde AB hukukunda, kamu güvenliği/ulusal güvenlik gibi amaçlarla veri koruma rejimine getirilecek sınırlamalar GDPR m.23'te açıkça düzenlenmiş; bu sınırlamaların temel haklarla dengeli, ölçülü ve güvenceli bir yasal çerçeve içinde kurgulanması gerektiği kabul edilmiştir.[81]

Dijital gözetimin yalnızca yasal dayanağa sahip olması tek başına yeterli değildir; ayrıca bu uygulamaların kanunilik, meşru amaç ve ölçülülük ilkeleri çerçevesinde yürütülmesi ve denetlenmesi gerekir. Dolayısıyla bu istisnaların evrensel veri koruma ilkeleriyle uyumlu hale getirilmesi gerekmektedir. Bu uyumun yalnızca ilke düzeyinde kalmaması; kolluk ve istihbaratın kişisel veri işleme pratikleri bakımından etkin iç/dış denetim mekanizmalarıyla desteklenmesi gerekir; aksi hâlde istisna rejimi hak ihlallerini derinleştirebilir.[82] Evrensel veri koruma ilkeleri; şeffaflık, amaca uygunluk, verinin asgari düzeyde toplanması, doğruluk, süreli saklama, verinin bütünlüğü ve gizliliğinin korunması gibi prensipleri kapsamaktadır. Bu bağlamda, gözetim araçlarının amaç dışı ve süreklilik arz edecek şekilde kullanımı, kişisel verilere erişim ve işleme üzerinden özel hayatın gizliliği bakımından ihlal riskini büyütür. Dolayısıyla, güvenlik gerekçesiyle kurulan sistemlerde dahi amaçla sınırlılık ve zaman bakımından sınır (saklama süresi/erişim süresi) somutlaştırılmadıkça ilke düzeyi koruma pratikte zayıflamaktadır.[83] Örneğin, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)'ne göre, veri işleme faaliyeti açık bir meşru amaca dayanmalı ve bireylerin temel haklarıyla dengelenmelidir. GDPR'daki "*amaca uygunluk*" ilkesi, veri işlemenin belirli, açık ve meşru bir amaca yönelik olması gerektiğini ifade eder. Öte yandan, "*veri minimizasyonu*" ilkesi ise sadece gerekli olan verilerin toplanmasını öngörmektedir.

Saklama süresi ve silme prosedüründeki belirsizlik, güvenlik veri tabanlarında tipik bir hak ihlali kaynağıdır. Nitekim idari veri tabanlarında kayıtların ne kadar süre tutulacağına dair belirsizlik ve silme işlemlerindeki gecikmeler, kişinin özgürlüğü ve diğer haklarını kullanımı üzerinde doğrudan sonuçlar üretebilmektedir; benzer risk, 'trol/şüpheli hesap' listeleri gibi veri madenciliği çıktılarının uzun süre saklanması halinde de ortaya çıkacaktır.[84]

Bunun yanı sıra GDPR 23. maddesinde; millî güvenlik, kamu güvenliği ve suçların önlenmesi gibi belirli amaçlarla veri koruma rejimindeki bazı yükümlülük ve hakların "*yasama tasarrufu*" ile sınırlandırılabilmesine izin vermekle birlikte, bu sınırlandırmanın temel hakların özüne saygılı olması ve

[78] Yenisey, s.38.

[79] AYM T.19.2.2020, E.2018/91, K.2020/10, para. 89 vd.

[80] Uzunparmak, s.1106.

[81] Atlı, s.18.

[82] Atlı, s.16-21.

[83] Özkaya ve Toprak, s.1298.

[84] Özkaya ve Toprak, s.1300.

demokratik toplumda zorunlu ve orantılı bir tedbir olarak kurgulanması şartını aramaktadır. Bu nedenle AB hukukunda istisna/sınırlama rejimi, soyut bir yetkilendirmeden ziyade kapsamı, amacı, kişi kategorilerini, erişim-saklama sınırlarını ve denetim güvencelerini somutlaştıran bir güvence paketi mantığıyla işletilmektedir. Bu çerçevede, Türkiye'deki uygulamaların bu ilkelerle uyumlu olması için somut düzenlemelere ihtiyaç vardır. AB'de risk-temelli yaklaşım kapsamında, yüksek riskli gözetim sistemleri için kamu otoritelerine temel haklara etki analizi yükümlülüğü getirilmesi, istisnaların soyut yetki olmaktan çıkarılıp ölçülebilir ve denetlenebilir güvencelere bağlanmasına örnek teşkil etmektedir.[85]

Bununla birlikte Anayasa'nın 20. maddesi, bireylerin kişisel verilerinin ancak açık rızaları veya kanunda öngörülen durumlarda işlenebileceğini açıkça belirtmektedir. Örneğin, Anayasa Mahkemesi'nin (AYM) 2014/74 Esas ve 2014/201 Karar sayılı 25.12.2014 tarihli kararında, kişisel verilerin hukuka aykırı işlenmesinin temel hak ihlali oluşturduğu belirtilmiştir. Kararın gerekçesinde yer alan açıklamalar oldukça dikkat çekici ve yol göstericidir:

> *"Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi; daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması; verilere erişim ve veri transferinin kolaylaşması; kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler, günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, 'Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.' hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır."*

İleri sürdüğümüz hukuka uygun bir düzenleme ve denetim mekanizması oluşturulmasının gerekliliğini AYM 2014 yılında dile getirmiştir. AYM kararında bireylerin özel hayatlarına ilişkin bilgilerin izinsiz toplanmasının ve işlenmesinin Anayasa'ya aykırı olduğunu, dolayısıyla hukuka uygunluk koşullarının açıkça tanımlanması gerektiğini belirmektedir. Mahkeme, kişisel verilerin işlenmesi sürecinde kamu otoritelerinin keyfi uygulamalarının önlenmesi için güçlü yasal güvencelerin gerekli olduğuna işaret etmiştir. Karar, birey haklarının korunması açısından örnek bir yaklaşım sunarak, veri işleme faaliyetlerinin ölçülü, amaca uygun ve açık rıza temelinde yapılması gerektiğini şart koşmaktadır. Aradan geçen on yılı aşkın süreye rağmen tek ilerleme sayılabilecek düzenleme yukarıda değindiğimiz KVKK'nın istisnalara ilişkin maddeleridir. Ancak bu maddeler trol ağı niteliğindeki toptancı bir veri toplama pratiğine ilişkin özel bir düzenleme getirmemektedir.

Benzer şekilde, AİHS'nin 8. maddesi, *"herkesin özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkını"* güvence altına almaktadır. Avrupa İnsan Hakları Mahkemesi'nin (AİHM), *Klass ve Diğerleri v. Almanya* davasında verdiği kararda, bireylerin telefon görüşmelerinin izlenmesinin sadece zorunlu ve ölçülü olduğu durumlarda hukuka uygun bulunabileceği belirtilmiştir.[86] Ayrıca, *S. ve Marper v. Birleşik Krallık* davasında AİHM, polis tarafından alınan DNA ve parmak izi verilerinin süresiz saklanmasının, bireyin özel hayatına orantısız bir müdahale teşkil ettiğini kararlaştırmıştır. Öyle ki, AİHM'e göre *"Yeni teknolojilerin gelişiminde öncü rol oynama iddiasında olan her ülke bu alanda adil bir denge bulma özel sorumluluğunu taşımaktadır."*[87] *Roman Zakharov v. Rusya* davasında ise, geniş çaplı telefon dinleme sistemlerinin, yeterli yasal ve pratik güvenceler olmadan uygulanmasının AİHS'nin 8. maddesini ihlal ettiği hükmüne varılmıştır. Aynı davada Mahkeme böylesi geniş bir yetkinin kötüye kullanılmasını önlemek için yasada belirtilmesi gereken aşağıdaki asgari güvenceler geliştirmiştir: dinleme emrine yol açabilecek suçların niteliği belirlenmelidir; telefonlarının dinlenebileceği kişi kategorileri tanımlanmalıdır; telefon dinlemesinin süresine ilişkin sınır tespit edilmelidir; elde edilen verilerin incelenmesi, kullanılması ve saklanması için izlenecek prosedür açıklanmalıdır; veriler diğer taraflara iletilirken alınacak önlemler; ve kayıtların silinebileceği veya yok edilebileceği durumlar belirlenmelidir.[88]

Türkiye'de kolluğun veri toplama ve genel anlamda farklı kamu kurumlarının veri tabanlarındaki bilgilere sınırlı bir şekilde erişebilme yetkisi bulunmaktadır. Öyle ki, Ceza Muhakemesi Kanunu[89] *"Cumhuriyet savcısının görev ve yetkileri"* başlıklı 161. maddesinin (1), (2) ve (4) numaralı fıkralarına göre Cumhuriyet savcısı doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir, adli soruşturmayla ilgili sonucu ulaşabilmek için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir. Dolayısıyla, Kanun'da yargı mercilerine, anılan görevin yerine getirilmesini sağlayabilecek bilgiler de dahil

[85] Uzunparmak, s.1103.

[86] *Klass and Others v. Germany*, App no. 5029/71 (ECtHR 06.09.1978).

[87] *S. and Marper v. the United Kingdom*, 30562/04, 30566/04 (ECtHR [GC] 04.12.2008).

[88] *Roman Zakharov v. Russia*, App no. 47143/06 (ECtHR [GC] 04.12.2015).

[89] 5271 sayılı Ceza Muhakemesi Kanunu, RG: T.17.12.2004, S.25673.

olmak üzere suç soruşturmasıyla ilgili bilgilere erişme yetkisinin de tanındığı görülmektedir. Ancak kamu kurum ve kuruluşları dışındaki kurumlarda örneğin şirket veritabanlarına (özel veritabanlarına) erişim söz konusu olduğunda kolluğa, 4422 sayılı kanunda olduğu gibi açık bir yetki verilmemiştir. Denilebilir ki, yargı kararı ile özel veritabanlarına erişim yetkisi verilmiş olabilir. Bu durumda da kolluğun yine de trol ağı metodu ile veri depolaması ve analiz yapma yetkisi açıkça bulunmamaktadır. Zira Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere

> "*... adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler...*" kişisel veri olarak kabul edilmektedir.[90]

Bu bilgilerin sistematik olarak analizini yapmak, veri madenciliğini kullanmak yetkisini beraberinde getirmektedir. Dolayısıyla, AYM, AİHM kararları, GDPR ve evrensel veri koruma ilkeleri dikkate alınarak kişisel verilerin kolluk tarafından herhangi bir yargı mercinin kararı olsa dahi kanunla ayrıntılı bir şekilde düzenlenmesi gereken böylesi bir özel yetkiyi kullanamaz.

Özellikle pek çok terör soruşturmasında şüpheli şahısların kullandığı telefonların tespit edilmesi yöntemi, trol ağı metodunun ya da en azından bilgisayar eşleştirmesi metodunun kullanıldığına işaret etmektedir. Zira sadece kamu kurum ve kuruluşlarının veritabanlarından değil, özel veritabanlarından da verilerin elde edildiği görülmektedir. Soruşturma aşamasında Savcılık kararıyla, kovuşturma evresinde ise hâkim kararıyla binlerce ceza yargılamasında dosyaya eklenen ve aşağıda ayrıntılarına yer vereceğimiz evraklar, çerçevesi hukuken kesin bir şekilde belirlenmemiş bir trol ağı tarama metodunun uygulandığını apaçık ortaya koymaktadır. Kişisel verilerin korunması amacıyla evraklarda yer alan isim, soyisim, kimlik numarası ve telefon numaraları ile e-mail adresleri usulüne uygun şekilde karartılmıştır.

Şekil 1'e göre hedef şahıslara ait olduğu düşünülen telefon numaraları i) tespit edilenler "T" harfiyle, ii) hedef şahıs tarafından diğer kurum ve kuruşlara beyan edilen "B" harfiyle, iii) hedef şahsın abonelik kapsamında verdikleri "A" harfiyle gösterilmiş ve veri tabanlarından çekilmiştir.

HEDEF ŞAHSIN NUMARASININ/NUMARALARININ KAYNAK LİSTESİ

HEDEF ŞAHSIN NUMARASI	KAYNAK TİPİ(ABONE, BEYAN, TESPİT)
505	B
507	B
531	A,B
537	B
538	B
542	B

•Tespit edilen telefon numaraları 'T' ile gösterilmektedir. Savcılıklarca/Mahkemelerce şüpheli/sanık tarafından kullanıldığı tespit edilen telefon numaraları gösterilmektedir.

•Beyan edilen telefon numaraları 'B' ile gösterilmektedir. Soruşturma kapsamında alınan veriler ile Daire Başkanlığımız bünyesinde bulunan veri kalemleri içerisinde yer alan telefon bilgileri gösterilmektedir.

•Abonesi olunan telefon numaraları "A" ile gösterilmektedir. Ankesör / büfe HTS havuzunda bulunan baz ve karşıbaz tablolarındaki diğer numara hanesinde yer alan BTK kayıtlarındaki abonelik bilgilerinden gelen telefon numaraları gösterilmektedir.

Şekil 1. Hedef Kişinin Telefon Numaralarının Kaynağı

Şekil 2'ye göre, Savcılıklar/Mahkemeler tarafından hedef kişinin kullandığı tespit edilen telefon numarası/numaraları, hedef kişinin/kişilerin beyan ettiği telefon numarası/numaraları ve BTK (Bilgi Teknolojileri ve İletişim Kurumu) tarafından HTS[91] havuzundaki diğer kayıtlarda hedef kişinin/kişilerin abone olduğu bildirilen telefon numarası/numaraları yukarıdaki tabloda gösterilmektedir.

[90] AYM T.09.04.2014, E.2013/122, K.2014/74; T.02.10.2014, E.2014/149, K.2014/151; T.25.12.2014, E.2014/74, K.2014/201; T.19.03.2015, E.2014/180, K.2015/30; T.12.11.2015, E.2015/32, K.2015/102.

[91] Historical Traffic Search (HTS); arama trafiği tarihçesi ya da arama trafiği kayıtları.

HEDEF ŞAHSIN NUMARASININ/NUMARALARININ TESPİT / BEYAN / ABONE LİSTESİ

BEYAN EDİLEN VE DAİRE BAŞKANLIĞIMIZCA DÜZELTİLEN TELEFON NUMARASI	BEYAN EDİLEN ADSOYAD	TESPİT EDİLEN / BEYAN EDİLEN / ABONESİ OLUNAN ORİJİNAL TELEFON NUMARASI	TESPİT EDİLEN / BEYAN EDİLEN / ABONESİ OLUNAN KİŞİ BİLGİSİ	TESPİT EDEN / BEYAN EDİLEN KURUM	TESPİT / BEYAN TARİHİ	TİP A:ABONE B:BEYAN T:TESPİT
505		90505	T.C. (Kendisi)(Kendisi)	OSYM	13.02.2012	B
505		90505	T.C. (Kendisi)(Kendisi)	OSYM	13.02.2012	B
505		505	T.C. (Babası)	MHRS TELEFON	16.02.2022	B
505		505	T.C. (Babası)	ELEKTRİK ABONE TELEFON		B
542		+90-542	T.C. (Kendisi)(Kendisi)	EGM-GERÇEK ŞAHIS-Sürücü Belgesi	19.11.2020	B
542		542	T.C. (Kendisi)(Kendisi)	DOĞALGAZ ABONE TELEFON		B

• Hedef şahıs tarafından kullanıldığı Savcılıklar/Mahkemeler tarafından tespit edilen telefon numarası/numaraları ile hedef şahıslarca beyan edilen telefon numarasını/numaralarını beyan eden diğer şahıs/şahıslar ve hedef şahısların HTS havuzunda yer alan kayıtlarında abonesi olduğu BTK tarafından bildirilen telefon numarası/numaraları yukarıdaki tabloda gösterilmiştir.

Şekil 2. Hedef kişinin telefon numaralarının kamu veri tabanlarından çıkarılması

Şekil 1 ve Şekil 2'ye göre hedef şahısın kullandığı düşünülen telefon numaraları; ÖSYM, Merkezi Hekim Randevu Sistemi (MHRS), Elektrik, Doğalgaz ve Su abonelik sistemleri, Pasaport ve sürücü belgesi sistemlerinde beyan edilen numaralarla karşılaştırılarak tespit edilmiştir. Bu sistemlerin kamu kurum ve kuruluşlarına ait olması dolayısıyla herhangi bir tereddüt yaşanmayacaktır. Zira PVSK kapsamında polis bu veritabanlarından talepte bulunabilmekte ya da veritabanlarına erişim sağlayabilmektedir. Öte yandan söz konusu evrakların devamında, Şekil 3'te görüleceği üzere *Dominos*, *Çiçeksepeti*, *Hepsiburada*, *McDonalds*, *Little Caesars*, *Sahibinden.com* gibi özel şirketlerin veritabanlarından elde edilen verilere de yer verilmektedir.

531		531	T.C. (Ad Soyad Bilgisi Bulunamadı)	DOMINOS_VERILERI	13.12.2013	B
531		531	T.C. (Ad Soyad Bilgisi Bulunamadı)	CICEKSEPETI_VERILERI	09.02.2016	B
531		0-531	T.C. (Ad Soyad Bilgisi Bulunamadı)	SAHIBINDEN_VERILERI	05.12.2015	B
531		531	T.C. (Ad Soyad Bilgisi Bulunamadı)	MCDONALDS_VERILERI	04.11.2015	B
531		531	T.C. (Ad Soyad Bilgisi Bulunamadı)	LITTLECAESARS_VERILERI		B
53		538	T.C. (Ad Soyad Bilgisi Bulunamadı)	HEPSIBURADA_VERILERI	26.05.2008	B

Şekil 3. Hedef kişinin telefon numaralarının özel veri tabanlarından çıkarılması

Gerek savcılık kararıyla gerekse hâkim kararıyla kolluğun kamu kurum ve kuruluşları veritabanlarının yanı sıra şirketlere ait veritabanlarından da verilerin toplanması, trol ağı tarama metodunun uygulandığını göstermektedir. Benzer şekilde Şekil 4'te yer verilen başka bir evrakta "*... isimli hedef şahıs tarafından Genelkurmay PBS ve soruşturma kapsamında temin edilen ÖSYM, AÖF, MEB, Elektrik, Doğalgaz, DASK, e-fatura, İstanbul Organize Şube verileri ile pasaport, ehliyet, noter işlemlerinin yapıldığı resmî kurumlara beyan edilen GSM hat/hatları:*" açıklaması sonrasında hedef şahsa ait farklı veritabanlarından elde edilen telefon numaralarına yer verilmektedir. Ancak her ne kadar açıklamada "resmî kurumlara beyan edilen" denilse de Morhipo, Madamecoco, Sahibinden.com, Modanisa, vb. şirketlerin veritabanlarına da erişecek şekilde trol ağı taraması uygulandığı görülmektedir.

Daha tedirgin edici olan ise, böylesi teknik bir kapasiteye sahip olan kolluğun sadece hedef şahıslarla *sınırlı* bir veri toplama faaliyeti yapıp yapmadığı ve trol ağı tarama metoduyla ülke çapında kamu-özel tüm veritabanlarına erişebilen kolluğu herhangi bir şekilde denetleyebilecek hukuki düzenlemelerin olmamasıdır.

A) [redacted] T.C.No: [redacted]) isimli şahıs tarafından Genelkurmay PBS ve soruşturma kapsamında temin edilen ÖSYM, AÖF, MEB, Elektrik, Doğalgaz, DASK, e-fatura, İstanbul Organize Şube Md. verileri ile Pasaport, Ehliyet, Noter işlemlerinin yapıldığı resmi kurumlara beyan edilen GSM hat / hatları;

TCKN	AD SOYAD	TELEFON	E-MAIL	ÜYELİK TARİHİ	KAYNAK
		545	@ho tmail.de	2017-07-25 11:46:19.3700000	MORHIPO
		545			MADAMECO CO
		545			ISTANBUL GARNIZON KOM.
		545	@ gmail.com	2016-11-12 00:00:00.0000000	SAHIBINDEN
		545		20.02.2015 10:05	OSYM
		545	@hotm ail.com	2014-07-30 11:07:34.0000000	MODANISA
		553			ISTANBUL GARNIZON KOM.
		553		7.03.2013	POLNET
		553	@ gmail.com	2012-10-12 14:15:53.3866667	MORHIPO
		553		20.03.2013 21:49	OSYM
		553		6.02.2014 14:16	OSYM

Şekil 4. Hedef kişinin telefon numaralarının diğer özel veritabanlarından çıkarılması

Öte yandan acaba bu faaliyetleri, PVSK Ek 7. maddesi uyarınca "*... ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir...*" cümlesi içerisinde yorumlamak mümkün olabilir mi? sorusu sorulabilir. Fakat bu soruya *evet* diyebilmek söz konusu maddenin lafzen ve manen oldukça geniş ve keyfi bir şekilde yorumlanması olacaktır. Zira Anayasanın 13. maddesi uyarınca temel hak ve hürriyetler, *özlerine dokunulmaksızın* yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve *ancak kanunla sınırlanabilir*. Trol ağı tarama metodu gibi şüphelilerin yanı sıra masum insanların da bireysel hak ve özgürlüklerini sınırsız ve keyfi bir şekilde, özlerine dokunarak sınırlayan bir uygulama sadece bir yorum ile açıklanamaz. Dolayısıyla, kolluk güçlerine 4422 sayılı kanunda olduğu gibi bir yetki tanımlaması yapılması ve bunun sınırlarının çizilmesi hem kolluk hem de kişisel verilerin korunması açısından hukuki güvence ve istikrar sağlayacaktır. Halihazırda böylesi bir yetkilendirmenin ve denetim mekanizmalarının bulunmaması hukuksuz fiili bir durumu yaratmakta, hak ihlali oluşturmaktadır.

Şen, trol ağı metodu "*denilen toptancı bir bakış açısı ile yapılacak delil toplama ve değerlendirme sonucunda suçun ve failinin belirlenmesi yönteminin hukuka aykırı*" olduğunu ifade etmektedir.[92] Nitekim "*trol ağı*" metodunun bir delil elde etme yöntemi olamayacağı, Yargıtay Ceza Genel Kurulu kararıyla da ortaya koyulmuştur. Yargıtay, trol ağı tarama metodunun, şüpheli ve sanıklar dışındaki kişilerin verilerine erişim sağlayan uygulamalarını hukuka aykırı bulmuştur. Karara göre "*günün belli bir zaman diliminde baz istasyonundan görüşme yapan tüm abonelere ait açık adres ve kimlik bilgilerini kapsayacak şekilde arayan ve aranan dökümlerine ilişkin bilgilerin dökümü iletişimin tespiti işlemidir. Tüm suçlar yönünden bu tedbire başvurma olanağı bulunduğundan, işlendiği iddia olunan hırsızlık suçu yönünden iletişimin tespiti kararı verilmesi olanaklı ise de hakkında tedbir kararı verilen kişiler yönünden tedbir kararının isabetli olup olmadığının belirlenmesi gerekmektedir. İletişim tespiti ancak, şüpheli ve sanık hakkında uygulanabilir. Haklarında iletişimin tespiti tedbiri talep edilen kişiler, baz istasyonundan hizmet alan üçüncü kişiler*

[92] Ersan Şen ve Buğra Şahin, 'Ankesörlü veya Sabit Hattan Ardışık, Periyodik ve Tekil Arama', *Ersan Şen Hukuk ve Danışmanlık*, 01.04.2021, https://sen.av.tr/tr/makale/ankesorlu-veya-sabit-hattan-ard%C4%B1ş%C4%B1k-periyodik-ve-tekil-arama [Erişim 20 Nisan 2024].

olup, şüpheli veya sanık sıfatına sahip olmadıklarından haklarında iletişimin tespiti tedbirine başvurulması olanağı yoktur."[93]

Dolayısıyla, Yargıtay bir baz istasyonuna bağlanan tüm abonelere ait açık adres, kimlik bilgileri ve arama dökümlerinin çıkarılmasını şüpheli ve sanık ile masum kişiler arasında ayrım gözetilmeden yapıldığı (trol ağı tarama metodu) için kabul edilemez bulmuştur. Özellikle terörle mücadele bağlamında istatistiksel çıkarımlara dayalı kara listeler, gerçekte terör bağlantısı bulunmayan kişilerin dahi (örneğin) seyahat hakkının engellenmesi gibi aleyhe sonuçlar doğurabileceğinden, 'geniş tarama' pratikleri hak temelli bir daraltma ve güvencelendirme rejimi gerektirir.[94] Dolayısıyla bu noktada suçla mücadele çerçevesinde bir sınırlama yapılmaktadır. Ancak her ne kadar kişisel hak ve özgürlükler bakımından geri dönülemez sonuçlara yol açacağı tartışmasız olsa da gerçek suçlu ile masumların ortaya çıkarılması noktasında faydalı sonuçlar alınabilecektir. Zira aksi durumda ankesörlü hatlardan yapılan aramalarda aramayı gerçekleştiren gerçek suçlunun tespiti akim bırakılmaktadır. Oysa aramanın gerçekleştiği zaman dilimiyle o bölgedeki baz istasyonundan sinyal veren kişilerin tespiti trol ağı tarama metoduyla kolaylıkla gerçekleştirilebilecektir. Son tahlilde, kolluğun gerek önleyici gerek adli süreçler kapsamında trol ağı tarama metodu kullanımına ilişkin olarak müstakil bir düzenlemeye ihtiyaç vardır.

Türkiye'de önleyici veri madenciliğinin anayasa yargısındaki izini en somut biçimde gösteren güncel içtihatlardan biri, Anayasa Mahkemesi'nin 8 Mart 2023 tarihli ve 2020/16168 sayılı bireysel başvuru kararıdır. Karara konu olayda başvurucu, FETÖ/PDY'nin askerî mahrem yapılanmasına üyelik suçundan, büyük ölçüde ankesörlü/kontörlü sabit hatlardan yapılan aramalara ilişkin HTS (Historical Traffic Search - Arama Trafiği Geçmişi) kayıtlarına ve bu kayıtların kolluk tarafından yapılan teknik analizine dayanılarak mahkûm edilmiştir. Başvurucu, iletişimin tespitine ilişkin kayıtların hukuka aykırı biçimde elde edildiğini ve mahkûmiyette tek veya belirleyici delil olarak kullanıldığını ileri sürerek adil yargılanma hakkının ihlal edildiğini iddia etmiştir.[95]

Anayasa Mahkemesi, kendi görevinin delillerin hukuka uygun elde edilip edilmediğini bizzat tespit etmek olmadığını; yalnızca ilk bakışta ya da derece mahkemelerince hukuka aykırı olduğu belirlenen delillerin tek veya belirleyici delil olarak kullanılıp kullanılmadığını ve bunun yargılamanın bütününe etkisini denetlemek olduğunu vurgulamıştır. Bu çerçevede Mahkeme, Başsavcılığın hâkim kararı doğrultusunda ankesörlü/kontörlü hatlara ilişkin HTS kayıtlarını BTK'dan getirtmesini ve bu kayıtlar üzerinde 'şüpheli olabilecek kişilerin tespiti amacıyla' kolluk birimlerince teknik analiz yapılmasını 'bariz takdir hatası veya açık bir keyfîlik içeren bir uygulama' olarak değerlendirilemeyeceği sonucuna varmış ve başvuruyu kabul edilemez bulmuştur.

Bu karar, çalışmanın temel iddiası bakımından çift yönlü bir öneme sahiptir. Bir yandan, henüz somut bir suç şüphesi kişiselleşmeden önce ülke genelinde geniş bir abone kütlesine ait iletişim verilerinin toplanıp 'soruşturma konusu suçla ilgisi bulunmayan kişiler elendikten sonra' şüpheliye ulaşılması yönteminin -ki bu tam olarak trol ağı tarama mantığıdır- anayasa yargısı önünde meşru sayıldığını göstermektedir. Öte yandan Mahkeme, yöntemin kendisini kanunilik, öngörülebilirlik ve ölçülülük ölçütleri açısından bağımsız biçimde denetlemek yerine, Yargıtay'ın istikrar kazanmış kabulüne atıf yaparak 'açık keyfîlik' eşiğinin aşılmadığını saptamakla yetinmiştir. Böylece kitlesel HTS taramasının önleyici-adli ayrımını belirsizleştiren yapısı ile 'ön alan evresi'nde toplanan verilerin sonradan ceza muhakemesi deliline dönüşmesi sorunu esaslı bir anayasal denetime tabi tutulmamıştır. BVerfG'nin somut tehlike eşiği ve ABAD'ın hedefli saklama ölçütü etrafında ördüğü güvence rejimiyle karşılaştırıldığında, Türk anayasa yargısının bu alandaki denetim yoğunluğunun görece düşük kaldığı; öngörücü polislik pratiklerinin barındırdığı hata ve ölçüsüzlük riskini karşılamaya elverişli, öngörülebilir ve denetlenebilir bir çerçevenin hâlâ mevcut olmadığı görülmektedir.[96]

Sonuç

Bilişim teknolojileri günümüzde hayatın her alanına derinlemesine nüfuz etmiştir. Akıllı cihazlar aracılığıyla günlük hayatta sıkça kullandığımız e-posta adresleri, sosyal medya hesapları ve diğer uygulamalar kullanıcılar hakkında çeşitli veriler toplamaktadır. Bu durum, kişisel veri paylaşımını aşan bir boyuta ulaşmıştır; artık bireyler, gündelik yaşamlarından paylaşımlar yaparak veri ve bilgi akışına katkıda bulunmaktadır. Bu bağlamda, kamu kurumları ve özel sektör her gün büyük miktarlarda veri toplamakta ve depolamaktadır. Ancak bu veri bolluğu düzensizdir ve işlenmeye ihtiyaç duyar. Verilerin işlenmesi ve anlamlı bilgilere dönüştürülmesi büyük bir sorun olarak karşımıza çıkmaktadır.

Veri madenciliği, bu sorunu çözmek için bir araç olarak ortaya çıkmıştır. Bu teknik, var olan veri tabanlarını koordineli bir şekilde kullanarak yenilikçi çözümler sunmayı amaçlar. Veri madenciliği, eğitimden ticarete, mühendislikten bankacılığa kadar geniş bir

[93] Yargıtay CGK T.15.11.2011, E.2011/6-140, K.2011/222, (Kazancı İçtihat Bilgi Bankası).

[94] Özgül, s.91.

[95] Anayasa Mahkemesi (Genel Kurul), Murat Albayrak Başvurusu, B. No: 2020/16168, 8/3/2023 (RG: T.23.5.2023, S.32199).

[96] Devlet eliyle yürütülen veri madenciliğinin bir yasal çerçeveye olan ihtiyacı için bkz. Fred H. Cate, 'Government Data Mining: The Need for a Legal Framework', *Harvard Civil Rights-Civil Liberties Law Review* Vol.43 (2008), s.434-489. Öngörücü polislik ve gözetim teknolojilerinin anayasal sınırları konusunda bkz. Christopher Slobogin and Sarah Brayne, 'Surveillance Technologies and Constitutional Law', *Annual Review of Criminology* Vol.6 No.1 (2023), s.219-240; Andrew Guthrie Ferguson, 'Policing Predictive Policing', *Washington University Law Review* Vol.94 No.5 (2017), s.1109-1189. Mahremiyet-güvenlik dengesine ilişkin 'saklayacak bir şeyi olmama' argümanının eleştirisi için bkz. Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011).

yelpazede uygulama alanı bulmaktadır. Örneğin, deprem verilerinin analizi, kredi kartı kullanıcı profillerinin incelenmesi veya öğrenci başarısının belirlenmesi gibi birçok alanda veri madenciliği kullanılmaktadır. Ancak, veri madenciliği sadece ticari veya akademik amaçlar için değil, aynı zamanda suçların tespiti ve önlenmesi gibi kolluk kuvvetleri tarafından da kullanılmaktadır. Bu durum, adli bilişim tekniklerinin gelişmesine ve suçla mücadelede yeni stratejilerin benimsenmesine olanak tanımaktadır.

Ancak, veri madenciliğinin kullanımıyla ilgili bazı hukuki sorunlar ortaya çıkmaktadır. Gerek verimliliğin artırılması gerek önleyici gerek suçla mücadele kapsamında, veri madenciliği etkili bir araçtır. İlk uygulamaları Almanya'da gerçekleştirilen önleyici amaçlı veri madenciliği, ülkemizde açık bir yasal zeminden yoksundur. Öte yandan, bireylerin kişisel verilerinin işlenmesi ve profil oluşturulması gibi konularda gizlilik endişeleri mevcuttur. Bu nedenle, veri madenciliği uygulamalarının düzenlenmesi ve denetlenmesi gerekmektedir. Ayrıca, özel veritabanlarına erişim gibi konularda da belirli kuralların belirlenmesi önemlidir. Bu şekilde, veri madenciliği tekniklerinin etkin ve adaletli kullanılması sağlanabilir.

Verilerin toplanması ve depolanmasına ilişkin birtakım sınırlı yetkiler kolluğa tanınmıştır. Ancak bu verileri değerlendirme, işleme ve analize tabi tutmak özel yetki gerektiren bir konudur. Türkiye'de trol ağı tarama ve bilgisayarlı eşleme gibi veri madenciliği metotlarının açık bir yasal düzenleme olmaksızın uygulanması, hukuki belirlilik ve öngörülebilirlik ilkeleri açısından ciddi riskler barındırmaktadır. Özellikle özel veri tabanlarına erişim, kişisel verilerin sistematik şekilde analiz edilmesi ve bireylerin profillenmesi gibi uygulamalar, hem Anayasa'nın 20. maddesi hem de AİHS'nin 8. maddesiyle güvence altına alınan özel hayatın gizliliği hakkı ile doğrudan ilgilidir.

Her ne kadar Anayasa Mahkemesi, sanal devriye yetkisini iptal eden 2020 tarihli kararı veya kişisel verilerin korunmasına ilişkin içtihatlarıyla bu alanda sınırlayıcı bir rol üstlenmişse de uygulamada fiilî durumun devam ettiği görülmektedir. Benzer şekilde Yargıtay Ceza Genel Kurulu da trol ağı tarama metodunun masum bireyleri kapsayan yönünü hukuka aykırı bularak önemli bir içtihat ortaya koymuştur. Ancak bu tür kararların, sistematik ve bağlayıcı bir yasal çerçeveyle desteklenmediği sürece yeterli koruma sağlayamayacağı açıktır.

Öte yandan, 6698 sayılı KVKK'nın istisna hükümleri, kolluk ve istihbarat faaliyetlerine geniş veri işleme yetkisi tanımakta, ancak bu yetkilerin sınırlarının nasıl denetleneceği konusunda yeterli güvenceler sunmamaktadır. Avrupa Genel Veri Koruma Tüzüğü (GDPR) ve AİHM içtihadı, istisna rejimlerinin ancak çok net ve sınırlı düzenlemelerle meşru olabileceğini vurgulamaktadır. Türkiye'de ise "önleyici faaliyet" adı altında yapılan veri işleme işlemleri, çoğu zaman hem maddi hukuk hem de usul hukuku açısından belirsizlik taşımaktadır.

Bu çalışmanın karşılaştırmalı çerçevesi ile Türkiye uygulamasına ilişkin bulguları bir arada değerlendirildiğinde iki özgün sonuç öne çıkmaktadır. İlk olarak, Şekil 1-4'te somut soruşturma evrakları üzerinden gösterildiği üzere, Türkiye'de trol ağı tarama mantığı yalnızca kuramsal bir tartışma değil; ÖSYM, MHRS ve tapu-nüfus gibi kamu veri tabanlarının yanı sıra özel şirket veri tabanlarına da erişimi kapsayan fiilî ve yaygın bir uygulamadır. Bu tablo, önleyici veri madenciliğinin 'ön alan evresi'nde ürettiği verilerin, yeterli güvence bulunmaksızın doğrudan ceza muhakemesi deliline dönüşebildiğini göstermektedir.

İkinci olarak, karşılaştırmalı hukuktan türetilebilecek bir güvence paketi önerilebilir. Bu paket; (i) trol ağı tarama ve otomatik veri analizinin ancak somut ve nitelikli bir tehlike ya da suç şüphesi eşiğinde uygulanabileceğini öngören, önleyici ve adli aşamaları birbirinden ayıran müstakil bir kanuni dayanağı; (ii) BVerfG'nin somut tehlike ölçütü ve ABAD'ın hedefli saklama yaklaşımıyla uyumlu, amaçla sınırlı ve ölçülü bir veri işleme rejimini; (iii) saklama sürelerinin, silme prosedürlerinin ve erişim yetkilerinin açıkça tanımlanmasını; (iv) SyRI kararının vurguladığı şeffaflık ilkesi doğrultusunda, kullanılan analiz yöntemlerinin denetlenebilirliğini ve etkili bir yargısal denetimi sağlayacak usuli güvenceleri içermelidir. Aksi hâlde, algoritmik ve otomatik analiz kapasitesinin hukuk devletini aşındırma riski, teknik kapasitedeki her artışla birlikte büyümeye devam edecektir.[97]

Sonuç olarak, veri madenciliği teknikleri suçla mücadelede önemli imkânlar sunsa da bu tekniklerin keyfi, ölçüsüz ve denetimsiz biçimde uygulanması hukuk devleti ilkesiyle bağdaşmamaktadır. Mevcut uygulamalar yalnızca bireysel özgürlükleri değil, aynı zamanda devletin demokratik meşruiyetini de zedeleme potansiyeline sahiptir. Bu nedenle, Türkiye'de trol ağı tarama ve benzeri veri madenciliği uygulamaları için açık, sınırlı, denetlenebilir ve insan hakları ile uyumlu bir yasal çerçevenin acilen oluşturulması elzemdir. Böyle bir düzenleme hem kolluğun etkinliğini artıracak hem de bireysel hakları güvence altına alacaktır.

[97] Algoritmik düzenlemenin kamu sektöründe hukuk devletini aşındırma riski konusunda bkz. Nathalie A. Smuha, *Algorithmic Rule by Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law* (Cambridge University Press, 2024). Türk hukukunda önleyici kolluk hizmetlerinde verilerin elde edilmesi ve korunmasına ilişkin bütünlüklü bir değerlendirme için bkz. Muhammet Kerim Coşkun, *Kişisel Verilerin Korunması Hukuku Kapsamında Önleyici Kolluk Hizmetlerinde Verilerin Elde Edilmesi ve Korunması* (Adalet, 2024).

Ek Beyan

Yazar Katkı Beyanı	: Çalışmanın araştırma fikrinin geliştirilmesi, teorik ve hukuki çerçevesinin oluşturulması, literatür taraması, kaynak ve yargı kararlarının incelenmesi, verilerin değerlendirilmesi, makalenin yazımı, gözden geçirilmesi ve son hâlinin onaylanması dâhil olmak üzere tüm aşamaları yazar tarafından gerçekleştirilmiştir.
Finansman Beyanı	: Bu çalışma, herhangi bir kurum veya kuruluş tarafından finanse edilmemiştir.
Yapay Zekâ Beyanı	: Bu çalışmanın hazırlanması sürecinde yalnızca Extended Summary bölümünün hazırlanması, ana metnin ise dil ve yazım hatalarının tespit ve kontrolüne yardımcı olunması amacıyla yapay zekâ destekli araçlardan yararlanılmıştır. Çalışmada kullanılan kaynaklar, yargı kararları, hukuki değerlendirmeler ve ulaşılan sonuçlar sadece yazar üretilmiş ve yazılmıştır. Yapay zekâ tarafından sağlanan öneri veya içeriklerden kaynaklanabilecek tüm akademik ve hukuki sorumluluk yazara aittir.
Çıkar Çatışması Beyanı	: Yazar, bu çalışmanın yayımlanmasıyla ilgili herhangi bir çıkar çatışması bulunmadığını beyan eder.
Etik Onayı	: Bu çalışmanın tüm süreçlerinde, Terazi Hukuk Dergisi yayın ilkelerine uyulmuştur. Çalışma, insan veya hayvan denekler üzerinde doğrudan herhangi bir uygulama içermemekte; mevzuat, yargı kararları, akademik literatür ve kişisel verileri karartılmış/anonimleştirilmiş belgelerin hukuki analizine dayanmaktadır. Bu nedenle çalışma için etik kurul onayı gerekmemektedir.

Kaynakça

Makale ve Kitaplar

Adalet Bakanlığı, *Adalet Bakanlığı Stratejik Planı (2010-2014)*, https://sgb.adalet.gov.tr/Resimler/SayfaDokuman/24122019093355stratejikplan.pdf [Erişim 28.12.2024]

Adalet Bakanlığı, *Türkiye Hukuk Kamu Araştırmaları Programı* (TÜBİTAK, 2006) http://www.tubitak.gov.tr/tubitak_content_files/ARDEB/kamag/Turkiye_Hukuk_Kamu_Arastirma_Programi.pdf [Erişim 28.12.2024]

Akıncıoğlu, Niyazi Umut, 'Yapay Zekâ Destekli Suç Tahmin Sistemleri: Uygulamadaki Sorunlar ve Hukuki Boyut', *Liberal Düşünce Dergisi* Y.30 S.120 (Güz 2025), 81-102

Alexander, Yonah, *Counterterrorism Strategies: Successes and Failures of Six Nations* (Potomac Books, 2006)

Atlı, Turan, 'Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi', *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* C.2 S.1 (2019), 4-22

Bekkum, Marvin van and Frederik Zuiderveen Borgesius, 'Digital Welfare Fraud Detection and the Dutch SyRI Judgment', *European Journal of Social Security* Vol.23 No.4 (2021), 323-340

Bostancı Bozbayındır, Gülşah, 'Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2016/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler', *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi* C.17 S.2 (2018), 51-103

Cameron, Iain, *National Security and the European Convention on Human Rights* (The Hague, 2021)

Can, Neslihan, 'Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2020)

Cate, Fred H., 'Government Data Mining: The Need for a Legal Framework', *Harvard Civil Rights-Civil Liberties Law Review* Vol.43 (2008), 434-489

Clutterbuck, Richard, *Terrorism, Drugs & Crime in Europe after 1992* (Routledge, 2013)

Coşkun, Muhammet Kerim, *Kişisel Verilerin Korunması Hukuku Kapsamında Önleyici Kolluk Hizmetlerinde Verilerin Elde Edilmesi ve Korunması* (Adalet, 2024)

Çetinkaya, Aytaç, 'Yapay Zekâ Destekli Kolluk Uygulamalarında İdarenin Hukuki Sorumluluğu', *Bilişim Hukuku Dergisi* C.6 S.2 (2024), 508-548

Demirci, Yılmaz, 'Kamu Hizmetlerinde Veri Madenciliği: Çözüm Masası Verileri Temelinde Bir Araştırma', Yayınlanmamış Doktora Tezi, *Sakarya Üniversitesi* (2018)

Doğan, Onur, 'Türkiye'de Veri Madenciliği Konusunda Yapılan Lisansüstü Tezler Üzerine Bir Araştırma', *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* C.19 S.3 (2017), 929-951

EFDPO - European Federation of Data Protection Officers, 'A Landmark Judgment Turns 40: The German Census Judgment of 1983', 14.12.2023, https://www.efdpo.eu/a-landmark-judgment-turns-40-the-german-census-judgment-of-1983/ [Erişim 28.12.2024]

Erbaşı, A. Aslıhan, 'Avrupa Birliği Terör Politikası Işığında Almanya Örneği', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2009)

Erdoğan, Irmak, *Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri* (Seçkin, 2022)

Ferguson, Andrew Guthrie, 'Policing Predictive Policing', *Washington University Law Review* Vol.94 No.5 (2017), 1109-1189

İçer, Zafer, 'Yapay Zekâ Temelli Önleyici Hukuk Mekanizmaları-Öngörücü Polislik', *Yapay Zekâ Çağında Hukuk* (İstanbul Barosu, 2021), 30-48

Kaplan, Onur, 'İdari Kolluk Faaliyetlerinde Dijital Dönüşümün Etkileri ve Sınırları: İki Artı İki Beş Eder Mi?', *Bilişim Hukuku Dergisi* C.7 S.1 (2025), 46-78

Karatay, Rifat, 'Kolluğun Önleyici Faaliyetler Kapsamında Kişisel Veri İşlemesi', ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, *Kişisel Verilerin Korunmasına Uzman Bakış* (KVKK, 2023), 329-361

Kaşli, Enver, 'Kolluk Faaliyetlerinde Kişisel Verilerin Korunması: Avrupa Birliği 2016/794 Sayılı Europol Tüzüğü ve 2016/680 Sayılı Kolluk-Ceza Adaleti Direktifi Işığında Bir İnceleme', *Ankara Avrupa Çalışmaları Dergisi* C.22 S.1 (2023), 97-115

Kavak Güven, Neslihan, *Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Profilleme ve Otomatik Karar Alma* (On İki Levha, 2022)

Keiber, Jason, 'Surveillance Hegemony', *Surveillance & Society* Vol.13 No.2 (2015), 168-181

Keser Berber, Leyla, *Adli Bilişim (Computer Forensic)* (2004)

Kızılırmak, Baran, 'Önleyici Amaçla Elde Edilen Verilerin Ceza Muhakemesinde Kullanılabilirliği', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2018)

Konak, Orkun ve C. Gazi Uçkun, 'Yapay Zekânın Suçla Mücadelede Kişi Profili Oluşturulmasında Kullanımı: Kısa Bir Değerlendirme ve Etik Analiz', *TURAN-SAM Uluslararası Bilimsel Hakemli Dergisi* C.17 S.68 (2025), 46-50

Kunter, Nurullah, Feridun Yenisey ve Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı olarak Ceza Muhakemesi Hukuku* (2008)

Mauldin, Alan, 'Do Submarine Cables Account for Over 99% of Intercontinental Data Traffic?', *Telegeography*, 04.05.2023, https://blog.telegeography.com/2023-mythbusting-part-3 [Erişim 20.04.2024]

Miller, Helena, 'How Does Big Tech Use Data Mining?', *humanID*, 23.06.2021, https://human-id.org/blog/how-does-big-tech-use-data-mining/ [Erişim 28.12.2024]

Nijboer, Johannes F., 'Section 3: Concept Paper and Questionnaire- Information Society (Including Information Technology) and Criminal Justice', *Combatting Cybercrime*, 2013, https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/preparatory-colloquium-section-iii-concept-paper-and-questionnaire.pdf [Erişim 15.04.2024]

Nuhoğlu, Ayşe, 'Trol Ağı Araştırma Metoduna İlişkin Alman Anayasa Mahkemesi Kararı', *Hukuk ve Adalet* S.10 (2007), 201-205

ODATV, 'Emniyet verileri milli yazılıma emanet: BİYOTEKSAN kuruldu', *Odatv.com*, 17.05.2024, https://www.odatv.com/guncel/emniyetteki-biyometrik-veriler-milli-yazilima-emanet-biyoteksan-kuruldu-120044143 [Erişim 24.08.2024]

Özgül, Nurullah, 'İnsan Haklarının Korunması ve Geliştirilmesinde Yeni Bir Sorun Alanı: Algoritmik Profilleme', *TİHEK Akademik Dergisi* Y.5 S.9 (2022), 83-115

Özkaya, Ömer ve İbrahim Toprak, 'Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi', *Manas Sosyal Araştırmalar Dergisi* C.11 S.3 (2022), 1291-1305

Pehlivan, Oğuz Kaan, 'Amerika'da Paradigma Değişimi: NSA ve İstihbaratın Denetimi', *Özgürlük ve Güvenlik Dengesinde Siber Dünya* (2024), 7-9

Pehlivan, Oğuz Kaan, 'İpin Ucunu Kaçırmak: NSA', *Özgürlük ve Güvenlik Dengesinde Siber Dünya* (2024), 10-13

Pehlivan, Oğuz Kaan, 'Kişisel Verilerin Korunması Kanunu ne vadediyor?', *Al Jazeera Turk*, 03.05.2017, https://www.aljazeera.com.tr/gorus/kisisel-verilerin-korunmasi-kanunu-ne-vadediyor [Erişim 25.04.2024]

Rachovitsa, Adamantia and Niclas Johann, 'The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case', *Human Rights Law Review* Vol.22 No.2 (2022), 1-15

Radley-Gardner, Oliver, Hugh Beale and Reinhard Zimmermann (eds), *Fundamental Texts on European Private Law* (Hart Publishing, 2016)

Sağır, Özgür ve Nur Banu Albayrak, 'Veri Madenciliğinin Siber Suçlarda Kötüye Kullanımı', *Journal of Kocaeli Health and Technology University* C.2 S.3 (Aralık 2024), 68-80

Savaş, Serkan, Nurettin Topaloğlu ve Mithat Yılmaz, 'Veri Madenciliği ve Türkiye'deki Uygulama Örnekleri', *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi* C.11 S.21 (2012), 1-23

Slobogin, Christopher and Sarah Brayne, 'Surveillance Technologies and Constitutional Law', *Annual Review of Criminology* Vol.6 No.1 (2023), 219-240

Smuha, Nathalie A., *Algorithmic Rule by Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law* (Cambridge University Press, 2024)

Solove, Daniel J., *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011)

Stronge, Tim, 'Does 70% of the World's Internet Traffic Flow Through Virginia?', *Telegeography*, 30.05.2019, https://blog.telegeography.com/does-70-of-the-worlds-internet-traffic-flow-through-virginia [Erişim 20.04.2024]

Şen, Ersan ve Buğra Şahin, 'Ankesörlü veya Sabit Hattan Ardışık, Periyodik ve Tekil Arama', *Ersan Şen Hukuk ve Danışmanlık*, 01.04.2021, https://sen.av.tr/tr/makale/ankesorlu-veya-sabit-hattan-ard%C4%B1s%C4%B1k-periyodik-ve-tekil-arama [Erişim 20.04.2024]

Temizsoy Bayram, Nihal, 'Ceza Muhakemesi Hukukunda Moleküler Genetik İnceleme ve Elde Edilen Verilerin Delil Olarak Kullanılması', Yayınlanmamış Yüksek Lisans Tezi, *İstanbul Üniversitesi* (2018)

U.S. Department of the Treasury, 'Computer Matching Programs', 19.03.2024, https://home.treasury.gov/footer/privacy-act/computer-matching-programs [Erişim 20.04.2024]

Uzunparmak, Murat, 'Dijital Gözetimin Kavramsal ve Hukuki Çerçevesi: Yapay Zeka Destekli Gözetim Sistemlerinin Anayasal Sınırları', *Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* C.27 S.3 (2025), 1089-1116

Ünver, Yener, 'Federal Almanya'da Terör ve Organize Suçluluk ile İlgili Düzenlemeler', *Nurullah Kunter'e Armağan* (1998), 407-420

Velden, Lonneke van der, 'Leaky Apps and Data Shots: Technologies of Leakage and Insertion in NSA-Surveillance', *Surveillance & Society* Vol.13 No.2 (2015), 182-196

Weil, Ari, 'The Red Army Faction: Understanding a Measured Government Response to an Adaptive Terrorist Threat', *Cornell International Affairs Review* Vol.10, No.2 (2017), 129-159

Wood, David Murakami and Steve Wright, 'Before and After Snowden', *Surveillance & Society* Vol.13, No.2 (2015), 132-138

Yenisey, Feridun, *Kolluk Hukuku* (2023)

Yüksel Civelek, Dilek, 'Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi', *Bilgi Toplumu Dairesi Başkanlığı, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı*, Uzmanlık Tezi (2011)

Mahkeme Kararları

ABAD, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*, Joined Cases C-793/19 and C-794/19, 20 Eylül 2022

ABAD, La Quadrature du Net and Others (La Quadrature du Net II), C-470/21, 30 Nisan 2024

Lahey Bölge Mahkemesi (Rechtbank Den Haag), NJCM ve diğerleri v. Hollanda Devleti (SyRI), C/09/550982 / HA ZA 18-388, 5 Şubat 2020

Almanya Federal Anayasa Mahkemesi (BVerfG), 1 BvR 1547/19, Rn. 1, 16 Şubat 2023

Almanya Federal Anayasa Mahkemesi (BVerfG) (1. Senat), 1 BvR 1873/13, 1 BvR 2618/13, 27 Mayıs 2020

Almanya Federal Anayasa Mahkemesi (BVerfG) (1. Senat), 1 BvR 966/09, 1 BvR 1140/09, 20 Nisan 2016

Almanya Federal Anayasa Mahkemesi (BVerfG) (1. Senat), 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08, 2 Mart 2010

Almanya Federal Anayasa Mahkemesi (BVerfG) (1. Senat), 1 BvR 518/02, 4 Nisan 2006

Anayasa Mahkemesi, T.09.04.2014, E.2013/122, K.2014/74

Anayasa Mahkemesi, T.02.10.2014, E.2014/149, K.2014/151

Anayasa Mahkemesi, T.25.12.2014, E.2014/74, K.2014/201

Anayasa Mahkemesi, T.19.03.2015, E.2014/180, K.2015/30

Anayasa Mahkemesi, T.12.11.2015, E.2015/32, K.2015/102

Anayasa Mahkemesi, T.19.2.2020, E.2018/91, K.2020/10

Anayasa Mahkemesi (Genel Kurul), Murat Albayrak Başvurusu, B. No: 2020/16168, 8/3/2023

Avrupa İnsan Hakları Mahkemesi, *Klass and Others v. Germany*, App no. 5029/71 (ECtHR 06.09.1978)

Avrupa İnsan Hakları Mahkemesi, *Roman Zakharov v. Russia*, App no. 47143/06 (ECtHR [GC] 04.12.2015)

Avrupa İnsan Hakları Mahkemesi, *S. and Marper v. the United Kingdom*, 30562/04, 30566/04 (ECtHR [GC] 04.12.2008)

Yargıtay Ceza Genel Kurulu, T.15.11.2011, E. 2011/6-140, K. 2011/222

Resmî Belgeler ve Kanunlar

2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), OJ L 119, 04.05.2016

2016/680 sayılı Kolluk-Ceza Adaleti Direktifi, OJ L 119, 04.05.2016

2016/794 sayılı Europol Tüzüğü, OJ L 135, 24.05.2016

2024/1689 sayılı Avrupa Birliği Yapay Zeka Yasası, OJ L, 2024/1689, 12.07.2024

2559 sayılı Polis Vazife ve Salahiyet Kanunu, Resmî Gazete No. 2751, 14.07.1934

4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, Resmî Gazete No. 23773, 01.08.1999

5271 sayılı Ceza Muhakemesi Kanunu, Resmî Gazete No. 25673, 17.12.2004

6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete No. 29677, 07.04.2016

7545 sayılı Siber Güvenlik Kanunu, Resmî Gazete No. 32846, 19.03.2025

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, C. 119, C. 119 Official Journal of the European Union §(2016)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), C. L 119/1, C. L 119/1 Official Journal of the European Union §(2016)