

# İnsan Hakları, Kişisel Verilerin Korunması ve Ceza Muhakemesi Hukuku Açısından Önleyici Kolluk Hizmetleri ve İstihbari Çalışmalarda Toplu Veri ve Metadata Kullanımı

S u n a n

**Prof. Dr. Murat Volkan DÜLGER**

*İstanbul Aydın Üniversitesi Hukuk Fakültesi*

**Polis ve Ceza Hukukunda Kişisel Verilerin Korunması**

*Uluslararası Kongresi*

**Tarih:** 14–15 Mayıs 2026 **Yer:** Polis Akademisi Gölbaşı Yerleşkesi, Ali Birinci Kültür Merkezi, Ankara

**Düzenleyen Kurumlar:** T.C. İçişleri Bakanlığı • Emniyet Genel Müdürlüğü • Polis Akademisi Başkanlığı



## BİRİNCİ KISIM

- 1 Sorunun Ortaya Konulması
- 2 Hipotetik Senaryo: Platform Metadata'sına Dayalı Kitlesele Gözetim
- 3 Kavramsal Çerçeve: Metadata, Mozaik Etkisi, Bilgisel Özbekirleme
- 4 Anayasa m. 13 Filtresi: Üç Aşamalı Test
- 5 Anayasa m. 20 ve m. 22 Bağlamında Müdahalenin Yoğunluğu
- 6 Usuli Güvenceler ve Etkili Başvuru Hakkı

## İKİNCİ KISIM

- 7 PVSK Ek m. 7'nin Yapısal Sınırları
- 8 AİHM İçtihadı: Weber Ölçütleri ve Big Brother Watch
- 9 AB Hukuku ve ABAD İçtihadı
- 10 Karşılaştırmalı Anayasa Hukuku (Almanya, ABD, BK, Fransa)
- 11 Veri Koruma İlkeleri ve Ceza Muhakemesi Felsefesi
- 12 Bütüncül Uygulama ve Sonuç



# Giriş: Sorunun Ortaya Konulması

## Dijitalleşme Çağında Devletin Veri Talebi

XXI. yüzyılda iletişim, ödeme, ulaşım, sağlık ve sosyal etkileşim büyük ölçüde dijital platformlara taşınmıştır.

*Kamu otoritelerinin "suçla mücadele" ve "millî güvenlik" gerekçeleriyle dijital hizmet sağlayıcıların veri tabanlarına erişim talepleri hızla artmaktadır.*

**"Önce herkesin verisini alalım, sonra ayıklarız."**

— Klasik bireyselleştirilmiş tedbirden kitlesel gözetim rejimine evrilen yaklaşım.

## Çalışmanın Sorgulamaları



### Hukuki Nitelik

Tüm kullanıcı evrenine ait kütük verisinin periyodik aktarımı hangi hukuki kategoride değerlendirilmelidir?



### Anayasal Filtre

Hipotetik karar, Anayasa m. 13'ün ölçülülük ve demokratik toplum gereklerini karşılayabilir mi?



### Uluslararası Standart

AIHS m. 8 ve ABAD içtihadındaki Weber Ölçütleri ile Big Brother Watch testini geçer mi?



### Karşılaştırmalı Hukuk

Almanya, ABD, Birleşik Krallık ve Fransa anayasal içtihadı paralel uygulamayı nasıl konumlandırır?

### VARSAYIM

*Bir dijital hizmet sağlayıcının tüm kullanıcılarına ait kimlik, iletişim, konum, işlem ve bağlantı verilerinin — somut bir suç şüphesi veya kişi ayrımı yapılmaksızın — periyodik, sürekli ve aylık güncellenen bir veri akışı şeklinde kolluk ve istihbarat birimlerine aktarılması.*

#### KİMLİK

Ad-soyad, T.C. kimlik no, kayıt bilgileri

#### İLETİŞİM

Telefon, e-posta, iletişim taraf bilgileri

#### KONUM

IP adresi, baz istasyonu, fiziksel adres

#### BAĞLANTI (Metadata)

İşlem kayıtları, oturum, etkileşim örüntüleri

### Yapısal Dönüşüm

**Klasik bireyselleştirilmiş tedbir mantığı:** Önce hedef belirlenir, sonra ona ait veri toplanır.

**Hipotetik model:** Önce platformun tamamına ilişkin veri havuzu kurulur, sonra havuz içinden sorgulama yapılır.

## Platform Metadata'sına Dayalı Kitlesele Gözetim

*Belirli hedeflere indirgenmeksizin,*

tüm kullanıcı evreninin kimlik, iletişim, IP, erişim, hesap ve bağlantı verilerinin topluca, sistematik ve süreklilik arz edecek biçimde kamu makamlarına aktarılmasıdır.

Bu mimari, **bireyselleştirilmiş tedbir mantığını tersine çevirir**; devlet önce belirli bir kişiyi hedeflememekte, önce veri havuzunu kurmakta, sonra o havuz içinden sorgulama imkânı edinmektedir.

## Klasik vs. Hipotetik Model

|        | KLASİK TEDBİR             | HİPOTETİK MODEL         |
|--------|---------------------------|-------------------------|
| Hedef  | Belirli kişi / olay       | Tüm kullanıcı evreni    |
| Şüphe  | Somut, kişiselleştirilmiş | Yok (ön-toplama)        |
| Süre   | Sınırlı süre              | Periyodik / sürekli     |
| Kapsam | Dar, parametrik           | Geniş, ayırım gözetmez  |
| Mantık | Bireyselleştirme          | Veri havuzu + sorgulama |

**TANIM** Metadata, bir iletişimin veya işlemin *içeriği* değil; o iletişimi/işlemi *çevreleyen* bilgiler bütünüdür: telefon numaraları, IP adresleri, oturum kayıtları, baz istasyonu konumları, oturum süreleri, bağlantı kalıpları ve cihaz tanımlayıcıları.

## İÇERİK VERİSİ

Mesajın metni, sesin kendisi, görselin içeriği. Klasik anlamda en yoğun mahremiyet alanı.

## TRAFİK VERİSİ (Metadata)

Kim, ne zaman, kiminle, nereden iletişim kurdu — iletişimi çevreleyen bilgi katmanı.

## ABONE / KÜTÜK VERİSİ

Ad, adres, vergi no, telefon no — kullanıcı kaydına ilişkin temel kimlik verileri.

## PARADİGMA DEĞİŞİMİ

**Carpenter v. United States (2018):** Metadata, içerik verisinden daha yoğun biçimde bireyin yaşamını (aile, siyasi, dini, mesleki, kültürel) ifşa edebilir. *Geleneksel "metadata daha az hassastır" varsayımı, büyük veri analitiği çağında geçerliliğini yitirmiştir.*

## M o s a i c   E f f e c t

## Mozaik Etkisi

*Tek başına zararsız görünen veri parçacıklarının bir araya getirilerek, parçaların hiçbirinin tek başına ortaya çıkaramadığı bir bütünsel resmi ortaya koyması.*

AD

IP

KONUM

TEL

MAİL

SAAT

OTURUM

CIHAZ

BAĞLANTI

→ Süper-mahrem profil

## Yapısal Riskler

%87–95

## Yeniden Tanımlanma Oranı

Posta kodu, doğum tarihi, cinsiyet gibi yarı-belirleyiciler çapraz eşleştirildiğinde bireyler %87–95 oranında yeniden tanımlanabilir (AOL, Netflix vakaları).

7 Gün

## Carpenter Eşiği

ABD Yüksek Mahkemesi: 7 günlük baz istasyonu kaydı dahi kişinin fiziksel hareketlerine ilişkin makul mahremiyet beklentisini ihlal eder.

Algoritmik  
Yönetimsellik

## Rouvroy &amp; Berns

Alta-bireysel veri parçacıklarından üst-bireysel profiller türetilir; bireyin öznelliğine başvurulmaksızın yönetim mümkün hâle gelir.

## Volkszählungsurteil (BVerfG, 1983)

*Bilgisel Özbelleme Hakkı**informationelles Selbstbestimmungsrecht*

Kişi, kendi kişisel verilerinin açıklanması ve kullanımı üzerinde kural olarak **kendisi karar verebilmelidir**.

Sınırsız toplama, depolama, kullanma ve aktarmanın *özgür kişiliği tehdit edeceği* BVerfG tarafından açıkça vurgulanmıştır.

**Online-Durchsuchung (2008):** Bu mantık "bilgi teknolojisi sistemlerinin gizliliği ve bütünlüğü" hakkına evrilmiştir.

## Chilling Effect

## Soğutucu Etki

*Sürekli veri toplama altyapısının kurulması, bireylerde "her an izleniyorum" hissini yerleştirir.*

## İFADE ÖZGÜRLÜĞÜ

Öz sansür ve düşünce paylaşımının daralması

## ÖRGÜTLENME

Sivil toplum aktivitesinin ve katılımın baskılanması

## GAZETECİLİK

Kaynak korumasının zayıflaması, basın özgürlüğüne etki

## VII Hedefli Toplama vs. Toplu/Ayrim Gözetmeyen Toplama

### HEDEFLİ TOPLAMA

*Targeted Collection*

✓ **Belirli kişi/kategori odaklı**

Somut şüphe veya tehlike eşiği ile sınırlı.

✓ **Süre ve kapsam parametrik**

Önceden tanımlı yetki çerçevesi, hâkim onayı.

✓ **Anayasal denetime elverişli**

Ölçülülük testinden geçebilen, bireyselleştirilmiş tedbir.

✓ **Telafi imkânı mevcut**

Bildirim ve etkili başvuru yolu işlevsel.

### TOPLU / AYRIM GÖZETMEYEN

*Bulk / General and Indiscriminate*

✗ **Tüm kullanıcı evreni kapsamlı**

Şüpheli/şüpheli-olmayan ayrımı yapılmaz.

✗ **Veri havuzu mimarisi**

Önce topla, sonra sorgula yaklaşımı.

✗ **ABAD: Şart m. 7, 8, 11 ile bağdaşmaz**

Tele2 Sverige (2016) ve La Quadrature du Net (2020) içtihadı.

✗ **Masumiyet karinesini erozyona uğratır**

Vatandaş baştan veri-deneği konumuna iter.

## VIII Anayasa m. 13 Filtresi: Üç Aşamalı Test

**Anayasa m. 13:** (a) ilgili maddedeki sebepler, (b) kanunla öngörülme, (c) demokratik toplum düzeninin gerekleri, (d) ölçülülük ilkesi (elverişlilik – gereklilik – orantılılık).

1

### KANUNİLİK

*Quality of Law*

Belirlilik + erişilebilirlik + öngörülebilirlik. Kitlesele gözetimde standart YÜKSELTİLİR.

#### HİPOTETİK MODEL: ZAYIF

*Hangi koşulda hangi veriye erişileceği, suç tipi, süre ve teknik filtre tanımsız.*

2

### MEŞRU AMAÇ

*Legitimate Aim*

Suçla mücadele ve millî güvenlik amacının kâğıt üstünde değil, etkili biçimde gösterilmesi.

#### HİPOTETİK MODEL: TARTIŞMALI

*Daha hafif tedbirle aynı amaca ulaşmak mümkünse, en geniş tedbir testi geçemez.*

3

### ÖLÇÜLÜLÜK

*Proportionality*

Elverişlilik – gereklilik – orantılılık. "En az müdahaleci araç" zorunluluğu.

#### HİPOTETİK MODEL: GEÇMEZ

*Hedefli alternatif mümkünken, mozaik etkili kitlesele toplama orantısızdır.*

## YANSIMALI MÜDAHALE

Hipotetik karar yalnızca m. 20'deki kişisel verilerin korunmasına değil, m. 22'deki haberleşme özgürlüğüne de "yansımali" biçimde müdahale eder. *Malone v. UK*'ten itibaren AİHM içtihadı bunu "haberleşme" alanı içinde kabul etmektedir.

## Anayasa m. 20 • Kişisel Verilerin Korunması

**AYM kararlarında kişisel veri:** "Belirli veya kimliği belirlenebilir gerçek kişiye ilişkin her türlü bilgi."

**Kapsama girenler:** Ad, soyad, T.C. kimlik no, telefon no, IP adresi, konum, cihaz kimliği, oturum verileri.

**"Sadece metadata" savunması:** Anayasal müdahalenin ağırlığını azaltmaz. Modern dijital düzende metadata, çoğu zaman içerikten daha kapsayıcı profil çıkarımına imkân verir.

## Anayasa m. 22 • Haberleşme Hürriyeti

**AYM, AİHM içtihadıyla uyumlu olarak:** İletişimin yalnız içeriği değil, "kim, kim ile, ne zaman, nereden" verisi de m. 22 kapsamındadır.

**Malone v. UK (1984):** İletişimin trafik verisi AİHS m. 8 anlamında haberleşme alanı içindedir.

**AYM m. 148/3 yorum kaynağı:** Zakharov, Big Brother Watch, Centrum för Rättvisa ve Szabó-Vissy içtihadı, Anayasa yorumunda bağlayıcı yorum kaynağıdır.

m. 40/2

USULİ  
GÜVENCE**Kanun Yolu Gösterme Ödevi**

Devletin, ilgililere hangi kanun yollarına ve hangi sürede başvurabileceklerini belirtme yükümlülüğü.

⚠️ *Hipotetik kararın yol ve süre göstermemesi, daha esasa girilmeden hukuka aykırılık doğurur.*

m. 36

USULİ  
GÜVENCE**Mahkemeye Erişim Hakkı**

Hak arama hürriyeti ile organik bağ. AYM, yol/süre gösterilmemesini bağımsız ihlal sebebi sayar.

⚠️ *Bildirim yokluğunda mahkemeye erişim kâğıt üstünde kalır.*

Dijital Miranda

USULİ  
GÜVENCE**Şeffaflık İlkesi**

Veri sorumluları ilgilileri hakları konusunda bilgilendirmekle yükümlüdür.

⚠️ *Milyonlarca kullanıcı verisinin aktarıldığından haberdar olmayacaktır.*

AİHS m. 13

USULİ  
GÜVENCE**Etkili Başvuru Hakkı**

Klass v. Almanya: Gözetimin sona ermesinden sonra dahi bildirim ve itiraz makul biçimde işlemelidir.

⚠️ *Süresiz bildirimsizlik AİHS m. 13 standartlarını karşılamaz.*

**PVSK Ek m. 7**, polise belirli ağır suçların önlenmesi amacıyla sınırlı bir önleme dinlemesi ve önleyici istihbarat yetkisi tanır. "Bilgi-belge talebi" mekanizması, *tüm kullanıcıları kapsayan bir veri aktarımına elverişli değildir*.

#### Hedefleme Zorunluluğu

"Hakkında tedbir uygulanacak kişinin kimliği, aracı, IP, kapsam ve süre" unsurları normun kişiselleştirilmiş tedbir kurgusunu açıkça gösterir.

#### Süre ve Yenileme Sınırı

Sürekli ve otomatik veri aktarımı, "tedbir" olmaktan çıkar ve "kalıcı rejim"e dönüşür; 3 aylık yargısal denetim mekanizması fiilen işlevsiz kalır.

#### Bağımsız Etkili Denetim

Ex post denetim ve telafi imkânı kitlesel rejimlerde kritik bir güvencedir. Hâkim kararı sırf formalite olamaz.

**ULTRA VIRES — YETKİ AŞIMI:** Bilgi-belge talebi yetkisinin milyonlarca masum kullanıcıyı kapsayan veri havuzu yetkisine dönüştürülmesi açık bir yetki aşımı işlemidir.

**KVKK m. 28 İSTİSNASININ DAR YORUMU:** İstisna anayasal muafiyet anlamına gelmez; m. 13 ve m. 20'nin zorunlu eşiklerini ortadan kaldırmaz.

## XII AİHM Weber Ölçütleri: Big Brother Watch Sekiz Basamak Testi

Weber & Saravia v. Germany (2006) altı asgari ölçüt; Big Brother Watch v. UK (BD, 2021) iki ek güvence ile **sekiz basamaklı test**.

|                                                                                                                   |                                                                                                          |                                                                                                                      |                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>1</b> NEDENLER<br><i>Suç tipleri tanımı</i><br><b>Hipotetik: ZAYIF</b><br><i>Standart karşılanmıyor.</i>       | <b>2</b> KOŞULLAR<br><i>Kişi kategorileri</i><br><b>Hipotetik: YOK</b><br><i>Standart karşılanmıyor.</i> | <b>3</b> SÜRE<br><i>Süre sınırı</i><br><b>Hipotetik: SÜRESİZ</b><br><i>Standart karşılanmıyor.</i>                   | <b>4</b> TEMİNATLAR<br><i>İnceleme/saklama usulü</i><br><b>Hipotetik: BELİRSİZ</b><br><i>Standart karşılanmıyor.</i> |
| <b>5</b> PAYLAŞIM<br><i>Üçüncü taraf aktarımı</i><br><b>Hipotetik: TANIMSIZ</b><br><i>Standart karşılanmıyor.</i> | <b>6</b> SINIRLAR<br><i>İmha rejimi</i><br><b>Hipotetik: YOK</b><br><i>Standart karşılanmıyor.</i>       | <b>7</b> ÖNCEDEN<br><i>Bağımsız ön-yetkilendirme</i><br><b>Hipotetik: BİÇİMSEL</b><br><i>Standart karşılanmıyor.</i> | <b>8</b> SONRADAN<br><i>Ex post denetim/başvuru</i><br><b>Hipotetik: İŞLEVSİZ</b><br><i>Standart karşılanmıyor.</i>  |

**SONUÇ:** Hipotetik aktarım modeli, AİHM'in sekiz basamaklı standardını **yapısal olarak karşılayamamaktadır**.

*Roman Zakharov v. Russia*

BD, 2015

Gözetim alanındaki takdir yetkisi sınırsız ifade edilemez; bireye keyfiliğe karşı yeterli koruma sağlayacak açıklıkta kanunda gösterilmelidir.

★ *Hâkim izni + ex post inceleme*

*Szabó & Vissy v. Macaristan*

2016

"Sanal olarak herkesi kapsayabilen" anti-terör gözetimi, strict necessity testi uygulanmaksızın AİHS m. 8 ihlali oluşturur.

★ *Katı gereklilik (strict necessity)*

*Big Brother Watch v. UK*

BD, 2021

Toplu erişimin yürütmeden bağımsız organca yetkilendirilmemesi; arama terimlerinin ve subject selectors'ın bağımsız onaydan geçmemesi yapısal kusur.

★ *End-to-end safeguards*

*Centrum för Rättvisa v. Sweden*

BD, 2021

Veri yabancı ortaklara aktarılırken mahremiyet menfaati değerlendirilmemesi; etkili ex post inceleme yokluğu yapısal eksikliklerdir.

★ *Uçtan uca denetim*

**Direktif (AB) 2016/680 • Polis Direktifi (Law Enforcement Directive)**

(i) Belirli, açık ve meşru amaçla işleme | (ii) Yeterli, ilgili, aşırı olmayan veri | (iii) Gerekli olandan uzun saklamama | (iv) Güvenlik tedbirleri | (v) Hesap verebilirlik | (vi) İlgili kişi haklarının güvencesi (bilgi, erişim, düzeltme, silme).

**2014***Digital Rights Ireland*

2006/24 Veri Saklama Direktifi'nin Şart m. 7 ve 8'e aykırılığı; "genel ve ayırım gözetmeyen saklama" geçersiz.

**2016***Tele2 Sverige / Watson*

Tüm abonelerin tüm haberleşme verilerinin genel ve ayırım gözetmeyen saklanması Şart'a aykırıdır.

**2020***La Quadrature du Net*

Çizgi muhafaza edildi; yalnızca gerçek/mevcut/öngörülebilir ciddi millî güvenlik tehdidi varsa, süre sınırlı ve bağımsız denetimli istisna mümkün.

**İşlev Kayması (Function Creep)**

Başlangıçta terör veya millî güvenlik gibi ağır gerekçelerle oluşturulan veri sistemleri, zamanla daha geniş ve farklı amaçlarla kullanılmaya başlanabilir. Aylık periyotlarla sürekli akış, işlev kayması riskini yapısal olarak içerir.

## Bundesverfassungsgericht (BVerfG) — Çok Katmanlı Veri Koruma İçtihadı

| 1983                                              | 1999                                                                            | 2008                                                 | 2010                                                                 | 2013                                                                | 2016                                                                  | 2020                                                          |
|---------------------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
| <i>Volkszählungsurteil</i>                        | <i>G 10 Kararı</i>                                                              | <i>Online-Durchsuchung</i>                           | <i>Vorratsdatenspeicherung</i>                                       | <i>Antiterrordatei</i>                                              | <i>BKA-Gesetz</i>                                                     | <i>BND-Auslandsaufklärung</i>                                 |
| Bilgisel özbelleme hakkı (Anayasa m. 2/1 ve 1/1). | Anayasa m. 10 yalnız içeriği değil; bilgi edinme, işleme ve aktarımı da kapsar. | BT sistemlerinin gizliliği ve bütünlüğü temel hakkı. | Şüphesiz 6 aylık trafik verisi saklama ağır müdahale; sıkı koşullar. | Ortak veri havuzu mümkün, fakat sıkı yasal çerçeve + ek güvenceler. | Çekirdek özel yaşam alanının korunması; silme ve bağımsız ön denetim. | Stratejik gözetim için çok katmanlı güvence mimarisi zorunlu. |

*Smith v. Maryland (1979) • Klasik Doktrin*

Telefon numarası arama kayıtlarına ilişkin makul mahremiyet beklentisi yoktur; kişi verisini gönüllü olarak ifşa eder ("third party doctrine").

*United States v. Jones (2012)*

GPS ile uzun süreli takip "arama" niteliğindedir. Yargıç Sotomayor: "*Uzun süreli ve sistematik izleme, kısa süreli gözlemden çok daha ağır müdahaledir.*"

*Carpenter v. United States (2018)*

Cep telefonu baz istasyonu konum verisine (CSLI) erişim "arama" niteliği taşır ve kural olarak warrant gerektirir. *Üçüncü kişide bulunan veriye sınırsız erişim reddedilmiştir.*

*ACLU v. Clapper (2015)*

NSA'nın toplu metadata toplama programı, **USA Patriot Act §215 kapsamında verilen yetkiyi aşmıştır.** "*Önce tüm verileri topla, sonra analiz et*" yaklaşımı kanunilik bakımından kabul edilmedi.

## BİRLEŞİK KRALLIK

*IPA Rejimi & Privacy International Kararı****Big Brother Watch v. UK (BD, 2021)***

Toplu gözetim ilke olarak yasak değildir; ancak seçim–filtreleme–inceleme aşamalarındaki güvenceler yetersiz kalmıştır.

***R (Privacy International) v. IPT (UKSC, 2019)***

"Ouster clause" tartışmasında yargı denetiminin kapatılmasına karşı güçlü tutum.

**Temel mesaj:** Kitlesel veri toplama uygulamalarında etkili hukuk yolu ve denetim, lüks değil *meşruiyetin şartıdır*.

## FRANSA

*"Renseignement" Rejimi ve Anayasa Konseyi****Loi relative au renseignement (2015)***

İstihbarat faaliyetlerinin geniş yasal çerçevesi.

***Conseil constitutionnel — 23.07.2015, 2015-713 DC***

İstihbarat alanındaki algoritmik analiz sistemleri anayasal sıkı denetime tabidir.

**Veri saklama-erişim rejimi:** ABAD'ın La Quadrature du Net içtihadıyla yoğun gerilim alanı oluşturur. "İdari kolluk/istihbarat" ile "adli kolluk" ayrımı kitlesel tekniklerin anayasal denetimini ortadan kaldırmaz.

# XVIII Veri Koruma İlkeleri Açısından Analiz

1

## Amaç Sınırlılığı

*Purpose Limitation*

Belirli, açık ve meşru amaçlar. "İstihbarat havuzu" amaç sınırlılığının çekirdeğini yok eder.

2

## Veri Minimizasyonu

*Data Minimization*

Yeterli, ilgili ve gerekli olanla sınırlı. "Gelecekteki potansiyel değer" yaklaşımı ilkenin antitezidir.

3

## Tasarım Gereği Gizlilik

*Privacy by Design*

Sistemler en kısıtlayıcı ayarlarla çalışmalı. Hipotetik karar "varsayılan olarak gözetim" altyapısı kurar.

4

## Saklama-İmha Rejimi

*Retention/Deletion*

Gerekli olmayan veri derhal silinmeli. Aylık otomatik akış müdahaleyi kalıcı altyapıya dönüştürür.

5

## Şeffaflık

*Transparency*

İlgilinin haklarını kullanabilmesi için ön şart. Hipotetik modelde milyonlar bilgilendirilmez.

6

## Hesap Verebilirlik

*Accountability*

Veri sorumlusunun sorumlulukları somut, ölçülebilir ve denetlenebilir olmalıdır.

**Bireyselleştirilmiş Tedbir Mantığının Tasfiyesi**

CMK'nin koruma tedbirleri sistemi, somut bir kişiye yönelen belirli derecede şüpheyi varsayar. "Önce verisini al, sonra ayıkla" mantığı, somut olay bağı ve sebep gösterme gerekliliklerini ortadan kaldırır.

**İlgili Çerçeve:** *Klass v. Germany*

**Masumiyet Karinesinin Yapısal İhlali**

Genelleyici toplu toplama, tüm vatandaşları potansiyel olarak "şüphe altında" konumlandırır. Liberal ceza muhakemesi felsefesi, vatandaş devletın meşru kuşkusunun sınırlayıcı çerçevesi olarak konumlandırır.

**İlgili Çerçeve:** *Anayasa m. 38, AİHS m. 6/2*

**Nemo Tenetur ve Pasif Veri Üretimi**

Modern tartışmada nemo tenetur yalnızca aktif beyana karşı değil; pasif olarak ürettiğimiz dijital izlerin aleyhimize konuşturulmasına karşı da bir kalkandır.

**İlgili Çerçeve:** *Kendi aleyhine delil*

**Maddi Gerçek Hukuk Devleti Çerçevesinde**

Türk ceza muhakemesi öğretisinde yerleşik kabul: Hukuk devleti güvenceleri maddi gerçeğin araştırılmasının çerçevesidir. Etkin soruşturma, bağımsız denetim ve hak korumasının yok olduğu alan meşru görülemez.

**İlgili Çerçeve:** *Hukuk devleti ilkesi*

# XX Bütüncül Uygulama: Dört Soruluk Test ve İhlal Tablosu

1

Müdahale?  
VAR

2

Kanunla?  
SORUNLU

3

Meşru Amaç?  
VAR

4

Demokratik/Ölçülü?  
HAYIR

Anayasa m. 13 + AİHS m. 8/2 Birleşik Testi

Kırılma noktaları: Hedefleme yokluğu ("tüm kullanıcılar") + Süreklilik ("aylık güncelleme")

| İLGİLİ NORM                  | HAK / İLKE                       | YAPISAL SORUN                                                    |
|------------------------------|----------------------------------|------------------------------------------------------------------|
| Anayasa m. 13 / AİHS m. 8    | Ölçülülük ve gereklilik          | Mozaik etkili kitlesel veri havuzu; gereklilik testinin aşılması |
| Anayasa m. 20 / AİHS m. 8    | Kişisel veriler / özel hayat     | Kanunun kalitesi yoksunluğu; ayırım gözetmeyen saklama           |
| Anayasa m. 22 / AİHS m. 8    | Haberleşme hürriyeti             | Metadata üzerinden sürekli denetim altına alma                   |
| m. 40/2 – m. 36 / AİHS m. 13 | Etkili başvuru, mahkemeye erişim | Kanun yolu/süre gösterilmemesi; bireye bildirim olmaması         |
| AB Şart m. 7-8 (referans)    | Mahremiyet ve veri koruma        | "Genel ve ayırım gözetmeyen" toplama yasağı (LQDN)               |
| Hukuk devleti ilkesi         | Ultra vires, yetki saptırması    | "Bilgi-belge talebi"nin veri havuzu yetkisine dönüştürülmesi     |

# Bütüncül Değerlendirme

*"Önce herkesin verisini al, sonra ayıkla"* yaklaşımı, demokratik anayasal düzenle bağdaşır bir yöntem değildir.

1

## Anayasal Test Aşılmaz

m. 13, 20 ve 22: kanunilik, belirlilik, gereklilik ve orantılılık eşikleri karşılanamaz; hakkın özüne dokunma riski mevcuttur.

2

## AİHM Standardı Karşılanmaz

Weber + Big Brother Watch sekiz basamaklı testinin kategori, süre, denetim, ex post inceleme ve imha gereklilikleri sağlanamaz.

3

## AB Hukukuyla Bağdaşmaz

Polis Direktifi 2016/680 ve ABAD üçlemesi (DRI – Tele2 – LQDN) genel ve ayırım gözetmeyen toplamayı reddeder.

4

## PVSK Ek m. 7 Aşılır

Bilgi-belge talebi yetkisi, milyonlarca kullanıcıyı kapsayan kalıcı veri havuzu yetkisine dönüştürülemez.