PANEL 2- E-EVIDENCE REGULATION

JOSÉ MANUEL SÁNCHEZ SISCART
Senior Judge
High Court of Justice
Navarra - Spain

SPRING CONFERENCE 2026.
BARCELONA - SPAIN

Data at the Heart of Criminal Investigations

Ninety percent of criminal cases now rely on geolocation, metadata, and online activity as primary evidence.

DATA

The different types of data stored on a mobile phone

1. COMMUNICATION DATA

- Call logs (number, duration, time)
- SMS/MMS messages
- Emails
- Instant messaging (WhatsApp, Signal, Telegram, etc.)
- Voicemails
- Contact list

2. LOCATION DATA

- GPS location (real-time and history)
- Wi-Fi networks connected
- Cell towers / base stations
- Location history and frequent places

3. INTERNET & APP USAGE

- Browser history
- Search history
- Websites visited
- App usage and activity logs
- Cookies and online identifiers

4. MEDIA & FILES

- Photos and videos (including metadata: date, time, location)
- Audio recordings
- Documents and files
- Downloads

5. DEVICE & SYSTEM DATA

- Device identifiers (IMEI, IMSI, serial number)
- Operating system and version
- Installed apps and version
- System logs and diagnostic data
- Battery usage and performance data

6. SENSORS & ACTIVITY DATA

- Accelerometer (movement, steps)
- Gyroscope
- Fitness and health data
- Sleep patterns
- Activity and usage patterns

7. FINANCIAL & TRANSACTION DATA

- Mobile payments and wallets
- Banking app activity
- Purchase history
- Loyalty and reward programs

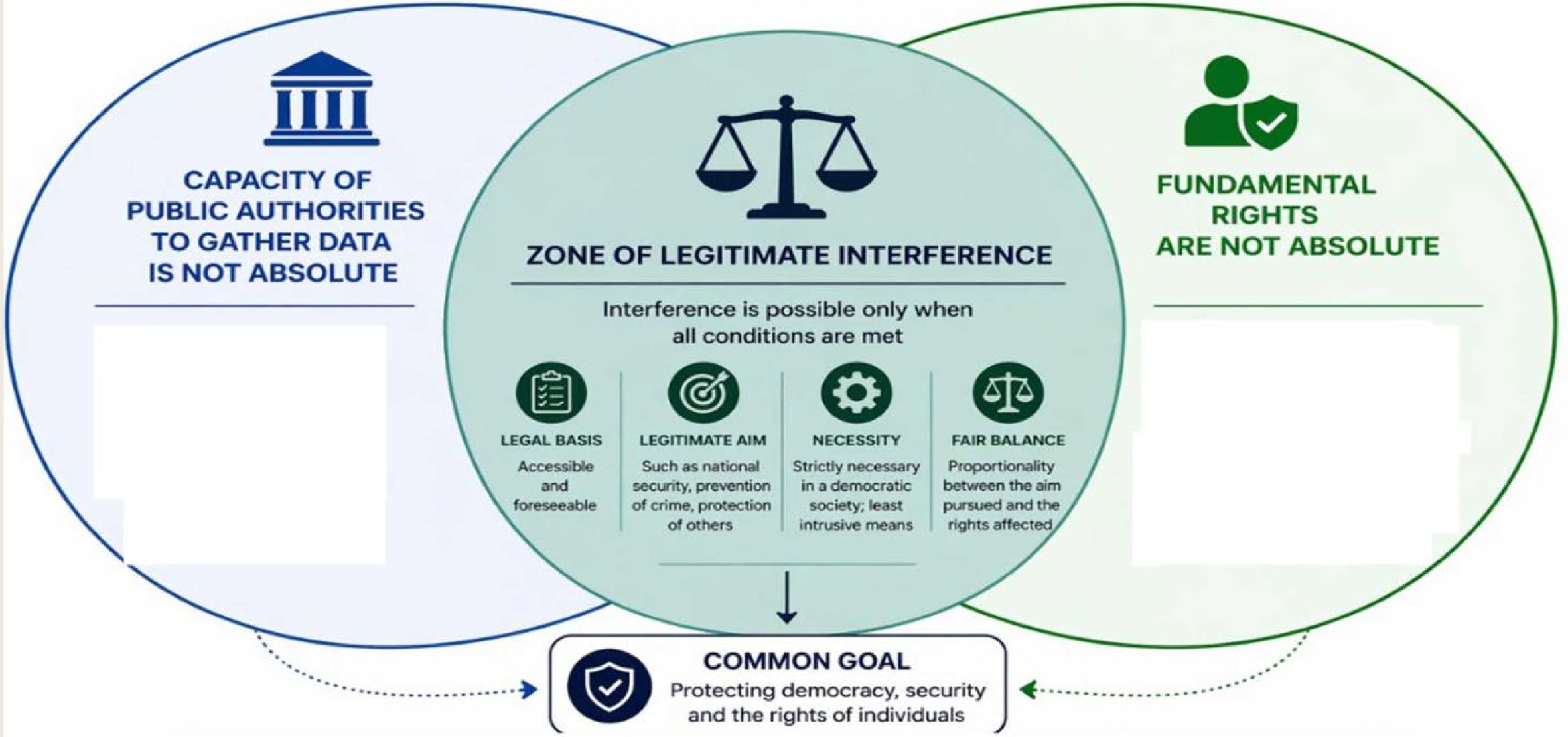
8. IDENTIFIERS & ACCOUNT DATA

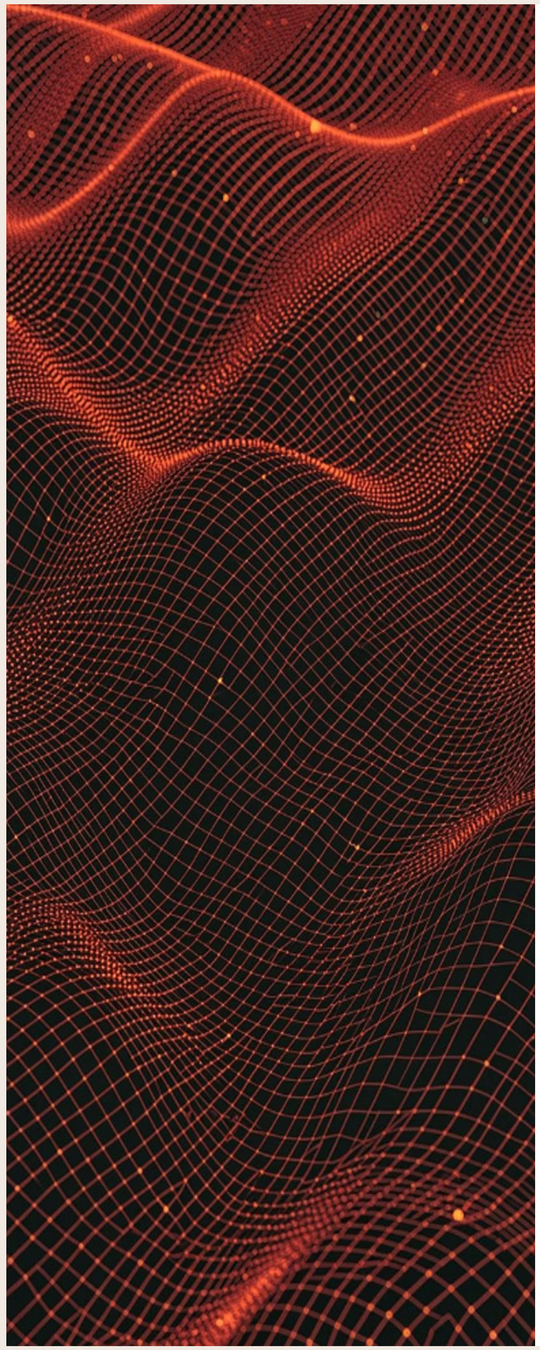
- Online accounts (Google, Apple ID, social media, etc.)
- Login credentials (saved)
- Account preferences and settings
- Backup and cloud data

WHY IT MATTERS

Even without accessing the content of communications, this data can reveal a lot about a person's life: habits, relationships, beliefs, movements, and personal preferences.

Finding the fair balance in a democratic society





Art. 7 & 8 Charter/ Art. 8 ECHR Framework

CJEU *Digital Rights Ireland* (2014): retention is an autonomous interference.

ECHR *Pietrzak v. Poland, Podchasov v. Russia, Skoverne v. Slovenia*

Proporcionality: technical & Legal aspects

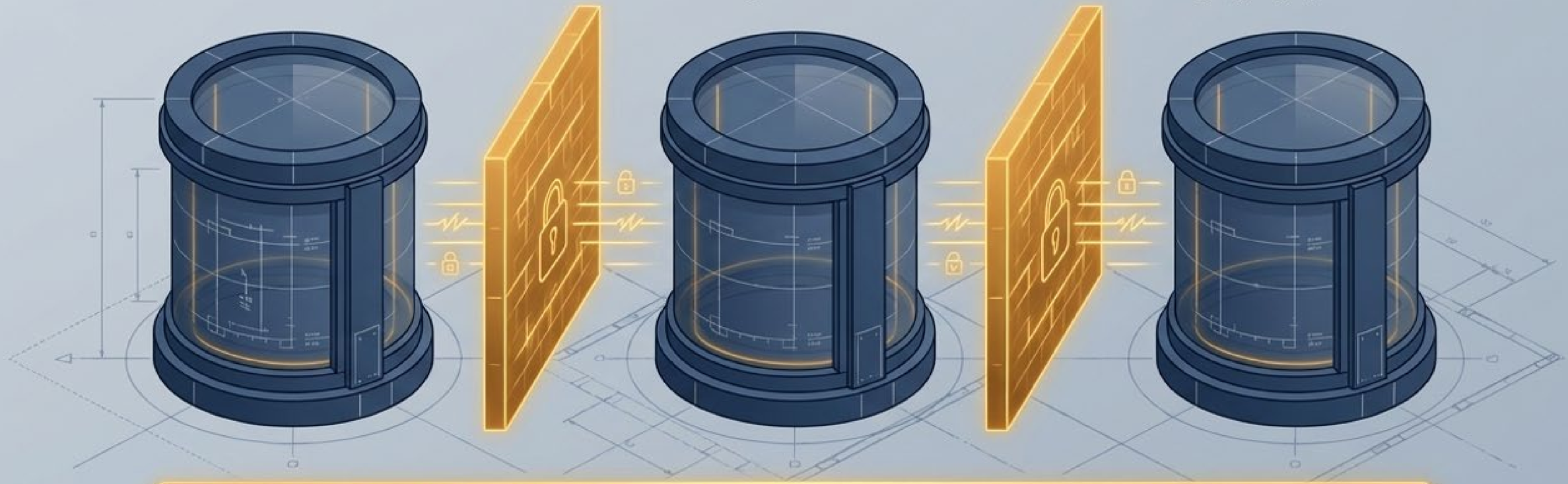
- Civil identity of users
- IP adresses assigned to the source
- Terrorism cases: serious threat to national security, genuine, present or foseeable, limited in time, prior judicial review
- Targeted retention
- Quick freeze

The prerequisite for ISPs: Genuinely watertight data separation

Vault A (Civil Identity):
Names, addresses, contact details.

Vault B (IP Addresses):
Static and dynamic IPs assigned to users.

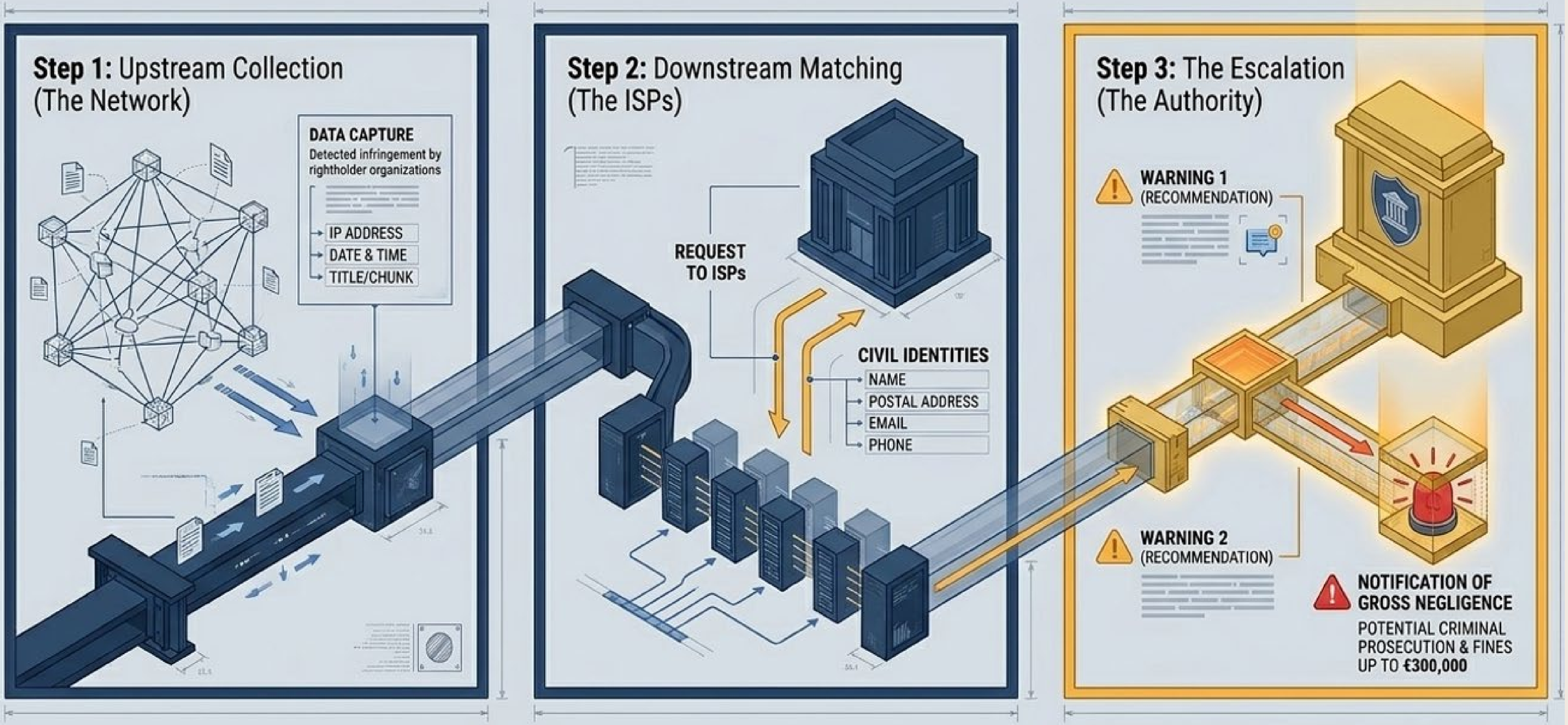
Vault C (Traffic & Location):
Clickstreams, communication logs, geographic data.



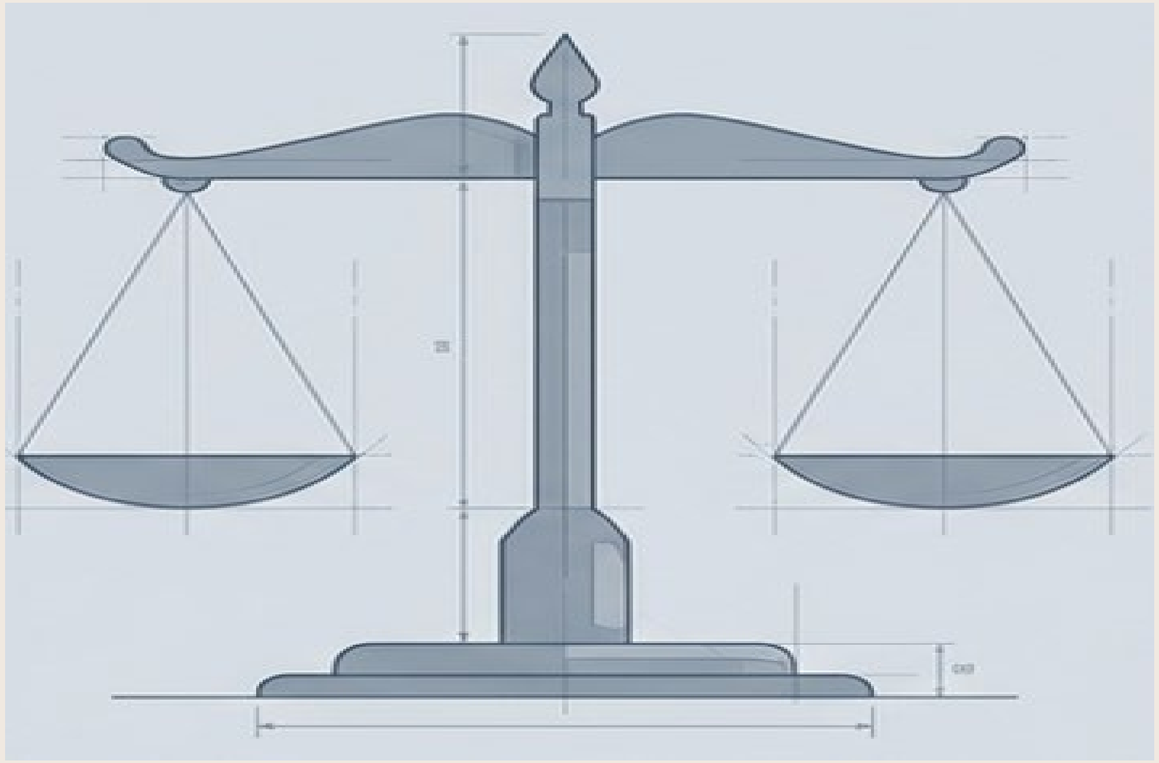
The Structural Mandate: To retain IP addresses generally and indisriminately, ISPs must implement a secure, reliable computer system that guarantees genuinely watright separation. The system must physically prevent data from being combined to draw precise conclusions about a user's private life.

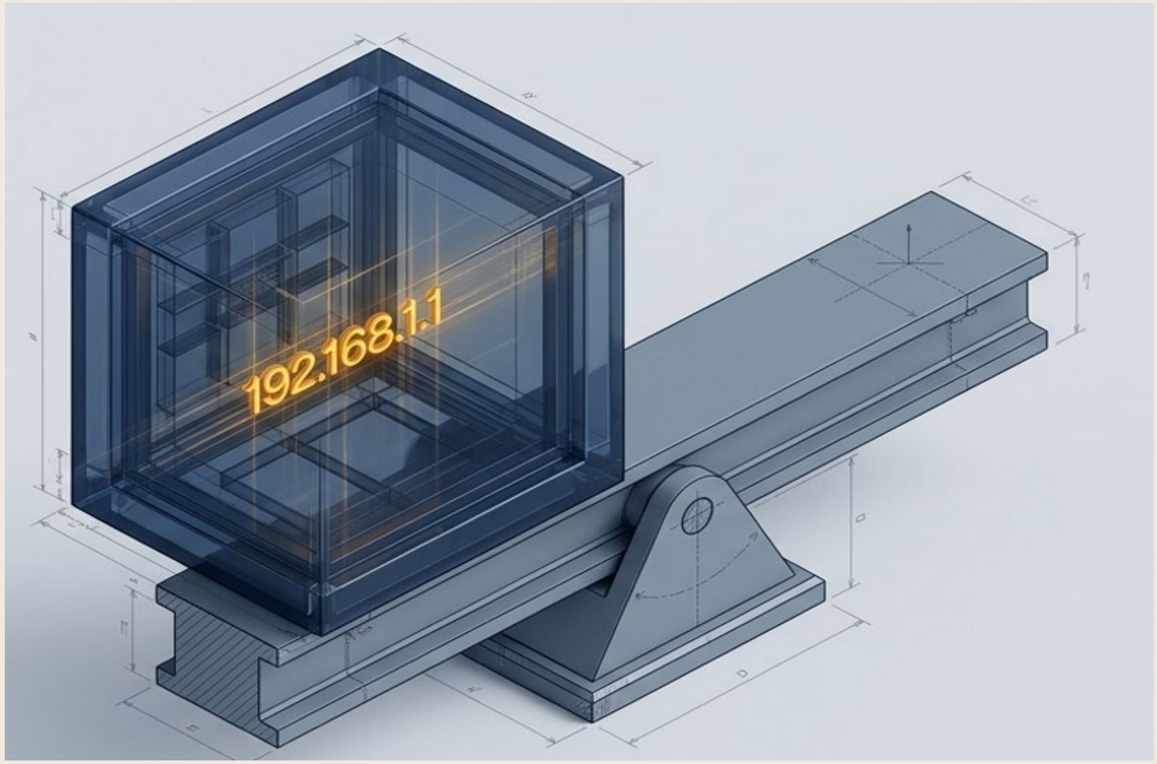
The CJEU Framework: Privacy interference is dictated by system architecture

The operational context: France's Graduated Response system

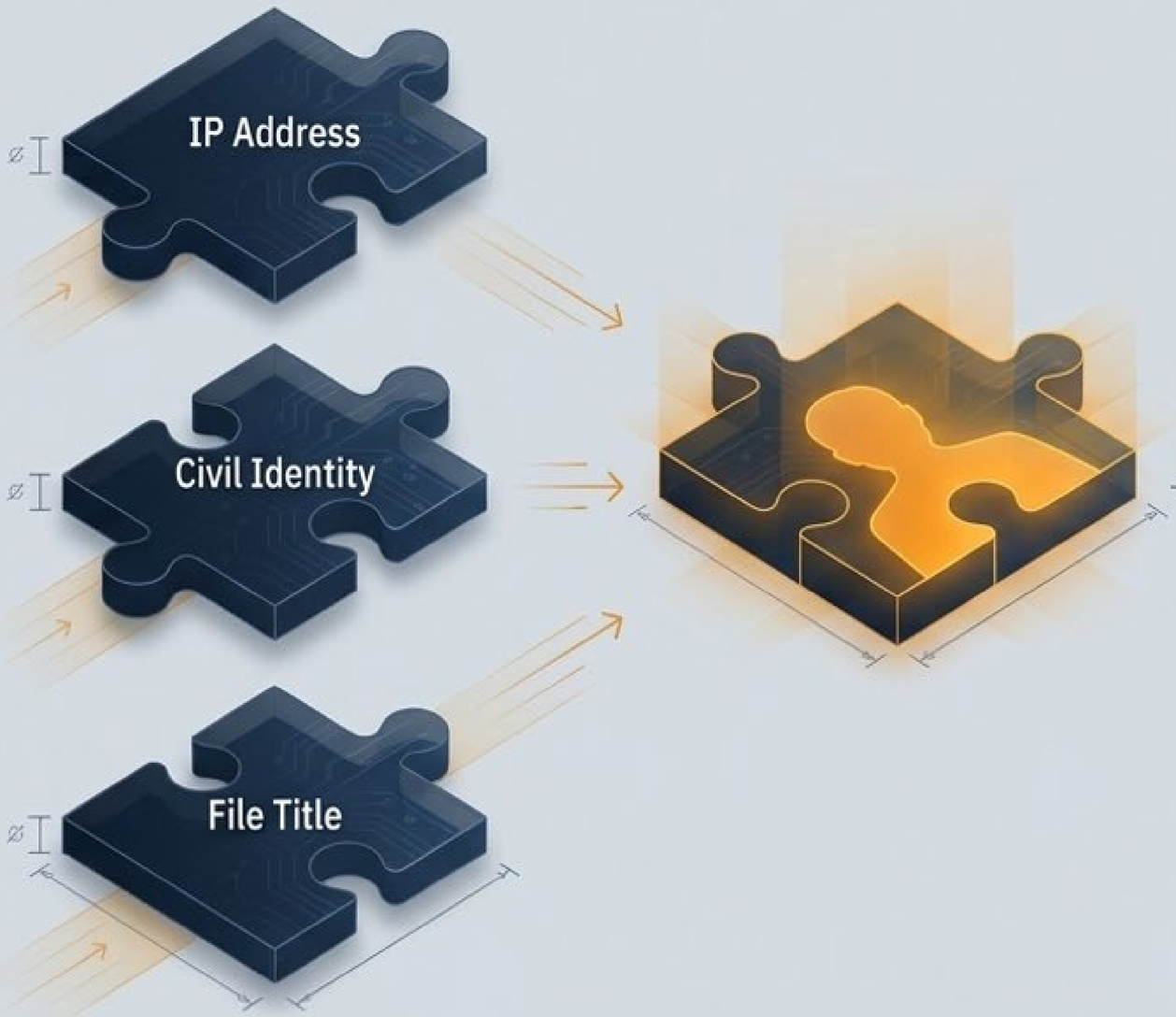


Before the authority can link the civil identity to the file titles to issue a notification of gross negligence or refer the case to prosecutors, an independent court or administrative body must approve the access.





The profiling anomaly: When isolated data becomes sensitive



The Trigger: An individual repeatedly (or on a large scale) infringes copyright on P2P networks.

The Accumulation: With each offense, the authority collects more data points linking a specific IP, a specific identity, and specific file titles.

The Atypical Risk: Even without clickstream tracking, repeatedly downloading specific types of files (revealing political opinions, sexual orientation, or health conditions) allows the authority to build a detailed profile of the user.

The Result: The privacy interference abruptly shifts from not serious to severe.

Privacy Rights & Dynamic IP Addresses: The Benedik v. Slovenia Precedent

THE CASE BACKGROUND

UNAUTHORIZED DATA DISCLOSURE

Police obtained subscriber information from an ISP without prior judicial authorization.

IDENTIFICATION VIA DYNAMIC IP

The applicant was identified and later convicted based on a dynamic IP address investigation.

THE ECtHR RULING

DYNAMIC IPs ARE PERSONAL DATA

Even if not directly identifying, IP data can be linked to specific individuals.

REASONABLE EXPECTATION OF PRIVACY

Internet users expect their identities to remain protected unless specific safeguards are met.

JUDICIAL AUTHORIZATION REQUIRED

Accessing data without a court order violates Article 8 due to insufficient safeguards.

Privacy Safeguards: Legal Standards for Data Access

CORE STANDARDS FOR ACCESS

Precise Conclusions

Establishing the threshold for when data reveals specific details of an individual's private life.

Prior Authorization

Identifying the specific authority or independent body empowered to grant data access.

Serious Criminal Offense

Defining the severity of crimes that legally justify the review and access of data.

THE HADOPI CASE RULING (§ 145)

Prior Review Requirement

Courts or independent bodies must review access requests for "gross negligence" offenses.

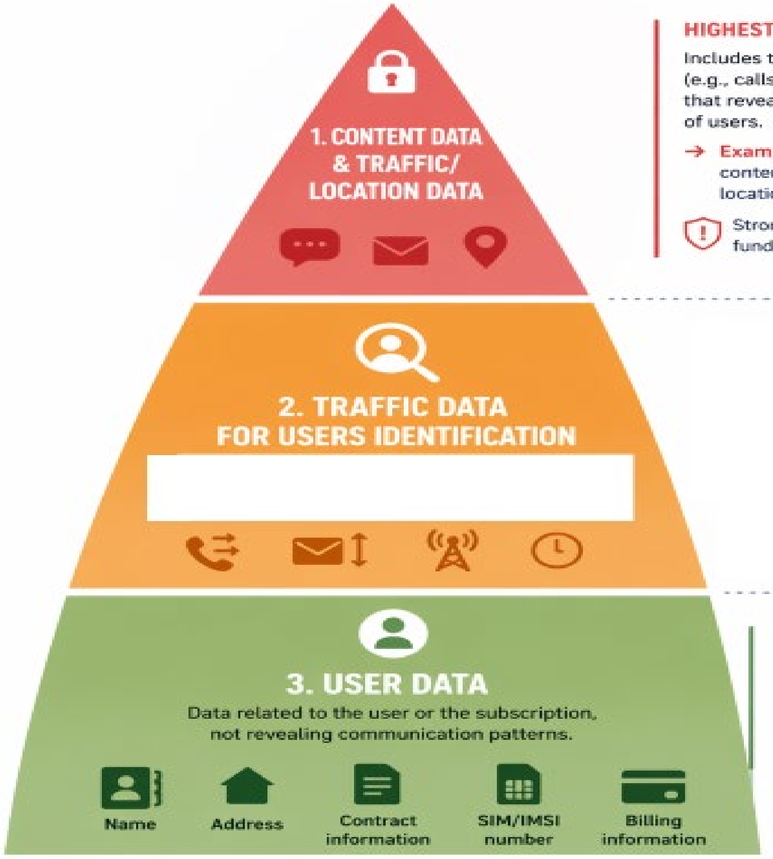
Mandatory Refusal

Access MUST be denied if it allows precise conclusions about a person's private life.

HIERARCHY OF TELECOMMUNICATIONS DATA

Levels of sensitivity and intrusiveness

This classification reflects the increasing level of intrusiveness for privacy and fundamental rights.



HIGHEST LEVEL OF INTRUSIVENESS

Includes the content of communications (e.g., calls, messages, emails) and data that reveals the location and movements of users.

→ **Examples:** call content, message content, internet content, precise location data.

Strongest impact on privacy and fundamental rights.

LOWEST LEVEL OF INTRUSIVENESS

Includes information about the subscriber or the service contract.

→ **Examples:** name, address, contract details, billing information, subscriber ID.

Lowest impact on privacy compared to other levels.

PRINCIPLE OF PROPORTIONALITY

Access to telecommunications data must be strictly necessary and proportionate, with appropriate safeguards and independent oversight, especially for the most intrusive categories (content and location data).

jm.sanchez.s@poderjudicial.es