



The Geospatial Evidence Loophole

Legal Guarantees, Privacy Rights, and the Path to 2026

Faustino Gudín
Vice President EUFJE / PhD Professor UNED



“The use of electronic evidence, does NOT require a different application of the safeguards of the art. 6 § 1... the key consideration is [it] must not be used in a way that compromises the fundamental principles of a fair trial.”

ECHR case *Yüksel Yalçınkaya v. Türkiye* [GC], 2023, §§ 312-313

**Judgment of the ECJ (Third Chamber) of 10 December 2009 —
European Commission v United Kingdom of Great Britain and
Northern Ireland (Case C-390/07) (**

"...contrary to what the United Kingdom asserts, that capture of images by remote sensing cannot, as such, be regarded as unreliable, the United Kingdom itself having recourse to such images to support certain of its arguments." (par.83)

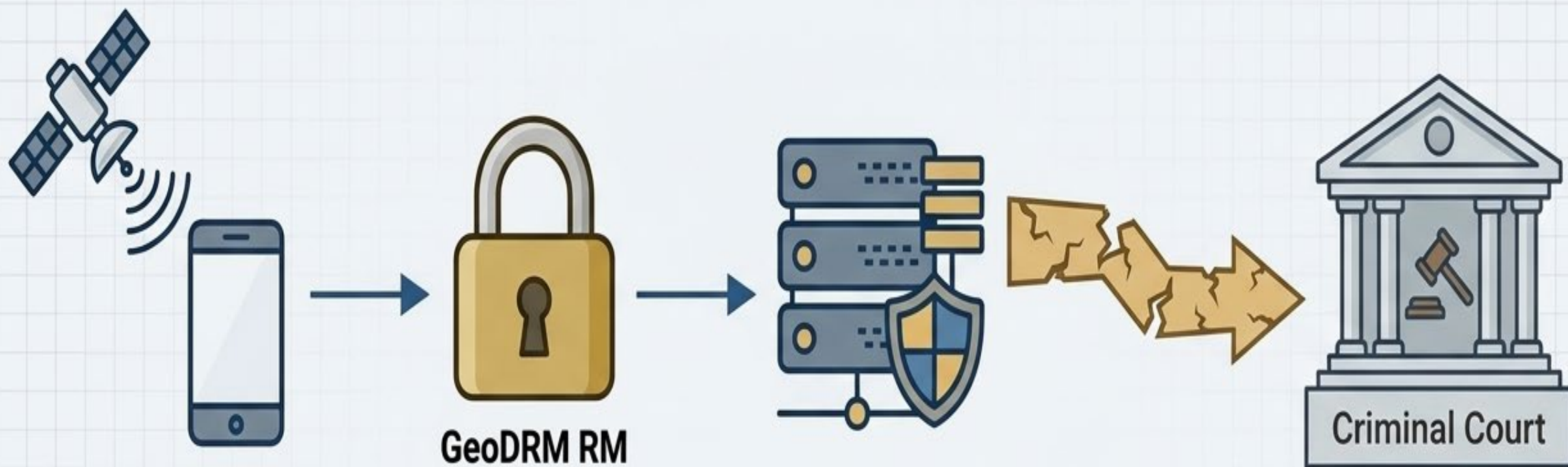
MAIN ISSUES CONCERNING GI AS EVIDENCE:

- OBTENTION
- INCORPORATION TO THE SPECIFIC PROCESS
- TRACEABILITY
- BURDEN OF PROOF
- VALUE OF PROOF (IURIS TANTUM VS. IURIS ET DE IURE)
- PROTECTIVE PRINCIPLES (GUARANTEES) DEPENDING OF WHETHER GI IS INCORPORATED TO
 - CRIMINAL
 - ADMINISTRATIVE (SPECIALLY, INFRACTIONS, FINES AND PROVISIONARY MEASURES)
 - CIVIL
 - LABOUR LAW
- CONFLICTING RIGHTS (DATA PROTECTION, INTIMACY, PRIVATE LIFE...)
- VALID AND INVALID EVIDENCE (EXCLUSIONARY RULE, FRUITS OF THE POISONOUS TREE)

BURDEN OF PROOF VS. VALUE OF PROOF

- BURDEN OF INCRIMINATING PROOF IN BOTH CRIMINAL AND SANCTIONATORY ADMINISTRATIVE LAW IS ALWAYS ON THE GOVERNMENT / PUBLIC PROSECUTORS/ ACTING ADMINISTRATIONS IMPOSING THE FINES
- THERE CAN NOT BE A *IURIS ET DE IURE* PROOF. EVIDENCE PRODUCED BY ACCUSATIONS MUST ALWAYS BE APT TO BE CHALLENGED BY DEFENDANTS. THERE MAY BE STRONG PROOF, OVERWHELMING EVIDENCE, NOTORIOUS PUBLIC KNOWLEDGE... BUT IT CAN NEVER SUPPRESS OR ELIMINATE THE DEFENDANT'S PRESUMPTION OF INNOCENCE.
- WHEN PROOF AGAINST DEFENDANT IS ROBUST ENOUGH, LAWYERS WILL FOCUS ON ATTACKING FORMAL OR SECONDARY ISSUES SUCH AS:
 - THE WAY EVIDENCE WAS OBTAINED (EXCLUSIONARY RULE AND THE FRUIT OF THE POISONOUS TREE DOCTRINE).
 - CHAIN OF CUSTODY (CoC), AND TRACEABILITY (POSSIBILITY OF TAMPERING OR BEING DAMAGED BY TIME OR NEGLIGENT MISHANDLING)

Chain of Custody for Digital Geographic Information



Geospatial Traceability

Complete tracing of product integrity from

Governing Standards

ISO/TC 211 and ISO/DIS 19153 (GeoDRM RM)

**ALL PROCEEDINGS MAY BE DISMISSED IF
THE EVIDENCE IS ILLEGAL**

Attacking the Evidence

The Exclusionary Rule: When the underlying tracking technology is robust, defense strategies pivot to formal or secondary flaws.

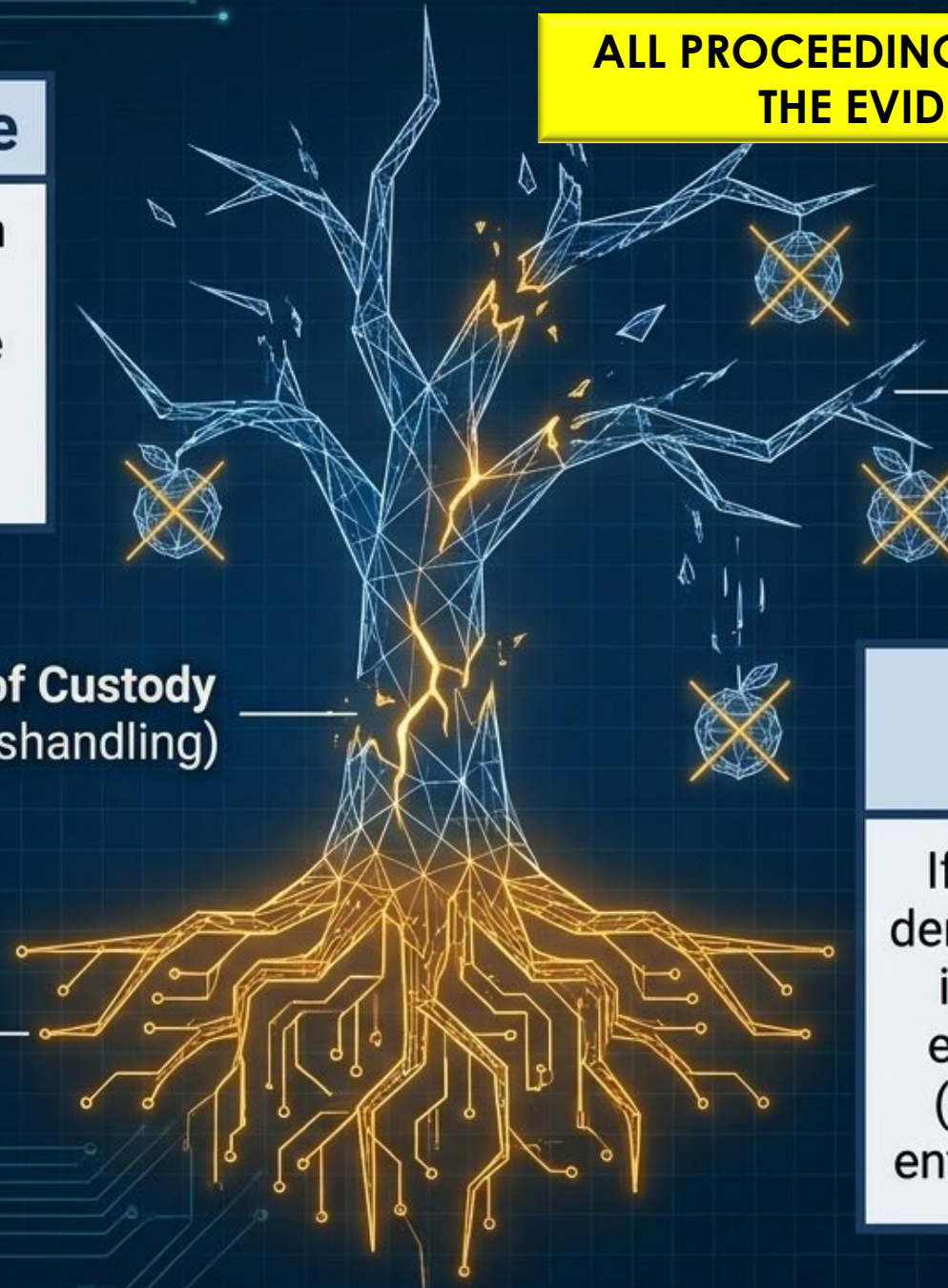
Broken Chain of Custody
(Tampering/Mishandling)

Flawed Obtention
(Illegal Search/Collection)

**Inadmissible
Evidence**

Fruit of the Poisonous Tree

If the source of the evidence (the root) is obtained illegally, all subsequent evidence derived from it (the fruit) is tainted and entirely excluded from trial.



GEOSPATIAL TRACEABILITY

The traceability service allows for the complete tracing product's integrity from its origin to its download. Traceability allows users to verify that data is original and untampered, as well as whether the product has been marked as obsolete



2 legal
considerati
ons

Due diligence

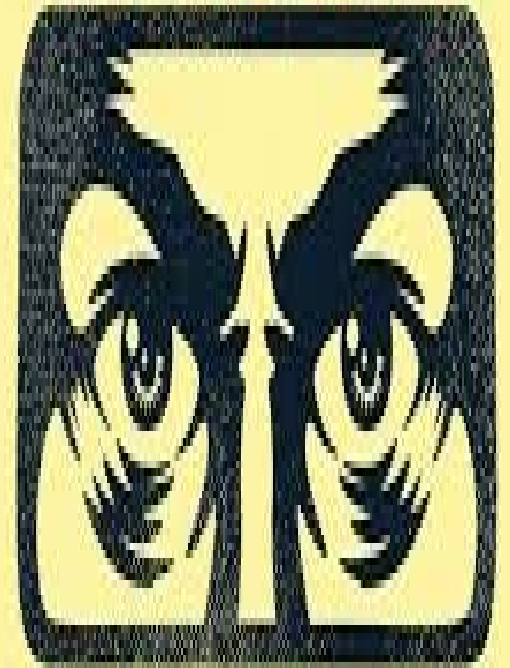
Data Standards and
Interoperability:

DATA PRIVACY (GEOPRIVACY):



- Collecting granular geospatial data raises **SIGNIFICANT PRIVACY CONCERNS**, especially when it can be linked to individuals or small communities (e.g., smallholder farmers).
- Compliance with general **DATA PROTECTION REGULATIONS** (like **GDPR** in the EU, **CCPA** in California) is crucial, requiring explicit consent, data anonymization/pseudonymization, and robust security measures.
- THE CHALLENGE LIES IN BALANCING THE NEED FOR TRACEABILITY WITH PROTECTING INDIVIDUAL PRIVACY**, especially in sensitive contexts (e.g., health data, vulnerable populations).

BIG BROTHER



IS WATCHING YOU

BASIC REGULATIONS

2
IMPORTANT
PIECES OF
EU
LEGISLATION

**DIRECTIVE
2002/58/EC,**
(also known as the
ePrivacy)

- FOCUSES ON PROTECTING PRIVACY AND CONFIDENTIALITY IN THE ELECTRONIC COMMUNICATIONS SECTOR WITHIN THE EU.
- IT REGULATES THE PROCESSING OF PERSONAL DATA AND ADDRESSES ISSUES LIKE ONLINE PRIVACY, CONFIDENTIALITY OF COMMUNICATIONS, AND THE USE OF COOKIES AND OTHER TRACKING TECHNOLOGIES

Guidelines 04/2020
on the use of
location data and
contact tracing
tools in the context
of the COVID-19

GDPR

**ART.4.1 OF THE GDPR
(DEFINITION)
CONSIDERS
LOCATION DATA TO
BE PERSONAL DATA**

THEREFORE, AS PERSONAL DATA, THE
LOCATION OR GEOLOCATION OF
INDIVIDUALS FALLS UNDER THE UMBRELLA
OF THE GDPR, WITH ALL THE
OBLIGATIONS CONTAINED THEREIN FOR
THE MANAGEMENT AND PROTECTION OF
SUCH INFORMATION BEING APPLICABLE.

**EU E.EVIDENCE
PACKAGE**

**Regulation (EU)
2023/1543**

Introduces binding legislative rules that
streamline cross-border electronic data
sharing for authorities.

**Directive (EU)
2023/1544**

Obligates digital service providers offering
services in the EU to designate a legal
representative or establishment to receive
these orders

INTERNATIONAL STANDARDS: ISO/TC 211



It's a standard technical committee formed within ISO, tasked with covering the areas of digital geographic information (such as used by geographic information systems) and geomatics. It is responsible for preparation of a series of International Standards and Technical Specifications numbered in the number range starting at ISO-19101.



THE GOAL IS THE STANDARDIZATION IN THE FIELD OF DIGITAL GEOGRAPHIC INFORMATION

ISO/DIS 19153 Geospatial
Digital Rights
Management Reference
Model (GeoDRM RM)



**NOT FIT TO BE USED IN
CRIMINAL LAW**

EU E.EVIDENCE PACKAGE

Regulation (EU)
2023/1543 and
Directive (EU)
2023/1544,

**BECOME
DIRECTLY
APPLICABLE
ON AUGUST
18, 2026**

**THE EU E-EVIDENCE REGULATION DOES APPLY TO
STORED GEOLOCATION DATA IF IT IS HELD AS TRAFFIC
OR TRANSACTIONAL DATA BY A COVERED SERVICE
PROVIDER, BUT IT DOES NOT APPLY TO REAL-TIME LIVE
TRACKING OR LIVE LOCATION MONITORING**

NO FUTURE DATA

ONLY COMMUNICATIONS DATA:
address to communication
services providers, such as
internet access services,
interpersonal communications
services, etc.

**EU E.EVIDENCE
PACKAGE**

Regulation (EU)
2023/1543 and
Directive (EU)
2023/1544,

**EUROPEAN
PRODUCTION
ORDER**

Hand over actual data
(content, traffic, or subscriber
data) to authorities.

Within 10 days of
receipt.

Within 8
hours in
urgent
cases.

**EUROPEAN
PRESEVATION
ORDER**

Freeze/lock data to prevent
deletion or modification.

Immediately upon
receipt.

Lasts for 60 days,
extendable by
another 30 days.

European Production Order

With the e-evidence proposal, this is how an EU law enforcement authority would obtain e-evidence from a service provider.



Mutual Legal Assistance (MLA)

Based on the current MLA procedure, this is how an EU law enforcement authority would obtain e-evidence from a U.S. service provider.



GDPR

GDPR

ART.6.1 OF THE
GDPR CONSIDERS
LOCATION DATA
TO BE PERSONAL
DATA

Recital 75 Risks to
the Rights and
Freedoms of
Natural Persons

DATA IMPACT
ASSESSMENT
AND PRIOR
CONSULTATION
(Article 35):

➤ **LAWFULNESS OF PROCESSING:**

- Processing geolocation data, like any personal data, must have a valid legal basis (e.g., explicit consent from the user).

location or movements, in order to create or use **personal profiles**; where personal data of vulnerable natural persons, in particular involves a large amount of personal data and affects a large number of data subjects.

THEREFORE, AS PERSONAL DATA, THE LOCATION OR GEOLOCATION OF INDIVIDUALS FALLS UNDER THE UMBRELLA OF THE GDPR, WITH ALL THE OBLIGATIONS CONTAINED THEREIN FOR THE MANAGEMENT AND PROTECTION OF SUCH INFORMATION BEING APPLICABLE.

EU Regulation and Digital Monitoring Technologies



Deforestation (EUDR 2023/1115)

Verifiable geolocation data integrated into an EU-wide system to prove deforestation-free origins.



Maritime Pollution (Dir 2005/35/EC)

EMSA CleanSeaNet satellite surveillance to detect oil spills and effectively penalize offenders.



Invasive Alien Species (Reg 1143/2014)

JRC-developed app for citizen-led geolocated observation tracking.

EU DEFORESTATION REGULATION 2023/1115

The Regulation (EU) 2023/1115 introduces a *new legal model of environmental traceability*. It targets the **entire supply chain** of certain commodities linked to deforestation and forest degradation (e.g., wood, cattle, soy, cocoa, palm oil, coffee, rubber).

The core principle:

Products entering or leaving the EU market must demonstrate a deforestation-free origin, proven through verifiable geolocation data integrated into an EU-wide information system.

THREE- PILLAR SYSTEM

**Pillar 1. Due
Diligence Obligation
(Articles 3, 4, 9)**

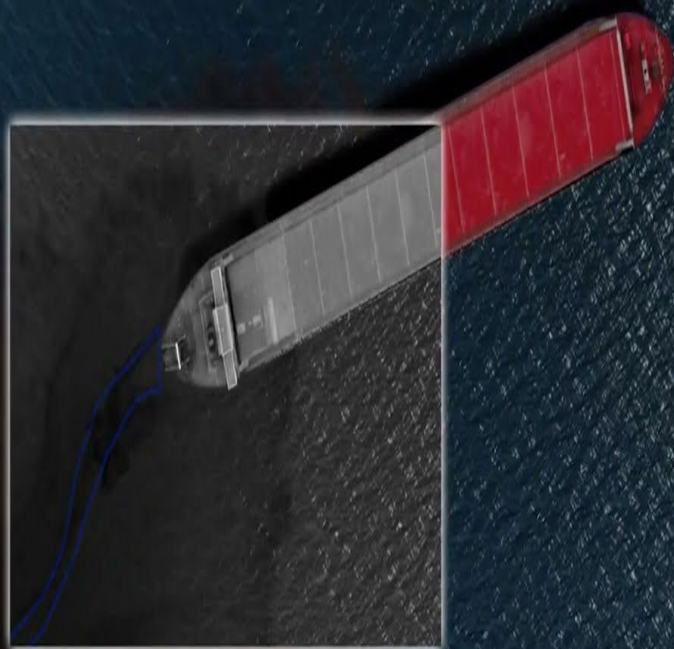
**Pillar 2. Centralised
Information System
(Article 33)**

**Pillar 3. Technical
Assistance and
Harmonisation
(Article 15)**



2023 EU'S REVISED REGULATION ON SHIP-SOURCE POLLUTION REGARDING DIRECTIVE 2005/35/EC

EMSA



EMSA CLEANSEANET

The European satellite-based oil spill
and vessel detection service.

CleanSeaNet is optimised through enhanced satellite surveillance and better exchange of information between Member States for all MARPOL annexes.

This would help build Member States' capacity to detect pollution incidents, collect evidence and effectively penalise offenders in a proportionate, timely and harmonised manner

INVASIVE ALIEN SPECIES EUROPE APP

TOOL FOR REGULATION (EU) 1143/2014 ON IAS (EASIN)

DEVELOPED BY THE JOINT RESEARCH CENTRE (JRC) OF
THE EUROPEAN COMMISSION



PURPOSE:



Engage citizens (amateurs and professionals) in tracking and sharing data on Invasive Alien Species (IAS) in Europe.



MAIN FUNCTIONS:



Record geolocated IAS observations via smartphone GPS and camera



Access detailed information on selected IAS: images, brief descriptions, and useful data.



CJEU Judgments: Differentiating Rules on Data Retention & Access

1. La
Quadrature
du Net (Oct
2020)

Focus: Data
Retention

❌ **Blanket Retention is Illegal.** No general or indiscriminate data collection is allowed.

✅ **Exception: Only Applicable to Genuine National Security Threats and strictly time-limited**
Requires independent oversight

🔍 **Why It Matters:** Defines when and how states can retain data — only in extreme, national security cases, not for ordinary crime prevention. 🔍

🔍 2.
Prokuratuur
Mar 2021)

Focus: Data Access &
Oversight

🔴 **Accessing Sensitive Data Requires More than a Green Light:** Access to **location data** is restricted to **serious crime** or **major threats**.

Approval must come from a **truly independent body** — **prosecutors may not qualify**.

⚖️ **Why It Matters:** Sets a **strict standard for judicial independence** in authorizing data access. Reinforces **checks and balances** in surveillance.

ECHR: GUARANTEES ON GEOLOCATION: KEY RULINGS

- **UZUN V. GERMANY (2010): Establishing Proportionality for Less Intensive Surveillance** The ECHR affirmed that systematic data collection, even with hidden GPS, constitutes interference with private life but deemed GPS tracking less intensive than other surveillance. German law, allowing such surveillance with judicial oversight, time limits, and justification by crime seriousness, was found adequate due to its **proportionality and legal basis for less intensive interferences**.
- **ZUBKOV AND OTHERS V. RUSSIA (2017): INSUFFICIENT SAFEGUARDS FOR RETROSPECTIVE DATA ACCESS:** The Court found a violation of Article 8 ECHR when Russian authorities accessed **retrospective mobile phone location data (from cell tower records) without adequate judicial authorization or effective oversight**. This case highlighted the necessity of robust safeguards for accessing historical location data revealing patterns of movement.
- **BEN FAIZA V. FRANCE (2018): REQUIREMENT FOR CLEAR AND FORESEEABLE LEGAL BASIS FOR REAL-TIME SURVEILLANCE:** The ECHR found a violation regarding real-time GPS surveillance due to a **lack of sufficient clarity and foreseeability in the French legal framework** at the time ("acts useful to the search for truth" was deemed not to meet the quality-of-law standard). This judgment underscored that real-time geolocation surveillance demands a precise and foreseeable legal basis to meet rule of law requirements.
- **FLORINDO DE ALMEIDA VASCONCELOS GRAMAXO V. PORTUGAL (2022): TRANSPARENCY AND PURPOSE IN EMPLOYER SURVEILLANCE:** The Court found **no violation of Article 8** when an employer used GPS data from a company vehicle to dismiss an employee, even with a second hidden GPS. The key factor was the **employee being informed about the initial GPS installation and its purpose**, emphasizing the importance of transparency and proportionality in workplace surveillance.

CONCLUSIONS

The defenseless situation of the environment demand new tools to protect it.

The integration of geospatial data into legal proceedings creates significant tensions regarding the fundamental right to a fair trial.

The EU E-Evidence Package establishes a binding legal framework to streamline cross-border digital investigations but leave critical loopholes by failing to adequately regulate real-time live tracking and future data collection.

A specialized EU protocol is urgently required to resolve these gaps and properly govern the use of digital geolocation evidence.

Developing this specific protocol ensures that the collection of geospatial data strictly respects individual privacy protections



Thank You.

Faustino Gudin
Vice President EUFJE
PhD Professor UNED
f.gudin@poderjudicial.es