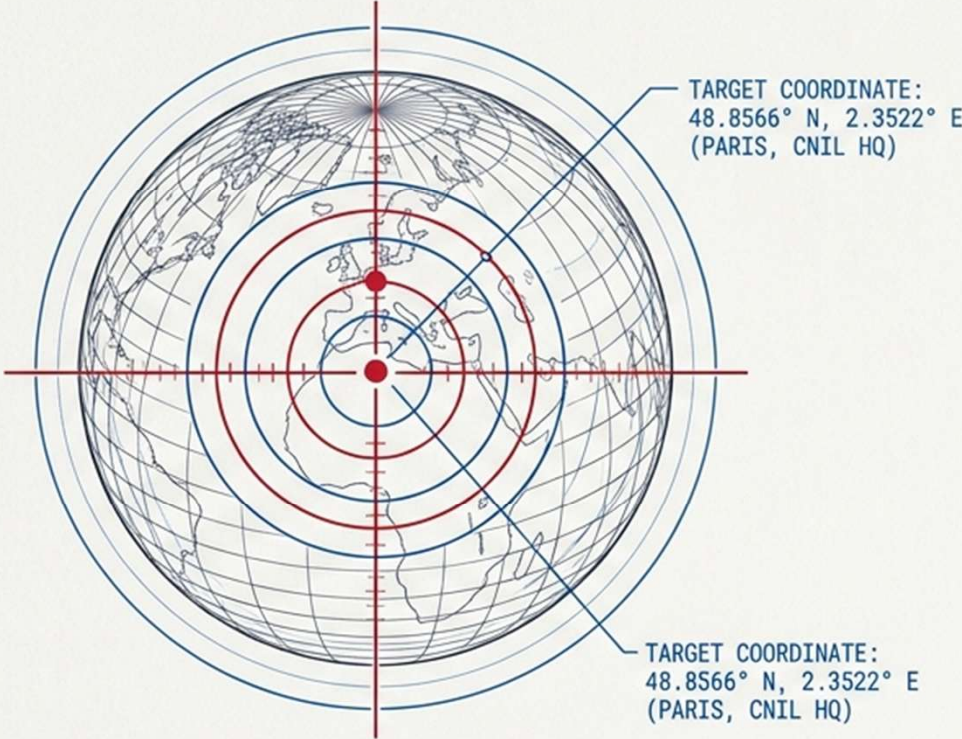




How CNIL Finds Non-Compliant Websites

And Why Your Business is More Visible Than You Think.

CNIL SURVEILLANCE VECTORS

AUTOMATED DETECTION	MANUAL & REPORT-BASED
WEB CRAWLERS & BOTS: [ACTIVE]	USER COMPLAINTS: [PRIORITY]
COOKIE SCANNING: [AUTOMATED]	AUDIT TRIGGER: [MANUAL REVIEW]
DATA LEAK DETECTION: [MONITORED]	CROSS-AGENCY INTEL: [SHARED DATA]
COMPLIANCE SCORING: [ALGORITHMIC]	PUBLIC BREACH REPORTS: [ANALYZED]

VISIBILITY FACTORS

TRACKING TECHNOLOGIES: [HIGH RISK]
DATA TRANSFER PATHS: [EXPOSED]
CONSENT MECHANISMS: [AUDITED]
THIRD-PARTY INTEGRATIONS: [VULNERABLE]
REGULATORY WARNING: NON-COMPLIANCE RISK IS CRITICAL. IMMEDIATE AUDIT RECOMMENDED. [CNIL.FR] [DASHBOARD]

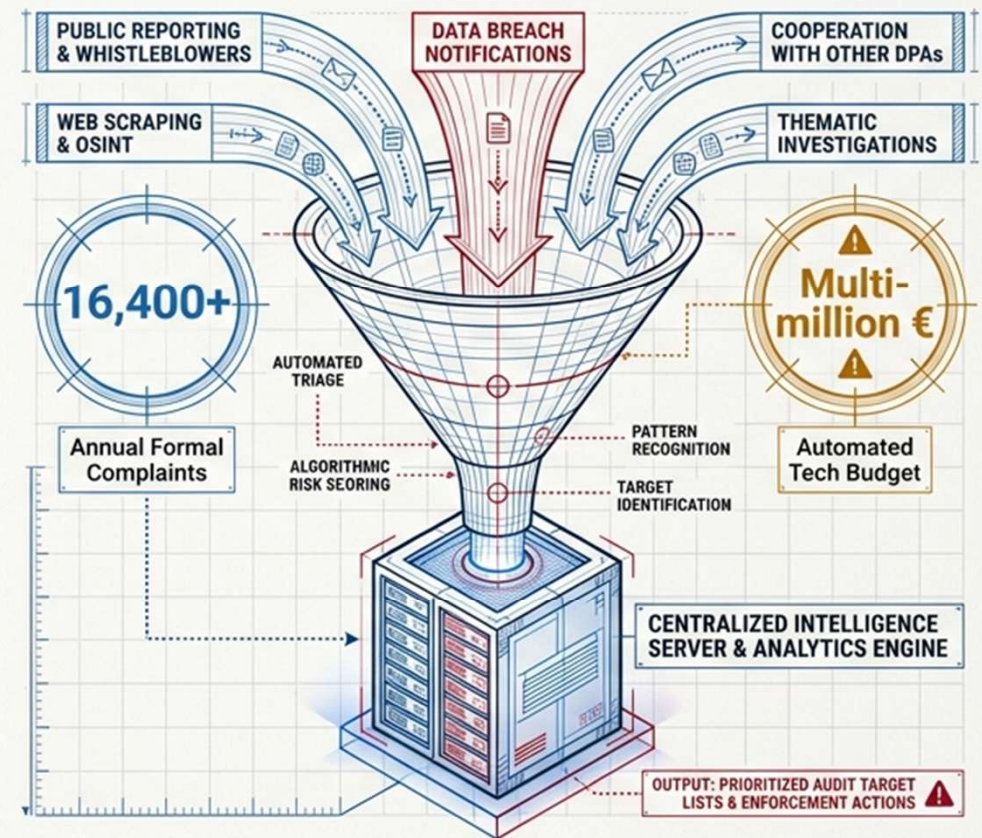
THE REACTIVE MYTH

The dangerous assumption that regulators simply wait for major disasters or massive breaches before launching investigations.



THE INDUSTRIAL-SCALE REALITY

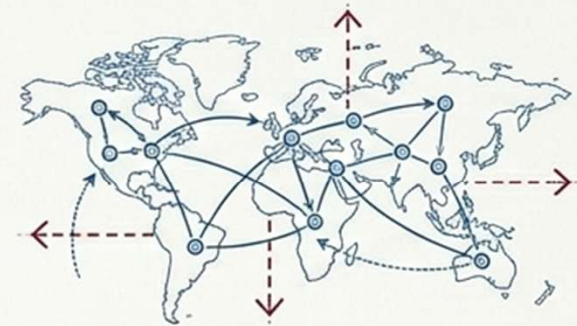
CNIL does not rely on chance discovery. They have built the infrastructure to find you at scale.



Origin: Human vs. System



Individual Complaints



NGO & Cross-Border Referrals



Automated Web Scanning



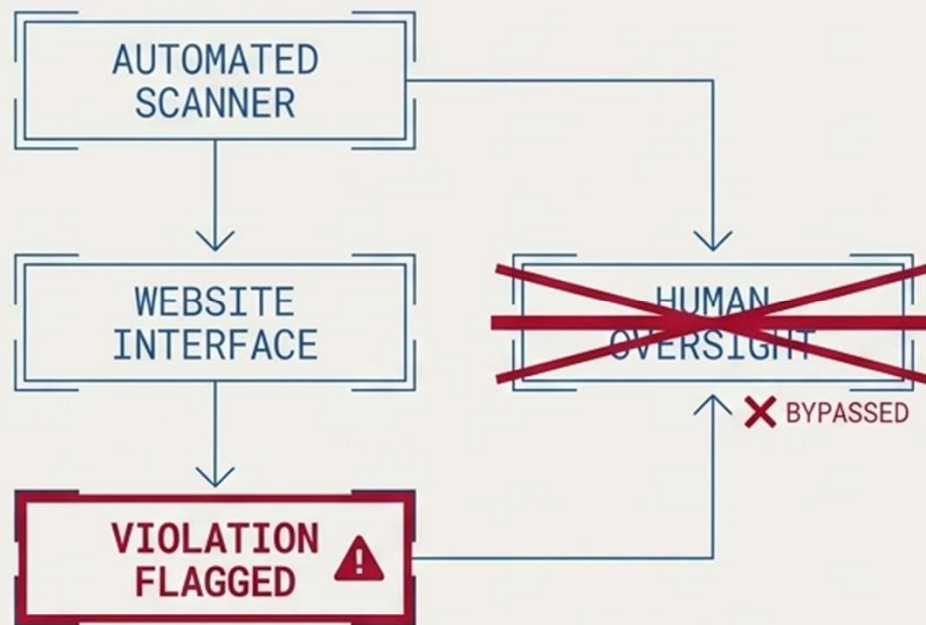
Sector-Wide Campaigns

Scale: Individual vs. Coordinated

Detection relies on **five unavoidable vectors**. You don't need a complaint to be discovered, and **distance** offers **zero protection**.

VECTOR 1: THE AUTOMATED SWEEP

CNIL bots sweep sites for cookie compliance without human intervention.
A non-compliant interface can be flagged without anyone ever visiting your site.



EVIDENCE BLOCK 01

Google: **€150M Fine** (2022)



EVIDENCE BLOCK 02

Meta: **€60M Fine** (2022)



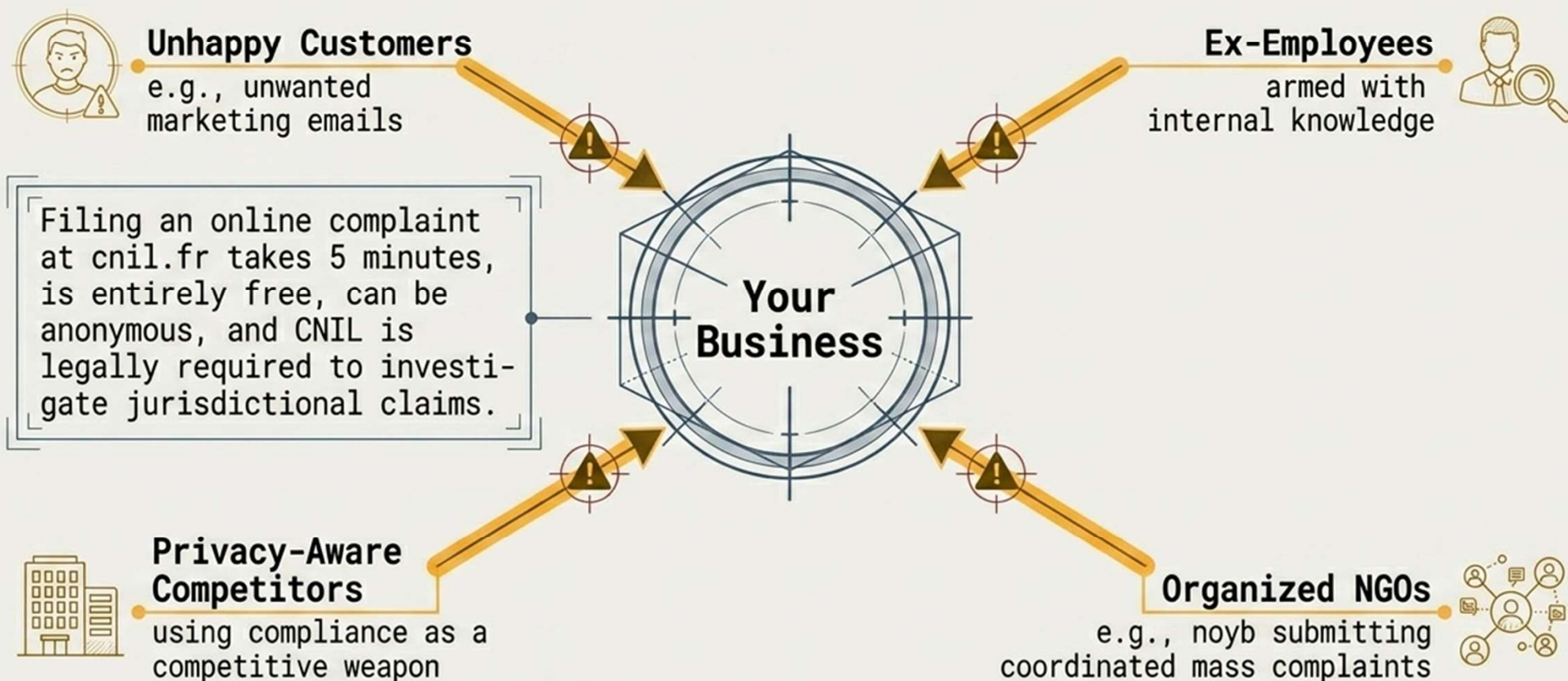
EVIDENCE BLOCK 03

Bing: **€60M Fine** (2022)



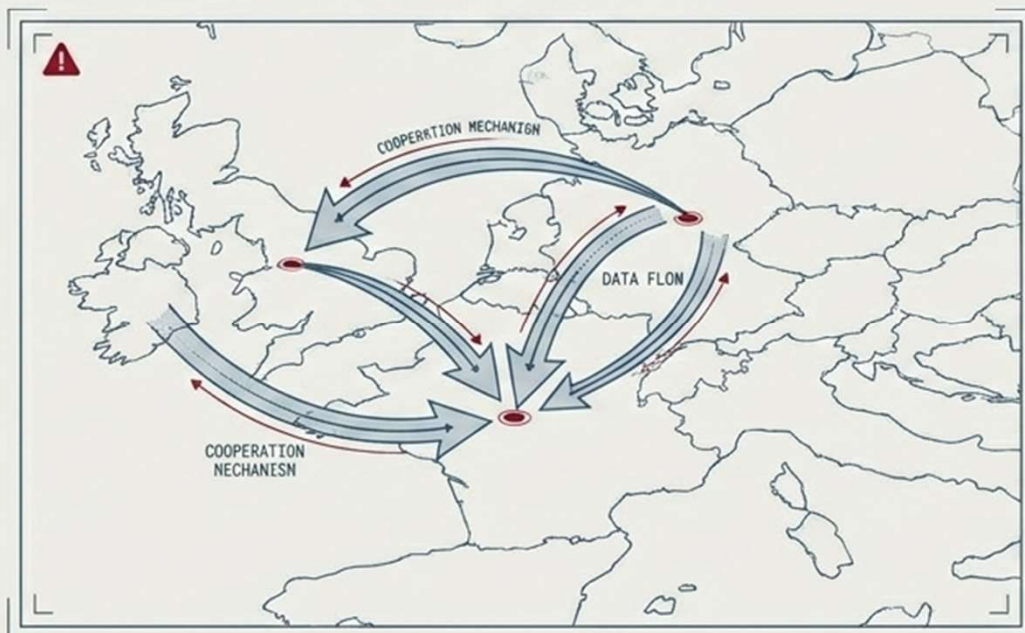
If tech giants' interfaces are automatically flagged, **smaller unmonitored sites** are **completely visible** to the sweep.

Vectors 2 & 5: The Human Triggers



Vectors 3 & 4: No Place to Hide

Distance is Not a Shield



Under GDPR cooperation mechanisms, if you target French consumers, geographic distance offers zero protection. CNIL actively coordinates with foreign DPAs (e.g., Germany, Ireland) to investigate external threats.

CNIL's Targeted Sectors

HIGH RISK TARGETS ⚠

- [+] Health & Medical platforms
- [+] HR & Recruitment job boards
- [+] Adtech & Online advertising
- [+] Children's platforms
- [+] E-commerce operations



Website X-Ray: What The Scanners Actually See

Takeaway: The code you don't see is exactly what the regulator's automated bots are looking at.

The Entry: Background Scripts

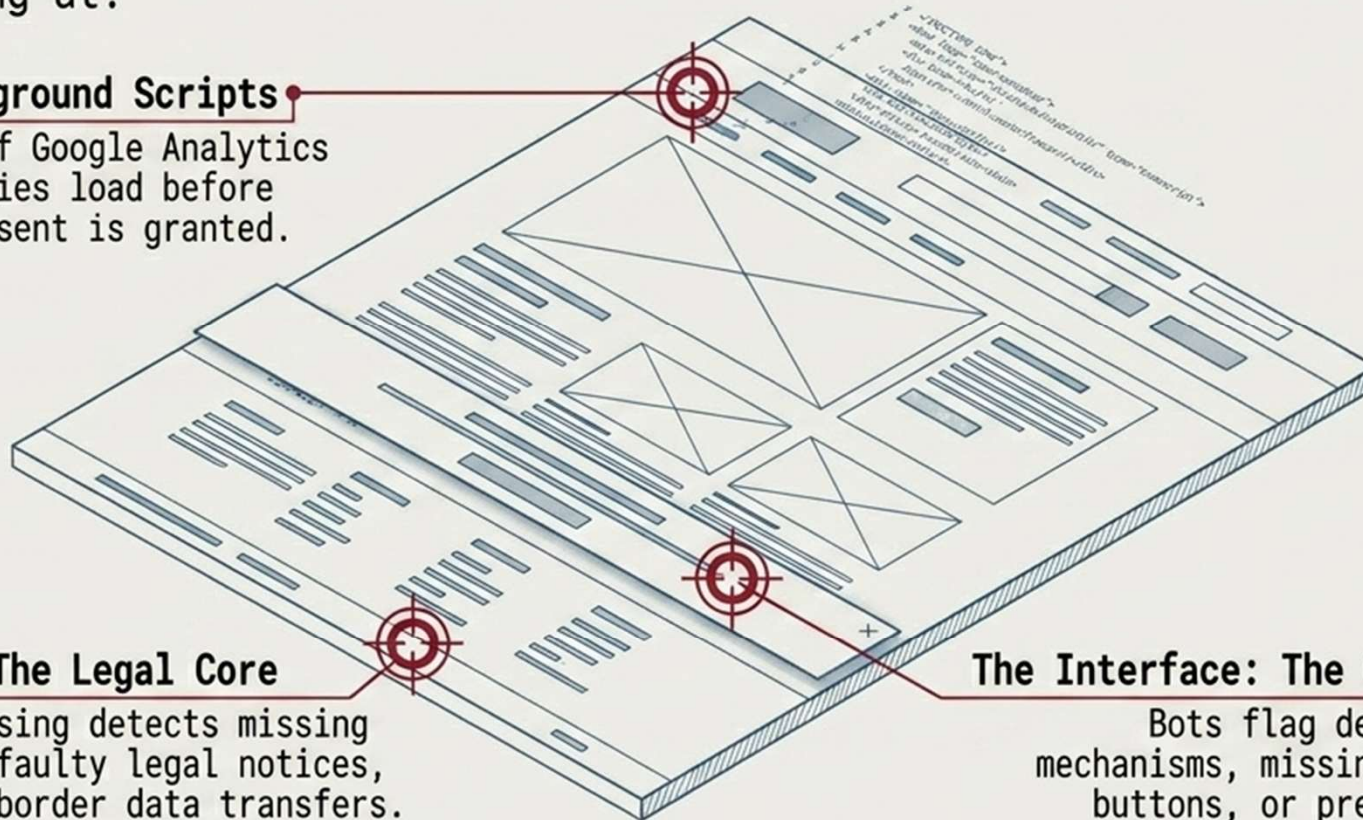
Scanners detect if Google Analytics or marketing cookies load before explicit user consent is granted.

The Foundation: The Legal Core

Automated text-parsing detects missing privacy policies, faulty legal notices, and exposed cross-border data transfers.

The Interface: The Cookie Banner

Bots flag deceptive cookie mechanisms, missing 'Reject All' buttons, or pre-ticked boxes.



Remediation Protocol: If You Are Exposed

1. Do Not Ignore



Formal notices have strict deadlines. Ignoring them upgrades a procedural issue into a severe violation.

2. Map Your Architecture



Instantly audit data flows, script loading orders, and cookie triggers.

3. Deploy Rapid Fixes



Close the technical gaps (banners, blocking scripts) before human investigators escalate the automated flag.

Legal Notice: This briefing does not constitute legal advice. If you receive formal communication from CNIL or any DPA, consult a qualified privacy lawyer immediately.

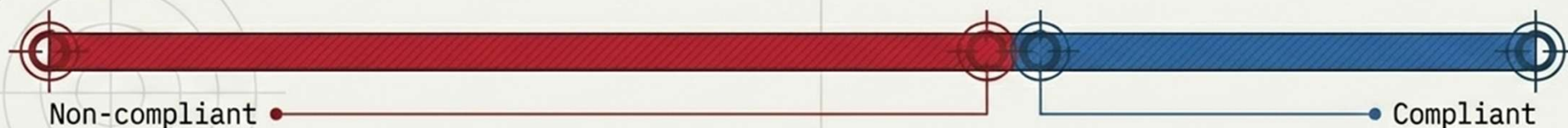
The Sitetals Reality Check

606,000+

Websites reviewed by Sitetals technology

46%

Fully compliant



Independent EU compliance monitoring designed for websites operating in France and Germany. See exactly what CNIL's tools would find on your site—before they do.

The question isn't if CNIL can find you. It's whether there's anything to find.

[Run a Free Sitetals Scan]

- Validates cookie consent
- Parses legal notices
- Audits data transfers

Results in under 60 seconds.

[Scan Your Website Now]

SiteTals.com | hello@sitetals.com