Observatoire ARGA

ARGA Atlas

HIDDEN INTERPOL TOOLS

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA, ARGA Atlas

Mailing address: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org, https://www.arga-atlas.com/

Anglet, 4 avril 2026

Purpose of the document:

This report is prepared to analyze those instruments of international police cooperation within the INTERPOL system which, in practical defense work, are often less visible than a Red Notice but are capable of generating comparable or even more difficult-to-detect transnational risk. The focus is primarily on diffusions, blue notices, message-based circulation, less visible categories of data exchange, and the procedural and institutional practices that allow states or National Central Bureaus to use international channels not only through the most public forms, but also through less transparent means of data dissemination. The practical function of the report is to demonstrate that a significant part of the threat to a client does not arise where there is a widely discussed public notice, but where data circulate within the system without sufficient external visibility and with a lower level of procedural recognition by the person concerned and their representatives. For ARGA, this topic is strategically important because a defense model focused only on Red Notices is increasingly late and incomplete. (interpol.int)

CONTENTS

1. Executive Summary

In public perception, the INTERPOL system is still associated primarily with the Red Notice. From the perspective of real transnational defense, however, that image is incomplete and potentially dangerous. INTERPOL expressly states that not all Red Notices are public, and the Rules on the Processing of Data apply not only to notices, but also to diffusions and messages. In addition to Red Notices, practice is shaped by blue notices, diffusions, direct police-to-police exchanges routed through National Central Bureaus, and other forms of data circulation within the INTERPOL Information System. These are precisely the tools that often create a situation in which a person is already exposed to arrest risk, heightened border control, extradition-related action or intelligence-based scrutiny without having any obvious confirmation that a public notice exists. (interpol.int)

The CCF's 2024 statistics confirm that the problem is not marginal. Among admissible requests from applicants actually subject to data, 59 percent concerned notices, but 29 percent concerned diffusions. That is an extremely significant share, especially given that diffusions generally attract less public attention and less immediate defensive recognition. Moreover, INTERPOL itself distinguishes between notices, which go through a more centralized review and publication logic, and diffusions, which are circulated directly by an NCB to selected or all member countries through the I-24/7 network. In practical terms, this means that hidden risk may already be embedded in the architecture of exchange before the defense has even begun to contest any "officially visible" notice. (interpol.int)

The central conclusion of this report is that hidden INTERPOL tools should not be treated as peripheral, but as a core element of the contemporary transnational risk environment. Defense must proceed from the presumption that the absence of a public Red Notice does not mean the absence of INTERPOL-related exposure. Successful work therefore requires prior inquiry into the possible existence of diffusions, blue notices, non-public notices, message traffic and derivative data circulation, as well as a strategy aimed not only at deletion, but at early detection, process mapping and multilevel mitigation. Everything else too often amounts to belated surprise, and belated surprise is almost never a useful legal resource. (interpol.int)

2. Context & Problem Statement / Why This Topic Has Legal and International Significance

The legal and international importance of hidden INTERPOL tools lies in the fact that international police cooperation has long moved beyond the boundaries of a single public symbol. A Red Notice is convenient as an object of public discussion, media attention and initial client diagnostics. But operational reality is significantly broader. INTERPOL's own legal documents make clear that its data architecture includes notices, diffusions and messages, along with other forms of circulation through the INTERPOL Information System. When defense is focused exclusively on whether there is a public Red Notice on the website, it is effectively replacing the question of the full extent of transnational risk with the question whether the most recognizable sign of that risk is present. (interpol.int)

For international legal practice this has several implications. First, the risk of detention or mobility restriction may arise without a publicly visible marker. Second, extradition and other coercive consequences may be triggered by data of which the person becomes aware only ex post, for example at the border, in visa refusal, through banking screening or in intelligence-led police action. Third, the asymmetry of information between the system and the individual becomes especially pronounced: the state and the NCB know what data were circulated and where, while the affected person often knows only that, at some point, "something fired." It is precisely on this terrain that some of the most serious defense failures are born. (interpol.int)

This topic is especially important for ARGA because hidden tools are often used where heightened scrutiny is undesirable. If a public notice would draw too much attention, trigger a rapid Article 3

challenge, intensify a human-rights response or make abuse too visible, less visible data channels become institutionally attractive. This does not mean that every diffusion or blue notice is abusive by nature. It does mean, however, that any defense strategy that ignores such tools is structurally behind the real operational practice. (interpol.int)

3. Legal Framework / Normative and Institutional Framework

The primary normative framework remains the Constitution of INTERPOL, the Rules on the Processing of Data, the procedural framework of the CCF and the official explanatory materials of INTERPOL on notices and diffusions. The RPD expressly define a notice as a request for international cooperation or alert allowing police in member countries to share critical crime-related information, and a diffusion as a message sent directly by one NCB or international entity to one or more countries through the I-24/7 network. Both categories are subject to rules on data quality, lawfulness, purpose and compatibility with the Constitution. Accordingly, the hidden character of a tool does not place it outside compliance review. The legal problem lies not in the absence of rules, but in the unevenness of visibility and practical access to challenge. (interpol.int)

A particularly important issue is the distinction between public and non-public notices. INTERPOL's public materials state that not all Red Notices are public and that only extracts of some notices are published on the website. This means that even with respect to Red Notices, public availability is optional rather than mandatory. A simple check of the INTERPOL website therefore cannot be treated as an exhaustive risk assessment. This point is legally critical because many individuals, and even some representatives, wrongly interpret the absence of a public notice card as proof that no notice exists at all. (interpol.int)

The Blue Notice also has distinct significance. INTERPOL defines it as a request to collect additional information about a person's identity, location or activities in relation to a criminal investigation. Although a Blue Notice is not arrest-oriented in the same manner as a Red Notice, it should not be underestimated. It may perform preparatory, intelligence-gathering and localization functions, thereby creating a platform for later coercive escalation. In transnational repression or corporate-conflict misuse cases, Blue Notices may thus operate as low-visibility, surveillance-like procedural instruments embedded in lawful-looking channels of police cooperation. (interpol.int)

The CCF maintains jurisdiction over requests for access, correction and deletion concerning personal data processed in INTERPOL systems, including notices and diffusions. The 2024 Annual Activity Report again confirms that admissible requests concern both categories in meaningful numbers. A protective route therefore formally exists. Practically, however, it remains post hoc, confidential and dependent on the applicant's ability to suspect and articulate hidden circulation. This is precisely where the legal framework confronts its operational limitation. (interpol.int)

4. Mechanisms of Practice / Abuse / Key Mechanisms of Practice, Abuse, or Conflict

The first mechanism of hidden use is the substitution of a highly visible centralized notice with a less visible diffusion. Diffusions may be circulated directly by an NCB to selected or all member countries. Although they remain subject to the INTERPOL legal framework, their operational profile differs: they are faster, less public and often less visible to the person concerned. This makes diffusion a convenient instrument where the initiating side wants international effect without the burden of public exposure. In practical terms, this may mean that a person experiences alert-like consequences without any public-facing trace. (interpol.int)

The second mechanism concerns the use of the Blue Notice as a low-visibility inquiry tool. Under the pretext of gathering information about location, identity or activities, states may in practice initiate international tracing or checking of a person who is not yet under public notice-based scrutiny. Even

where a Blue Notice does not directly generate arrest exposure, it may reinforce a later prosecution architecture by mapping the person's movement, connections and traceability. This is especially sensitive in cases where international mobility is itself central to the protection strategy. (interpol.int)

The third mechanism concerns message-based circulation and derivative data use. The RPD cover messages as part of the data-processing framework, and INTERPOL's system architecture permits significant police-to-police communication through NCBs and I-24/7. In some cases it is this message traffic, rather than a formal public-facing notice, that creates operational awareness, precautionary action or border-based scrutiny. For the defense, the difficulty is double: the risk is real, yet especially hard to prove before it materializes into an event. (interpol.int)

The fourth mechanism appears through cumulative layering. A state or NCB may use a combination of domestic warrants, non-public notice circulation, diffusions, blue notices, bilateral contacts and subsequent extradition requests. No single element, considered in isolation, looks maximally dramatic. Taken together, however, they form an effective architecture of transnational pressure. It is precisely the cumulative character of hidden tools that makes them especially dangerous: defense too often assesses each instrument separately and loses sight of the overall trajectory of coercive escalation. (interpol.int)

5. Case Patterns / Typical Scenarios, Patterns of Development, or Practice Models

The first typical scenario is the absence of a public Red Notice despite actual travel-related disruption. The person does not find themselves on the INTERPOL website and therefore assumes that international circulation is absent. Yet detention at the border, secondary questioning, refusal of boarding, a sudden visa problem or a request for local police contact later occurs. In such cases, one plausible explanation is that data were circulating through non-public channels, including diffusions or non-public notices. This scenario demonstrates how dangerous it is to equate public visibility with legal non-existence. (interpol.int)

The second scenario concerns preparatory use of Blue Notices. At an early stage, a state may not yet be ready for full red-notice-style escalation or may wish to avoid immediate challenge. Instead, it seeks information about the person's location and activities. For the affected individual, this phase often remains entirely invisible, yet it can later support more aggressive measures. The defense thus confronts not an isolated notice event, but an already prepared dossier built through incremental cross-border data gathering. (interpol.int)

The third scenario includes corporate or politically sensitive cases, where a public notice would attract scrutiny under Article 3 or generate reputational backlash for the requesting side. In such settings, lower-visibility tools may be preferable because they preserve operational effect while reducing transparency. This is especially important in cases of politico-economic persecution, sanctions-related disputes or conflicts over beneficial ownership, where the requesting actor does not necessarily need a loud public search, but rather controlled international friction around the target. (interpol.int)

The fourth scenario concerns defense failure through under-detection. Counsel performs a formal request or advisory assessment only around Red Notice risk and, after receiving a negative answer or finding no public record, closes the analysis. Meanwhile, the person remains subject to other categories of data. The CCF statistics confirming a substantial proportion of diffusion-related requests show that this is not a theoretical possibility, but a recurring operational reality. (interpol.int)

6. Risk Assessment / Main Risks, Legal Vulnerabilities, and Problem Areas

The first risk is false-negative diagnosis. The absence of a public notice creates a false sense of safety. For the client, this may mean continued travel, absence of urgent protective steps, delayed asylum coordination, unprepared border crossings and unmanaged extradition exposure. For counsel, it means a strategic error at the earliest stage. (interpol.int)

The second risk concerns asymmetry of information. State authorities and NCBs may know that data have circulated, while the individual does not. Since CCF review is generally triggered by request and remains confidential, the person often enters the process only after reacting to a partially hidden architecture. This asymmetry undermines legal certainty and effective access to remedy, because one cannot challenge in time what one cannot reasonably detect. (interpol.int)

The third risk concerns underestimation of Blue Notices and messages. Because they do not carry the same public reputation as a Red Notice, defense teams tend to regard them as secondary. But information-gathering tools can be operationally decisive, especially where surveillance of movement, tracing of contacts or confirmation of location is enough to trigger later steps. A legally less dramatic instrument may be strategically extremely effective. That is usually how systems behave when they would rather not attract attention. (interpol.int)

The fourth risk concerns fragmentation of remedies. One hidden INTERPOL-related risk may require simultaneous action before the CCF, national courts, asylum bodies, consular actors and compliance stakeholders. If defense treats the hidden tool only as a police-data issue, it underestimates its cascading consequences across legal systems. (interpol.int)

7. Institutional Gaps / Institutional Limitations, Gaps, Deficits of Safeguards, or Systemic Weaknesses

The first systemic weakness is that transparency in the INTERPOL environment is inherently uneven. Public red notice extracts create one visible layer, but a considerable portion of operational relevance lies outside that layer. The legal framework does not disappear outside publicity, yet detectability sharply decreases. This means that the system is more reviewable than fully knowable. For the defense, that is a fundamental problem. (interpol.int)

The second weakness is dependence on post hoc review. The CCF can review data, including diffusions, but generally only after the data exist and after the person or representative has reason to suspect them. This is valuable, but it is not equivalent to prior notice or real-time transparency. In cases involving fast-moving border or extradition risks, that temporal lag can be decisive. (interpol.int)

The third weakness lies in the operational attractiveness of lower-visibility tools. If a highly visible channel invites immediate scrutiny, lower-visibility channels may become functionally preferable for abusive or opportunistic use. The legal system formally regulates all these tools, but regulatory coverage and practical detectability are not the same thing. It is precisely in that gap that many contemporary forms of transnational repression emerge. (interpol.int)

8. Practical Guidance / Practical Recommendations and Model of Legal Action

The first step is to abandon red-notice exclusivity. Any preliminary diagnostic must begin not with the question “is there a public Red Notice?” but with “what categories of INTERPOL-related data circulation may exist in relation to this person?” This changes the entire protective approach and removes the basic blind spot. (interpol.int)

The second step is early symptom mapping. Counsel should record any indications of hidden circulation: unexplained border issues, consular anomalies, sudden screening problems, indirect

police outreach, arrest threats from third countries, or intelligence-like knowledge by authorities about travel or location. None of these elements alone proves the existence of a diffusion or Blue Notice, but collectively they may justify an urgent access or deletion strategy before the CCF. (interpol.int)

The third step is a layered filing strategy. Requests to the CCF should be framed broadly enough to capture notices, diffusions and other personal data processed in INTERPOL systems, rather than focusing narrowly on public Red Notices. At the same time, accompanying national and international protection measures should be activated: extradition defense, asylum track, non-refoulement notifications, travel-risk management and compliance communications where necessary. (interpol.int)

The fourth step is evidentiary discipline. Hidden-tool cases especially require chronology, documentary precision and forum translation. Each factual sign must be connected not merely to a narrative of suspicion, but to a specific legal concern: improper purpose, lack of international police interest, Article 3 context, due-process deficits, refugee implications or disproportionality. Without that discipline, hidden-risk files easily degrade into conjecture. (interpol.int)

9. Policy Recommendations / Recommendations on Legal and Institutional Approach

First, INTERPOL should continue increasing transparency concerning the categories and effects of notices and diffusions, including clearer public explanation that the absence of a website extract does not exhaust the existence of INTERPOL-related data. This is not merely a matter of informational hygiene; it directly affects access to remedy and legal certainty. (interpol.int)

Second, the CCF and related explanatory materials would benefit from more explicit guidance on hidden-risk scenarios, especially diffusions, non-public notices and Blue-Notice-linked concerns. If the system acknowledges that such tools carry meaningful operational consequences, applicants should be better equipped to identify and formulate relevant requests. (interpol.int)

Third, legal practice should adopt a doctrine of hidden circulation. Such a doctrine should proceed on the basis that transnational exposure may exist without public-facing notice visibility, and that defense must therefore be structured around categories of circulation, not around public symbolism. For ARGA, this is particularly important as part of an overall model of early detection of international pressure. (interpol.int)

10. Conclusion

Hidden INTERPOL tools are not secondary technical details. They are central instruments in the real architecture of contemporary transnational risk. Diffusions, Blue Notices, non-public notices and message-based circulation can generate substantial operational consequences while remaining far less visible than the public image of a Red Notice suggests. The legal and defensive problem is therefore not only misuse of INTERPOL channels, but delayed recognition of that misuse. (interpol.int)

For ARGA, the central conclusion is that effective defense must begin where visibility ends. The absence of a public notice is not proof of the absence of international risk. In current conditions, competent defense requires not only challenge capacity, but detection capacity: the ability to suspect, map and legally articulate hidden data circulation before it turns into an arrest event, an extradition crisis or irreversible mobility damage. Everything else too often amounts to defense after the system has already done its work. (interpol.int)

11. Appendix A. Terminology

Red Notice. A notice seeking the location of a wanted person and their provisional arrest pending extradition, surrender or similar legal action. Not all Red Notices are public. (interpol.int)

Diffusion. A message circulated directly by an NCB or international entity to one or more countries through the INTERPOL I-24/7 network, requesting arrest, location, additional information or other police cooperation. A less public, but highly significant instrument. (interpol.int)

Blue Notice. A notice requesting collection of additional information about a person's identity, location or activities in relation to a criminal investigation. It may play a preparatory and tracing role. (interpol.int)

Non-public notice. A notice existing within INTERPOL systems but not published as a public extract on the INTERPOL website. (interpol.int)

Hidden circulation. A working term for situations in which personal data relevant to police cooperation circulate through INTERPOL systems or related NCB channels without obvious public visibility to the person concerned. (interpol.int)

12. Appendix B. Risk / Powers / Legal Consequences Matrix

Task	**Legal risk**	**Legal limit**	**Possible consequence**	**Practical comment**
Check only the Red Notices website	False absence of risk	Not all red notices are public	Missed international circulation	A website check is never sufficient
Ignore diffusions	Incomplete picture of data processing	Diffusions are covered by INTERPOL rules and can trigger real consequences	Unexpected border, arrest or intelligence effects	Always assess the possibility of a diffusion
Underestimate the Blue Notice	Treat it as "harmless"	Information-gathering tools can support later coercive action	Escalation after a quiet tracing phase	Blue Notices matter strategically
File a narrow request only about a public notice	Fail to capture other data categories	The CCF can examine broader personal data in INTERPOL systems	Partial or ineffective result	Frame requests broadly
Fail to record indirect symptoms	Loss of early-warning evidence	Hidden tools are often inferred from effects	Late reaction and unprepared crossings	Build a symptom chronology early
Fail to combine CCF action with extradition/asylum strategy	Fragmented protection	INTERPOL review is not self-sufficient	Real harm before review outcome	Multilevel defense is essential
Treat hidden tools as exceptional	Underestimate systemic practice	2024 statistics show substantial diffusion-related caseload	Strategic blind spot	Treat hidden circulation as a mainstream risk

(interpol.int)

13. Official Sources

- INTERPOL, Rules on the Processing of Data. The main legal source governing the processing of notices, diffusions, messages and other data in INTERPOL systems. (interpol.int)

- INTERPOL, About Notices. Official explanation of the distinction between notices and diffusions and their operational role in international police cooperation. (interpol.int)

- INTERPOL, View Red Notices. Important source confirming that not all Red Notices are public and that website publication is only partial. (interpol.int)

- INTERPOL, What is a Blue Notice. Official description of the Blue Notice and its purpose in locating or gathering information about a person. (interpol.int)

- INTERPOL, 2024 Annual Activity Report of the CCF. A statistically significant source showing the share of diffusion-related admissible requests and the practical importance of non-public data categories. (interpol.int)