

Reframing European Common Operational Partnerships against THB and Migrant Smuggling

A public-private pre-investigative model inspired by FIU/AML cooperation, accountable OSINT and THB risk indicators

Sergio Bianchi, *Director of Agenfor International Foundation*

Natalina Cea, *Deputy Director of TJPS Institute-UPEACE, Senior strategic advisor on security, border and migration*

ABSTRACT

European Common Operational Partnerships (COPs) are collaborative law enforcement initiatives designed to disrupt transnational organized crime, particularly migrant smuggling and human trafficking. While these partnerships are centred on cooperation among public authorities, the European Union has, in some cases, acknowledged the importance of involving private-sector actors in related initiatives. In particular, the participation of non-governmental organizations, international organizations, and other non-profit entities has been recognized as adding significant operational value. This article argues that the current predominant model of COPs, which remains largely focused on public institutional participation, should be reconsidered and reshaped to become more inclusive to address the evolving operational realities of contemporary criminal organizations, whose activities often transcend the capacities and competences of state actors alone.

COPs against migrant smuggling and trafficking in human beings (THB) have generated significant value in terms of liaison, capacity building, training, and, where possible, cross-border information exchange. Nevertheless, the current model remains structurally incomplete insofar as it continues to reproduce a predominantly police-to-police information-sharing architecture. In the field of THB, the earliest indicators of exploitation are often identified not by national criminal police forces, but by a broader range of actors, including victim-support organisations, shelters, labour-rights services, trade unions, local authorities, municipal police bodies, ports and reception services, rescue operators, legal-aid providers, cultural mediators, internet service providers, platform operators, financial institutions, forensic experts, AI and OSINT specialists, and investigative civil society organisations with a special focus on local communities in border areas.

The new proposed model should include a formally governed public-private pre-investigative layer. The model is inspired by Financial Intelligence Unit and anti-money laundering (FIU/AML) cooperation but translated into a victim-centred THB context. Private and civil-society actors should not be deputised as police and should not conduct covert criminal investigations. They can, however, lawfully generate structured risk indicators, red-flag reports, typologies, OSINT preservation packages, victim-sensitive documentation and referral inputs before the opening of a criminal file. Public authorities retain exclusive responsibility for validation, prioritisation, criminal investigation, coercive measures, evidence and prosecution. The missing bridge is a disciplined system of THB indicators: a common language for translating weak signals into reviewable, minimised and auditable pre-investigative inputs.

1. Why the European COP model requires revision

The starting point is practical. THB and migrant smuggling are no longer organised only through territorial brokers, physical routes and face-to-face recruitment. They are increasingly supported by online advertising, encrypted communications, platform-based recruitment, mapping applications, informal transfer systems, cryptocurrencies, fake-document channels, remote guidance and digital logistics. This does not mean that the whole criminal process takes place online. Rather, the digital environment has added a new operational layer to traditional exploitation, recruitment, transport and control.

The current COP model has three strengths. First, it offers a flexible framework through which EU Member States and third countries can cooperate around a route, a criminal market or an operational gap. Secondly, it gives value to liaison officers, national interagency teams, capacity building, mentoring and secure information exchange. Thirdly, it can connect national investigations with Europol, Eurojust, Frontex, EMPACT and other EU or international instruments.

The weakness is that the model often remains too narrow. In practice, COP planning has tended to harden around inter-police and judiciary-police cooperation. This is understandable because arrests, searches, seizures, interceptions, evidence handling and prosecution must remain under public authority. But the same institutional caution becomes problematic when it prevents structured cooperation with the actors who observe the earliest signs of exploitation. THB investigations rarely begin with perfect evidence. They begin from fragments: a victim disclosure in a shelter, an employment dispute in agriculture or tourism, a suspicious advertisement, a repeated transport pattern, a false job offer, a platform profile, a phone number used in multiple contexts, a money transfer, a cultural-mediator interview, a forged document, a local-police inspection, a labour-union complaint, or a medical or social-service encounter.

This creates a design problem. If the only recognised COP information channel is police-to-police exchange, the system waits until law enforcement already has an investigative basis. But THB is often hidden precisely because that basis is missing. Victims may not self-identify. Exploiters may operate behind legitimate businesses. Migrants may fear expulsion, retaliation, stigma or loss of income. Digital traces may disappear before a formal request is made. Private platforms and service providers may hold data that are legally inaccessible without procedure, but they may also observe patterns that can be reported as risk indicators. NGOs and labour actors may have trust-based access to vulnerable people that police do not have. Local administrative bodies may detect anomalies before national units do. A COP therefore needs a pre-investigative layer: not a parallel police system, but a structured channel through which non-police actors can produce lawful, limited, documented and reviewable inputs. Finally, the current model risks undermining the emerging approach to analysis, which is shifting from explaining events after they occur (through storytelling, reporting, or post-event analysis) toward anticipation — namely, the identification of weak signals, the detection of emerging trends, and the prediction of future events. As a result, the existing framework may hinder the ability to capture and interpret weak signals in advance of an event, thereby limiting the capacity to plan and act proactively before the event occurs.

2. The FIU/AML analogy: a model for pre-investigative cooperation

The most useful analogy is the financial-intelligence model. In anti-money laundering and counter-terrorist financing systems, private obliged entities are not police forces. Banks, payment institutions, professional service providers and other obliged entities identify suspicious activity through customer due diligence, risk monitoring and internal controls. They report suspicions to Financial Intelligence Units. FIUs receive, analyse and disseminate financial intelligence to competent authorities when thresholds are met. The broader system distinguishes preventive private-sector obligations from public investigation and prosecution.

This model is relevant for COPs because it solves a structural dilemma: the state needs information before it can investigate, but not all information can or should be collected directly by police. AML law does not delegate coercive powers to banks. It creates a regulated pre-investigative environment where private actors observe, structure and transmit suspicious indicators under legal duties, supervisory standards, confidentiality rules, retention limits and accountability. The FIU then acts as an analytical buffer. It does not automatically convert every suspicious transaction report into a criminal investigation. It filters, enriches, grades and disseminates when appropriate. THB requires an analogous but more victim-sensitive model. A sheltering organisation is not a bank. A cultural mediator is not a compliance officer. A labour-rights association does not operate under the same reporting logic as a financial institution. A journalist and a victim-support NGO have different missions from law enforcement. The AML analogy should therefore not be copied; it should be translated. The translation is this: private and civil-society actors may generate pre-investigative leads, THB indicators, typologies, red-flag reports and preserved OSINT material; a public COP coordination unit or national competent authority assesses and validates those inputs; coercive investigation begins only when national procedural thresholds are met; and the entire process remains documented, minimised, auditable and rights-compliant.

The value of this model is especially clear in THB. Victim-support organisations may identify repeated profiles of control, debt bondage, document retention, threats, sexual exploitation or forced labour. Legal-aid providers may see recurring patterns in asylum, residence, labour or protection interviews. Cultural mediators may detect scripted narratives, identical recruitment stories or indicators of coercion. Trade unions and labour services may identify clusters of unpaid wages, abusive housing, illegal deductions or transport dependency. Reception and disembarkation services may see recurring routes, phone numbers, guides and facilitators. Internet providers and platforms may detect fraudulent advertisements, recruitment pages, repeated account behaviour or online payment funnels. Banks and payment services may identify suspicious transfers connected with recruitment fees, informal value transfer or coercive debt. OSINT analysts may map public indicators across languages, platforms and routes before police have an open case.

3. THB indicators as the missing pre-investigative grammar

The introduction of THB indicators is not a cosmetic addition to a COP methodology; it is the operational grammar of the pre-investigative layer. Indicators make weak signals comparable. They help non-police actors describe what they have observed without prematurely labelling a person as a suspect or a victim. They help public authorities triage information without absorbing every fragment into an uncontrolled intelligence reservoir. Properly designed, indicators are neither evidence nor accusation. They are structured risk signals that require validation, enrichment and, where appropriate, protective or investigative action.

This distinction is crucial. A fraudulent job advertisement, a repeated telephone number, a suspicious transport pattern, a shared online account, a coerced housing arrangement or a payment trail may be relevant, but none of these elements proves trafficking on its own. The same is true for digital indicators. Traffickers may use ordinary websites, social media, job portals, classified-ad platforms, dating applications, online messaging systems, mapping tools, ticketing platforms and payment applications. The fact that these tools are used does not automatically indicate a crime. The indicator-based model avoids both under-reaction and over-reaction: it allows early warning while preserving the presumption of innocence, data minimisation and victim protection.

A COP should therefore adopt a common THB indicator taxonomy. At minimum, it should cover five domains: recruitment, transport, exploitation, control and profit. Each domain should include both offline and digital signs. Recruitment indicators may include misleading job advertisements, fake agency websites, vague or unrealistic work conditions, inconsistent contact data, grooming through social media or dating platforms, and recruitment through emotional dependency or sextortion. Transport indicators may include repeated routes, recurring drivers, coordinated accommodation, forged documents, remote guidance, ticket purchases by third parties, and mapping or geolocation instructions. Exploitation indicators may include online advertisements of sexual services, repeated phone numbers across different profiles, shared management of accounts, frequent movement between cities, dependency on a third party for appointments, labour exploitation, unpaid wages, abusive deductions and overcrowded accommodation. Control indicators may include document retention, debt bondage, threats, blackmail, isolation, monitoring of communications, scripted narratives, restriction of movement and dependency on interpreters or intermediaries. Profit indicators may include recruitment fees, informal value-transfer codes, cryptocurrency addresses, repeated small transfers, cash collection points, prepaid cards, and links between apparently legitimate businesses and exploitative premises.

The value of indicators is greatest before a formal investigation exists. At that stage, the question is not “has the crime been proved?” but “is there a legally relevant risk signal that should be protected, verified, referred or escalated?” A shelter may identify a risk to a person. A labour inspector may identify a workplace pattern. A local police unit may identify an administrative anomaly. A platform may identify repeated fraudulent recruitment behaviour. A bank may identify payment patterns. An OSINT analyst may preserve public posts and account relationships. A COP indicator template gives all of these actors a common reporting language without requiring them to perform police functions.

3.1. Digital recruitment indicators

Digital recruitment deserves specific attention because it is often the earliest visible stage. Misleading job advertisements can appear on trusted job portals, web forums, social media and other virtual platforms. Some traffickers create fake agency websites and promote them online. Typical sectors include domestic work, childcare, hospitality, tourism, modelling, agriculture, construction, entertainment and, in some cases, advertised educational opportunities abroad. Red flags include absence of an identifiable employer, grammatical or language anomalies, vague job requirements, unrealistic conditions, no exact salary information, and contact details that appear in unrelated or adult-service contexts.

Other recruitment methods are less visible. The so-called lover-boy method and related grooming techniques may use social media, dating services, forums, chat rooms and encrypted messaging to create emotional dependency. Sextortion may be used to force a victim to move, comply or remain in exploitation through threats to publish intimate material. In these cases the indicator may not be a public post, but a pattern disclosed by a victim, a mediator, a counsellor or a digital forensic examination conducted by competent authorities. COP methodology should therefore distinguish open-source indicators from confidential victim-related indicators and ensure that the latter trigger protection and referral before any investigative exploitation of the information.

3.2. Indicators as triage, not proof

The practical rule should be simple: indicators trigger triage, not guilt. A pre-investigative report should classify each indicator according to source, confidence, urgency, victim risk, data category and suggested action. Some inputs will require immediate victim-protection referral. Some will require preservation before online content disappears. Some will be suitable for strategic analysis only. Some will require a labour or administrative response. Some will justify transmission to a prosecutor, criminal police unit, FIU, Europol or Eurojust. Some will be discarded. This triage logic prevents indicators from becoming a shortcut around criminal procedure.

This also protects private and civil-society actors. They do not need to determine whether a criminal offence has been committed. They need to record what they saw, how they saw it, when they saw it, why they believe it may be relevant, what risks exist for victims or non-suspected persons, and what material has been preserved. The competent public authority then validates, enriches, rejects or escalates the input. In this sense, THB indicators function as the THB equivalent of suspicious activity reporting: they are a disciplined pre-investigative trigger, not delegated policing.

3.3. Provenance and validation of the indicator model: UNCHAINED and INTERCEPTED

For this reason the indicator component should not be presented as an abstract taxonomy only. It is part of a tested operational lineage. Agenfor International contributed as developer of the THB indicator methodology within the EU-funded UNCHAINED project, where the indicators were

designed to translate victimisation patterns, digital recruitment signals, exploitation contexts and investigative red flags into a common operational language for practitioners. This development role is relevant because it links the indicator taxonomy to applied training, OSINT practice, forensic awareness and the needs of prosecutors, law-enforcement authorities and victim-facing actors.

The same indicators have also been used successfully in the INTERCEPTED project. That practical use confirms their value as a pre-investigative grammar: they help multidisciplinary actors recognise early risk signals, organise observations without premature criminal labelling, support victim-sensitive referral and provide public authorities with structured inputs that can be validated, rejected or escalated under the applicable legal thresholds. A revised COP should therefore treat THB indicators as a reusable and tested methodology, not merely as a descriptive checklist.

4. Why private actors are essential in THB and smuggling pre-investigation

The argument for private participation is not ideological; it is operational. THB is a crime of control, dependence and concealment. Criminal groups use legal markets, vulnerable labour sectors, mobility, online visibility and social invisibility at the same time. In many cases the victim is the only person who can explain the coercive relationship, but the victim may not approach police. Instead, victims may first interact with a shelter, a health service, a lawyer, a mediator, a religious organisation, a local NGO, a rescue operator, a labour union or a municipal office. Any COP model that ignores these actors loses the earliest and most reliable point of access to victimisation patterns.

The same applies to labour exploitation. Agricultural workers, domestic workers, logistics workers, tourism workers, construction workers and workers in hidden workshops may be exploited by criminal networks serving legitimate businesses. The investigative lead may not arise from a criminal complaint. It may arise from unpaid wages, housing overcrowding, unsafe transport, repeated administrative irregularities, medical complaints, labour-inspection findings, union claims or local-police controls. In this environment, local police bodies and municipal enforcement units matter. They may not always be recognised as full police forces in national or European cooperation architectures, but they exercise territorial control through street checks, administrative inspections, health and safety controls, licensing checks, traffic enforcement, market controls and proximity policing. They see weak signals that national criminal units may not see.

Technology deepens the need for private participation. Digital evidence, OSINT, AI-assisted analysis, platform data, hosting information, domain registration, payment data, device forensics and multilingual analysis are often held or operated by private entities. Some technologies used for forensic extraction, AI correlation, large-language-model analysis, RAG architectures, document

authentication and OSINT monitoring are more advanced in the private market than within police forces. A COP should use this capacity lawfully, by defining roles, lawful sources, prohibited conduct, reporting channels, data-protection duties and escalation thresholds.

There is also a jurisdictional dimension. Police are territorially and procedurally bounded. Private platforms, ISPs, financial intermediaries, NGOs and international organisations often operate across borders or maintain networks that do not stop at national frontiers. This does not mean that private actors have stronger legal powers; they do not. But they can observe cross-border patterns without being limited by the same organisational geography as police units. A COP should use this advantage by creating structured channels for pre-investigative alerts, not by informally asking private actors to conduct surveillance on behalf of the state.

Finally, since trafficking in human beings (THB) and migrant smuggling are inherently cross-border crimes that affect multiple territories and countries before reaching their final stage, the role of border communities is crucial in supporting border and law enforcement authorities. The involvement of these communities, together with the organisations operating on the ground, the ethnic and tribal ties that extend across borders, and the information and data they possess, have been identified as critical elements in combating cross-border trafficking through a regional approach.

In this context, the One Desert Initiative (ODI)^[1], launched by EUBAM Libya and supported by other CSDP missions in the Sahel, dedicated a specific action to the development of networks and communication channels between local cross-border communities and local security authorities.

5. The current risk: intelligence-led policing as a substitute for missing pre-investigative channels

Because investigations need pre-investigative information to start, the absence of a public-private pre-investigative layer has pushed many systems towards intelligence-led policing. This model can be effective when it is lawful, targeted, auditable and proportionate. The problem arises when intelligence becomes a substitute for criminal procedure, or when the boundaries between intelligence, police investigation and evidence are blurred.

The legal distinction matters. Intelligence is often preventive, strategic and risk-oriented. It deals with weak signals, networks, vulnerabilities, future threats and contextual assessment. Criminal investigation is case-oriented and legally constrained by procedural thresholds, judicial authorisation, defence rights, evidentiary rules, disclosure obligations and remedies. Criminal intelligence sits between these two worlds, but it cannot abolish the safeguards of either. When COPs are designed only as police-to-police information channels, they risk absorbing pre-investigative uncertainty into police intelligence systems without a clear governance model for

[1] One Desert Initiative Joint Declaration 22-23 October 2022.

source quality, data categories, non-suspected persons, victims, retention, deletion, audit logs and later evidentiary use.

The public debate around large-scale police data analytics in Europe illustrates the systemic danger: large analytical capacity without clear categorisation, access control, logging, deletion rules and oversight can undermine fundamental rights, fair-trial rights and trust in European cooperation. This is not an argument against Europol, OSINT or analytical technology. It is an argument for accountable architecture. If COPs expand digital monitoring, AI, OSINT, forensic capacity and cross-border information exchange, they must not reproduce informal intelligence reservoirs. They need a lawful route for pre-investigative information that does not pretend that every weak signal is evidence, and does not allow public or private actors to create bulk datasets without necessity, purpose limitation and review.

6. EMPACT, COPs and EU Police Networks: Multifaceted models and formulas

The distinction between EMPACT and COPs remains essential. EMPACT is the EU's permanent policy-cycle instrument for serious and organised international crime. It is Member State-driven and implemented through priorities, Operational Action Plans and Operational Actions. It may generate operational outcomes, including Joint Action Days and coordinated measures across jurisdictions, but the coercive dimension of those actions remains entirely national: arrests, searches, seizures, interviews, freezing measures and prosecutorial decisions are carried out by competent national authorities under national law. COPs, by contrast, are more concrete and project-based cooperation architectures. In the DG HOME/ISF context, they support structured operational cooperation between law-enforcement authorities, judicial authorities and other relevant services of participating Member States and third countries. They may include liaison officers, interagency teams, OSINT centres, training, mentoring, secure information exchange, operational support and pre-investigative coordination. They are therefore not a supranational investigative body and do not create new coercive powers.

This distinction should not be used to exclude private or non-public actors from COP-related methodologies. On the contrary, the broader landscape of European police cooperation shows that several EU-supported networks already contemplate, or functionally require, structured interaction with private actors. ENLETS is the clearest example, because its technology-oriented law-enforcement model is based on the connection between operational needs, industry, technological providers and research. EUCPN also provides a relevant precedent, since crime prevention structurally depends on public-private partnerships, civil society, researchers, local actors, media and other prevention stakeholders. EMPACT itself is multidisciplinary and may involve the private sector where relevant to the operational action. BRONETT, by focusing on critical broadband and public-safety communications, necessarily requires interaction with telecom operators, technology

providers and standardisation actors. AIRPOL, RAILPOL and AQUAPOL, while formally centred on law-enforcement cooperation, operate in environments — aviation, railways, ports and waterways — where transport operators, infrastructure managers, private security, logistics actors and other sectoral stakeholders are operationally relevant. TRACE / Conflict Armament Research is also significant because it illustrates the contribution of specialised non-governmental analytical capacity to operational knowledge.

These models should be distinguished from networks whose structure remains predominantly institutional or law-enforcement based, such as ENFSI, EPRIS, ENFAST, EODN, CARIN, AMON, MAOC-N, ATLAS, EU-HRSN and EIFS. In those networks, private-sector involvement is normally not part of the core governance or operational model, except through procurement, external expertise, training, technical support or ad hoc consultation. They are therefore less suitable as methodological references for THB-related COPs where early detection often depends on information held outside traditional law-enforcement channels.

The relevance of this distinction is particularly clear in trafficking in human beings. THB investigations often begin before there is a formal criminal case, and the earliest signals may be observed by victim-support organisations, shelters, labour inspectors, local authorities, transport operators, online platforms, banks, payment providers, OSINT analysts, journalists, cultural mediators and technology providers. These actors may detect misleading job advertisements, platform-based recruitment, online sexual exploitation indicators, repeated phone numbers or accounts, suspicious payment patterns, transport routes, forged-document channels, labour exploitation patterns or victim-protection risks. A COP that is limited to police-to-police exchange may therefore receive information too late, while an uncontrolled intelligence model would create risks for data protection, fair trial, victim protection and accountability.

The correct solution is not to transform private actors into delegated police. Their role should remain pre-investigative, technical, analytical or victim-support oriented. They may produce lawful OSINT material, typology mapping, THB-indicator reports, red-flag alerts, victim-sensitive documentation, technical expertise or referral information. Competent public authorities must then assess, validate, enrich, discard or escalate those inputs under the applicable legal framework. In this model, EMPACT Operational Actions can benefit from COP-generated typologies and structured indicators without importing uncontrolled datasets, while COPs can align more closely with EMPACT's multidisciplinary logic without becoming informal surveillance systems. Public authorities retain responsibility for validation, prioritisation, investigation, coercive measures, evidence and prosecution; private and civil-society actors contribute what they are best placed to observe, but within a governed, auditable and rights-compliant chain of responsibility.

This approach also corresponds to the operational evolution already visible in projects like OSINT RADAR. The project is built around liaison officers, national interagency teams, OSINT centres, digital-smuggling analysis, AI and forensic tools, training, live prototyping and sensitive or classified reporting. Its next methodological step should be to make the public-private pre-investigative layer explicit: eligible actors, lawful sources, prohibited conduct, reporting formats, source grading, data minimisation, secure handover, retention rules, triage procedures and feedback mechanisms should be defined in advance. In this way, COPs would not be confused

with EMPACT, nor with purely institutional law-enforcement networks. They would instead become the structured environment in which public authority, private technical capacity, civil-society knowledge and THB indicators are connected before the formal investigative threshold is reached, while EMPACT remains the wider EU policy-cycle and operational-priority framework.

7. A proposed public-private pre-investigative layer for COPs

The revised COP model should be built around a layered information cycle. The first layer is private and civil-society observation. Actors in this layer include shelters, victim-protection organisations, women's protection services, legal-aid providers, cultural mediators, reception services, rescue organisations, labour unions, labour inspectors, local police bodies, municipal authorities, health and safety inspectors, platform operators, ISPs, payment providers, banks, forensic providers, OSINT analysts, AI experts and investigative journalists. Their contribution is not to investigate suspects, but to identify and preserve indicators.

The second layer is structured pre-investigative reporting. Reports should not be informal emails or uncontrolled data dumps. They should follow standard templates: source identity or protected source code; legal basis or mission basis for collection; purpose of collection; category of person concerned; THB-indicator category; vulnerability indicators; type of information; date and method of collection; reliability assessment; confidence level; urgency; risk to victims; recommended protective action; and attached material with provenance, timestamps, URLs, screenshots, hashes or chain-of-custody notes where appropriate. In victim-related cases, informed consent, do-no-harm and referral principles should guide documentation.

The third layer is COP triage by a competent public unit. This unit should include law enforcement, prosecutors or judicial authorities where appropriate, data-protection expertise, victim-protection expertise and technical analysts. It should decide whether the input is irrelevant, useful for strategic analysis, useful for victim protection, suitable for administrative action, suitable for financial intelligence referral, suitable for Europol/Eurojust exchange, or sufficient to support an investigative step under national law. This triage function is the THB equivalent of the FIU analytical buffer.

The fourth layer is controlled escalation. When a pre-investigative input points to a concrete suspect, organisation, online account, payment channel, document-fraud provider, recruitment network or exploitation site, the competent authority should validate the information and apply the relevant national threshold. Only then should coercive measures be considered. The source file should remain separated from the evidence file unless procedural law allows its use and disclosure rules are respected. This protects both the investigation and the private or humanitarian actor.

The fifth layer is feedback and learning. One weakness of public-private cooperation is that private actors often report and then receive no feedback. A COP should provide lawful feedback without compromising investigations: typology updates, anonymised outcomes, quality guidance, training,

red-flag refinement, and lessons learned. This is essential to keep shelters, unions, platforms, financial institutions and local bodies engaged and accurate.

8. Eurojust-ICC procedures for public-private cooperation

The Eurojust-ICC Guidelines for Civil Society Organisations provide the most practical procedural benchmark for a public-private COP layer. They were developed by Eurojust, the Genocide Network and the Office of the Prosecutor of the International Criminal Court for civil-society organisations that collect and preserve information on international crimes and human-rights violations for accountability purposes. Their relevance to THB does not depend on transforming civil-society organisations into investigators. On the contrary, the guidelines expressly preserve the distinction between independent documentation work and the legal mandate of competent investigative and prosecutorial authorities.

For COP purposes, the guidelines can be translated into a standard operating procedure for pre-investigative cooperation. First, any actor collecting information should define its mandate, purpose and legal basis before collection. Secondly, the actor should apply a do-no-harm approach, especially where victims, children, migrants in irregular situations, persons in dependency relationships or traumatised persons are involved. Thirdly, informed consent should be obtained and recorded whenever the collection or transfer of information requires or appropriately relies on consent. Fourthly, documentation should remain objective, impartial and source-based: facts, inferences, uncertainty and analytical assumptions must be separated. Fifthly, provenance should be preserved through dates, methods of collection, source category, URLs, screenshots, hashes, chain-of-custody notes and secure storage where appropriate. Sixthly, repeated detailed interviews, over-documentation and any conduct capable of re-traumatising victims or contaminating later evidence should be avoided. Seventhly, information should be transmitted promptly and securely to the competent authority when it may be relevant to protection, prevention, investigation or prosecution.

This procedure is especially important for online investigations. Public posts, advertisements, profiles, routes, payment clues and recruitment narratives may disappear quickly. A private or civil-society actor may preserve a public trace for accountability or protection purposes, but it should record the collection method, avoid unlawful access, avoid covert coercion or impersonation, minimise third-party data, and indicate whether the material is public, voluntarily provided, platform-provided or requires legal request by an authority. Once transferred, the competent public authority must decide whether the material remains a pre-investigative lead, becomes criminal intelligence, supports victim protection, is referred to Eurojust or Europol, or is rejected.

The new role of the ICC strengthens the reason for using these procedures. The ICC has not acquired general jurisdiction over ordinary THB cases. However, the ICC Office of the Prosecutor's Policy on Slavery Crimes gives renewed prosecutorial and interpretative priority to

slavery-related conduct under the Rome Statute, including enslavement, sexual slavery and slave-trade patterns where the Court's contextual jurisdictional requirements are met. This is not a transfer of THB enforcement from national authorities to the ICC. It is a clarification that trafficking-related conduct may become relevant to international criminal accountability when it forms part of enslavement, sexual slavery, forced labour, detention, debt bondage, child exploitation or other slavery crimes committed in the context of Rome Statute crimes.

That ICC development justifies the use of Eurojust-ICC procedures in COPs even when most cases will remain national cases. COPs with third-country partners often operate in environments where exploitation, displacement, conflict dynamics, organised crime, corruption, document fraud, sexual exploitation, forced labour and migrant smuggling overlap. Using Eurojust-ICC documentation standards as a procedural benchmark increases the chance that information collected by private actors, NGOs or OSINT analysts can later support national proceedings, Eurojust coordination, mutual legal assistance, joint investigation teams or, in exceptional cases, international accountability. The practical value is therefore not jurisdictional expansion, but methodological discipline: victim-sensitive collection, reliable provenance, secure handover, chain of custody and respect for the limits of civil-society documentation.

9. Safeguards: from private OSINT to accountable OSINT

A public-private COP model is only defensible if it is safer than the informal alternatives. The first safeguard is legality of collection. Private OSINT analysts and civil-society actors should use lawful sources only. They should avoid hacking, unlawful access, unlawful impersonation, malware, covert coercion, intrusive surveillance, scraping that violates applicable law, restricted law-enforcement databases, and bulk processing of sensitive data without a lawful basis. They should distinguish between public information, voluntarily provided information, platform-provided information and information requiring a legal request.

The second safeguard is purpose limitation. A shelter collects information to protect victims, not to build a police dossier. A labour union collects information to defend workers, not to conduct undercover criminal investigations. A journalist collects information for public-interest reporting. A platform processes data under its terms, legal duties and regulatory obligations. A COP handover must respect these original purposes and document why transfer is lawful, necessary and proportionate. Where consent is required or appropriate, it must be informed and recorded. Where consent is not the legal basis, the actual legal basis must be identified.

The third safeguard is victim protection. Documentation standards developed for accountability work provide a useful benchmark: do no harm, informed consent, objectivity, confidentiality, risk assessment, protection of vulnerable persons, secure storage and careful analysis. These principles are directly relevant to THB, where victims may be traumatised, dependent on exploiters, undocumented, fearful of authorities or exposed to retaliation. THB indicators should never be collected in a way that re-traumatises victims, exposes them to retaliatory risks or contaminates later evidence.

The fourth safeguard is data categorisation. COP systems should distinguish suspected persons, convicted persons, victims, possible victims, witnesses, reporting persons, bystanders, relatives, service providers, legal entities and purely contextual entities. Data about non-suspected persons should remain contextual, provisional and minimised unless a competent authority lawfully determines that it is necessary and proportionate for a defined law-enforcement purpose.

The fifth safeguard is auditability. Every pre-investigative input should have provenance, date, source category, access restrictions, retention rule, deletion trigger, review date and responsible authority. AI-assisted analysis should be explainable enough for human review. Outputs should distinguish fact, inference, confidence and uncertainty. If an input is later used in criminal proceedings, the origin and chain of handling should be reconstructable, subject to the applicable rules on confidentiality, source protection and defence rights.

10. The local-police and administrative-control dimension

One of the most underdeveloped aspects of COP planning is the role of local police and administrative authorities. European cooperation frameworks often assume that “police” means national criminal police, border police, specialised organised-crime units or judicial police. Yet local police may control the territory more continuously. They observe street prostitution, massage centres, short-term rentals, informal dormitories, irregular transport, counterfeit goods, unlicensed businesses, illegal workshops, nightlife venues, markets, traffic routes, labour housing and neighbourhood dynamics. Health inspectors and administrative inspectors may enter premises and detect exploitation indicators that criminal police would not see until much later.

This does not mean that administrative powers should be used to bypass criminal-procedure safeguards. On the contrary, the revised COP model should prevent that risk by clarifying when an administrative observation remains administrative, when it becomes a pre-investigative risk indicator, and when it must be transferred to a prosecutor or criminal police unit. The same logic applies to labour inspections. A wage claim or workplace inspection may reveal forced labour indicators, debt bondage, document retention, coercive housing or threats. If these indicators are not channelled into a COP-compatible format, they remain isolated administrative facts. If they are channelled without safeguards, they risk becoming informal surveillance. The solution is a governed handover protocol.

A practical COP template should therefore include local-police and administrative authorities as territorial sentinels. Their role should be to collect legally obtained observations, identify THB indicators, protect victims, refer urgent risks and transmit structured reports. They should not be asked to conduct covert criminal investigations without the required legal basis. Training should cover THB indicators, victim identification, digital evidence preservation, labour exploitation, cultural mediation, non-discrimination, data protection and escalation thresholds.

11. A workable governance model

A revised COP should adopt seven governance instruments. First, a public-private participation protocol should define eligible actors, roles, lawful sources, prohibited conduct, reporting formats, secure channels, data categories, urgency procedures and feedback. Secondly, a THB-indicator and pre-investigative reporting template should translate weak signals into structured and comparable inputs without over-collecting personal data. Thirdly, a victim-sensitive documentation standard should incorporate do-no-harm, informed consent, vulnerability assessment, referral pathways, and rules against repeated unnecessary interviews. Fourthly, a source and reliability grading system should distinguish direct observation, victim statement, third-party report, public OSINT, platform data, financial indicator, administrative record and analytical inference.

Fifthly, a data-protection and retention schedule should define what may be kept, by whom, for how long, under which category and with which deletion rule. Sixthly, an escalation board or triage unit should decide whether inputs become strategic analysis, prevention, victim protection, administrative action, FIU referral, Europol/Eurojust exchange or criminal investigation. Seventhly, an accountability package should include audit logs, periodic review, independent data-protection checks, prosecutor oversight where appropriate, and an annual lessons-learned report.

This model would also support interoperability with Europol, Eurojust and EMPACT. Europol would receive better-structured inputs with source provenance and data categories. Eurojust would be better placed to coordinate when information becomes prosecutorially relevant. EMPACT Operational Actions could draw on COP pre-investigative typologies without importing uncontrolled datasets. National authorities would retain responsibility for coercive acts. Private actors would know what they can and cannot do. Victims would be better protected. Defence rights would be less likely to be undermined by opaque intelligence origins.

Conclusion: from closed COPs to accountable public-private COPs

The COP model should be revised because the operational environment has changed. THB and migrant smuggling are now digital, financial, transnational, labour-market based and victim-access dependent. A closed police-to-police COP cannot see enough, early enough to plan and act proactively before the event occurs. At the same time, an uncontrolled intelligence-led model would create serious risks for fundamental rights, data protection, fair trial, victim protection and democratic oversight. The answer is not to exclude private actors and not to deputise them as police. The answer is to create an accountable public-private pre-investigative layer.

The FIU/AML analogy shows that private-sector information can be made useful before criminal investigation without transferring coercive powers to private actors. In THB, the equivalent should be a system of structured alerts, victim-sensitive documentation, lawful OSINT, border local communities, labor and local-police indicators, platform and ISP cooperation, financial red flags, technical expertise and secure handover to competent authorities. THB indicators are the common

grammar of that system. They allow early recognition without premature criminal labelling; they support triage without replacing evidentiary thresholds; and they connect victim protection, administrative knowledge, private expertise and public authority within a lawful chain of responsibility.

Public authorities must remain responsible for validation, prioritisation, investigation, coercive measures, evidence and prosecution. Private actors should remain within their mission, but their knowledge should no longer be peripheral. A rights-compliant COP should place victims, local knowledge, lawful OSINT, private technical capacity and THB indicators at the beginning of the investigative chain, where they are most needed.

Selected references

- Council of the European Union, EMPACT Terms of Reference, ST 8975/23, 17 May 2023.
- Council of the European Union, Council conclusions on the enhancement of EMPACT and on EU crime priorities for the next EMPACT cycle 2026-2029, 13 June 2025.
- DG HOME / Internal Security Fund, Common Operational Partnerships to prevent and fight against migrant smuggling with competent authorities of third countries, ISF-2024-TF2-AG-COP.
- European Parliament and Council, Regulation (EU) 2016/794 on Europol, as amended by Regulation (EU) 2022/991.
- European Data Protection Supervisor, Decision concerning Europol processing of large datasets, 3 January 2022.
- Eurojust, Genocide Network and ICC Office of the Prosecutor, Documenting International Crimes and Human Rights Violations for Criminal Accountability Purposes: Guidelines for Civil Society Organisations, 2022.
- European Union Internal Security Fund - Police, Risk Indicators for Trafficking in Human Beings, section on digital society, new technologies and human trafficking.
- European Parliament and Council, Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- European Parliament and Council, Directive (EU) 2024/1640 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- International Criminal Court, Rome Statute of the International Criminal Court, consolidated text, 2025.
- International Criminal Court, Office of the Prosecutor, Policy on Slavery Crimes, December 2024.
- International Criminal Court, Office of the Prosecutor, Questions and Answers on the Policy on Slavery Crimes.
- OSINT RADAR, Description of Action and Amendment AMD-101102419-3, project documentation, 2026.

- One Desert Initiative Joint Declaration and Technical Road Map.
- UNCHAINED project materials, THB indicator methodology developed with the contribution of Agenfor International.
- INTERCEPTED project materials, operational use of THB indicators.
- UNODC, Global Report on Trafficking in Persons and related operational materials on trafficking indicators and victim identification.