WHITE PAPER

Scaling Up the Fight Against Human Trafficking

A Civilisational Imperative

For the attention of Heads of State
and the CEOs of leading high-tech companies

"It is possible to free one million victims from modern slavery,
to save one million human lives per year, if we want to, today."

Synthesis prepared from the work of the Pontifical Academy of Social Sciences (2013–2021),
the Rome Conference Against Human Trafficking (December 2025)
and the White Paper "How to use better technology to fight human trafficking" (2026).

Jean-Sébastien Mallet
June 2026

Contents

1. Executive Summary

Twenty-five years after the adoption of the Palermo Protocol, the fight against human trafficking remains one of the great collective failures of international governance. **Fewer than 1% of victims are identified and rescued each year.** The diagnosis is now shared across the field: what is lacking is neither the law nor the technology, but political will, coordination, and investment commensurate with the stakes.

This white paper has a single purpose: to convince Heads of State and the leaders of major technology companies to move this fight from the status of a secondary cause — relegated for a quarter of a century to the margins of international priorities — to that of a civilisational priority. It establishes the urgency, demonstrates the feasibility, and proposes the operational architecture.

The case in numbers

≈ 50 M people in modern slavery worldwide	**< 1%** of victims identified and rescued each year	**≈ $236 bn** estimated annual illicit proceeds of trafficking & modern slavery
≈ $200 bn spent yearly by tech on cyber-fraud & security	**< €200 M** spent worldwide on the fight against trafficking	**× 1000** order of magnitude of the resource mismatch

Note on figures: the International Labour Organization estimates the illegal profits from forced labour alone at US$236 billion per year (2024); broader estimates of the total illicit proceeds of human trafficking and modern slavery, including financial-sector coalition assessments, approach US$500 billion. Either way, the disproportion with the resources devoted to fighting the crime is staggering.

The thesis of this document

- **First,** trafficking is not a technical inevitability. The tools built against cybercrime and financial fraud — AI, network analysis, blockchain analytics, OSINT, behavioural-anomaly detection — would enable an immediate change of scale;
- **Second,** the bottleneck is political and economic, not technological. Platforms are not required to cooperate, legal frameworks are fragmented, and colossal criminal profits contrast with derisory public means;
- **Third,** the solution runs through a Global Coalition of willing Heads of State and technology leaders, backed by a structured investment plan of roughly €1 billion initially and €1.5–2 billion per year — a fraction of what trafficking earns its perpetrators.

> *Human trafficking persists not because of a lack of legal frameworks, but because of insufficient implementation, weak coordination, limited political will, and a severe mismatch between criminal profits and public investment.* — Conclusion of the Rome Conference, 25th anniversary of the Palermo Protocol, December 2025

2. Twenty-five years of effort, under 1% in results

The Palermo Protocol, adopted by the UN General Assembly on 15 November 2000, is among the most widely ratified legal instruments in the world. Yet effectiveness, measured by the number of victims actually rescued, **does not reach 1%**: roughly 100,000 victims freed each year against tens of millions of people exploited. These orders of magnitude — drawn from the US State Department's annual report — are confirmed by UNODC, OSCE and GRETA.

As early as 2015, leading voices — a former special adviser to the UN High Commissioner for Human Rights, the Director of the International Organization for Migration, a representative of UNODC — were already asking the same haunting question: have we made any real impact on the global problem of trafficking in twenty years? The UNODC representative compared trafficking in 2015 to the "white slavery" of the 1920s, observing that the recurring questions and obstacles remained identical.

A crime against humanity, not a footnote

The work conducted since 2013 at the Pontifical Academy of Social Sciences — seventeen seminars, more than 300 speakers from over 70 countries — converges on an unambiguous characterisation. Trafficking is the very negation of the human being: a violent, permanent domination, a social death inflicted on persons stripped of their most basic rights. As early as 2014, eight major religious leaders solemnly called for it to be recognised as a crime against humanity.

> *These new forms of slavery — human trafficking, forced labour, prostitution, organ trade — are very serious crimes, a wound on the body of contemporary humanity.* — Pope Francis, Pontifical Academy of Social Sciences, 2015

The engine of the crime: money

Transnational organised crime bypasses and weakens states; the United Nations estimates the annual revenues of organised crime in the hundreds of billions of dollars. Trafficking is among its most profitable and least risky branches. As a field witness put it before the Pontifical Academy, the only language the mafia understands is the language of money: as long as we merely catch the last links in the chain without striking the financial accumulation that is its essence, the networks will reconstitute themselves indefinitely.

Impunity is near-total. Prosecutions number in the thousands and convictions in the low thousands worldwide, while the vast majority of victims are never identified. In many countries, trafficking remains an invisible crime.

Root causes and aggravating factors

The root causes are well known: poverty, inequality, lack of education and employment, forced migration, conflict, cultural habits. Two aggravating factors compound them: corruption and the misuse of technology. The digital realm has radically transformed the dynamics of trafficking — recruitment through false job offers or the "lover boy" method, exploitation at scale — while institutional responses remain largely technology-neutral.

3. Why this is a civilisational imperative

Reducing trafficking to a humanitarian question would be an analytical error. It strikes at the heart of what democracies claim to uphold and engages, simultaneously, several vital dimensions of international life.

- **A security imperative:** trafficking is driven by transnational criminal networks whose profits finance other trafficking, sometimes terrorism, and destabilise entire states;
- **An economic necessity:** it is one of the most lucrative criminal economies; tolerating it means allowing unfair competition built on exploitation to flourish, including within the supply chains of legitimate firms (mining, textiles, agriculture, fishing, semiconductors);
- **A matter of sovereignty:** control of digital infrastructure and data has become a sovereignty issue; letting that infrastructure serve exploitation means abdicating control of it;
- **A moral imperative:** trafficking is a violation of fundamental rights and human dignity, and a civilisation is measured by how it treats its most vulnerable.

> *Injustice anywhere is a threat to justice everywhere.* — Martin Luther King Jr.

In an interdependent world, exploitation tolerated in one place undermines order, stability and security everywhere. This is therefore neither a peripheral nor a secondary cause: it is a central question of global governance, to be addressed as a moral and legal imperative rather than an act of charity.

4. The central paradox: the technology exists, deployment is missing

The decisive question is simple: can we change the scale of this fight by massively mobilising the tools developed by technology companies against cybercrime and financial fraud? The answer is yes.

The major technology players spend close to US$200 billion every year on fraud detection, cybersecurity, automated moderation and anti-spam systems. Microsoft reports blocking billions of fraud attempts and millions of fake accounts using AI. By contrast, tools specifically dedicated to fighting trafficking remain fragmented, developed by NGOs or small teams, for a worldwide total below €200 million.

What existing technologies already make possible

- data analytics and AI applied to online ads, social media and financial transactions to detect suspicious patterns;
- internet and dark-web monitoring; tools that automatically identify underage victims in online content (e.g. Thorn);
- facial recognition and biometrics for missing persons and international cross-referencing — under strict safeguards;
- blockchain traceability of supply chains and analysis of financial flows and crypto-assets;
- mobile reporting and help-request applications (e.g. Polaris).

Recent operations prove the point: “Global Chain” (Interpol/Europol, 43 countries) identified nearly 1,200 potential victims; “Flash-Weka” (Interpol/AFRIPOL, 54 countries) led to over 1,000 arrests and 823 victims identified. Without shared digital systems, tracking networks that operate across multiple countries would be nearly impossible.

Why technology is not enough — and where the real bottleneck lies

The main obstacle is not a lack of technical knowledge. **It is threefold:**

1. **Political —** no obligation for platforms to cooperate, fragmented legal frameworks, and an unresolved tension between security and liberty. A trafficker banned from one platform reappears on another within minutes;
2. **Economic —** trafficking does not directly affect company revenues, so incentives to invest are weak, and business models built on engagement and openness can conflict with rigorous moderation;
3. **Organisational & structural —** scattered data and incompatible formats, AI still too generic and prone to false positives, encryption and anonymisation, a shortage of specialised units, and inadequate victim protection.

In other words, the technical capabilities exist but are not fully used, because the key actors are not sufficiently compelled to act and because the issue is not yet treated as a global political and economic priority on a par with cybersecurity or terrorism.

5. The levers of a change of scale (the multiplier effect)

Moving from roughly 1% to 10% of victims rescued is ambitious but achievable — provided several levers are pulled at once. Improving a single area yields only limited impact; it is their combination that produces the multiplier effect.

#	Lever	Content
1	Shift from reactive to preventive	Act during recruitment: automatic detection of grooming messages, early warnings for vulnerable individuals, rapid suspension of suspicious accounts.
2	Make platform cooperation mandatory	Share high-risk signals, build common databases, prevent banned users from easily recreating accounts.
3	Scale AI strategically	Real-time analysis, detection of coded language, cross-referencing of images/locations/faces, prioritisation of urgent cases — co-designed with practitioners.
4	Build specialised human capacity	Dedicated units, targeted training, multidisciplinary teams combining technical and field expertise.
5	Reform legal frameworks	Harmonisation, faster but regulated data access, stronger accountability for negligent platforms.
6	Systematically track financial flows	Suspicious-transaction detection, cooperation with banks and fintechs, rapid asset freezing — without money, networks collapse.
7	Strengthen on-the-ground action (decisive)	Local NGO presence, secure housing, legal protection, psychological care: identifying a victim is not the same as rescuing them sustainably.
8	Reduce false positives	More accurate AI, prioritisation systems, strong human validation — so investigators are not overwhelmed and the innocent are not harmed.
9	Address root causes	Poverty, migration pressures, conflict, inequality: trafficking is fundamentally a social and economic problem.

The effect sought is not the product of a single innovation. It results from a composition: **technology × 2, cooperation × 2, human resources × 2, prevention × 2 — approaching a factor of × 10.**

6. The “Moonshot 2035” strategy

In the spirit of John Fitzgerald Kennedy’s intuition in the early 1960s — to send a man to the Moon within ten years — let us imagine an “ideal” situation in 2035 in which every lever works together. This is not science fiction, but pushing to the maximum what is already technically possible today.

Dismantling a transnational network in 2035: the scenario

Step 1 — Early detection (pre-operation). An AI flags an unusual pattern — one account contacting dozens of young women across countries, emotional language, job promises, a shift to encrypted messaging. The system cross-references other platforms, identifies 12 linked accounts and reused images. An alert is generated within minutes, instead of weeks today.

Step 2 — Instant sharing and enrichment. The alert is anonymised, shared with partner platforms and transmitted to a joint cell coordinated by Interpol. In under an hour, the authorities know the network is active in 4 countries and linked to an investigation opened six months earlier.

Step 3 — Smart prioritisation. A specialised AI classifies the case as immediate high-risk (possible minors, coercive signals, imminent travel). Investigators receive a pre-filled file and a complete map of the network.

Step 4 — Coordinated field + digital response. Within 24 hours: synchronised searches across countries, interception of communications, blocking of accounts and transactions. Local teams (police + NGOs) intervene directly with victims.

Step 5 — Immediate victim protection. Safe extraction, adapted housing, legal and psychological support, digital follow-up to avoid relapse or disappearance after rescue.

Step 6 — Financial dismantling. Automatic tracing of flows, freezing of linked accounts, tracking of crypto-assets via blockchain analysis. The network immediately loses its operational capacity.

Step 7 — Expedited forensic exploitation. Structured digital collection, consolidated evidence, clear chains of responsibility, smooth international judicial cooperation: faster and more robust trials.

Overall result: victims identified before full exploitation, intervention in 24–48 hours instead of weeks, networks dismantled simultaneously across countries, recurrence sharply reduced. The scenario rests on three ruptures: mandatory and systemic cooperation, tech–human integration, and very early (pre-operation) intervention.

Even in 2035, limits remain: off-the-radar areas with no digital infrastructure, technical circumvention (mass encryption, deepfakes, synthetic identities), and risks of drift (over-surveillance, algorithmic error, infringements of liberty). These limits do not justify inaction; they define the specification for the safeguards (Section 10).

7. A Global Coalition: architecture and governance

This transformation is achievable around a few strong ideas, which call for a voluntary commitment from Heads of State and technology leaders — the only path out of a situation with which no Head of State and no major executive can be satisfied.

- bring together a coalition of willing Heads of State and the leaders of the major technology companies;
- adapt the best existing technologies to the fight against trafficking and enable their massive deployment in the 50 most vulnerable countries, accounting for linguistic and cultural constraints;
- train, in-country, the public officials working on these issues at scale;
- develop targeted awareness for 100 million at-risk young people;
- act on social determinants, in line with the Sustainable Development Goals.

A launch framework: the G7, then enlargement

The G7 unites the major economic powers, the world's technology leaders, and a capacity for global normative influence. It is the only framework able to launch a founding coalition, in coordination with Interpol and Europol, before progressive enlargement. The coalition is not meant to create yet another body: it must enforce and scale the frameworks and tools that already exist.

Five strategic pillars

Pillar 1 — Platform accountability. Mandatory proactive detection, sharing of high-risk signals, independent audits. Treat trafficking profits as criminal, akin to money laundering or terrorism financing.

Pillar 2 — Shared technology infrastructure. Secure data-sharing platform, pooled AI tools, international standards. Coordination led by Europol and Interpol.

Pillar 3 — Human capacity building. Large-scale training (law enforcement, magistrates, social workers), specialised units, hybrid technology + field teams.

Pillar 4 — Victim protection and support. Immediate access to protection status, funding for safe housing and care, long-term support and reintegration, with a central role for NGOs.

Pillar 5 — Strengthened international coordination. Harmonised procedures, accelerated data exchange, shared governance frameworks, with the involvement of organisations such as the ILO.

Governance

The coalition brings together: willing states; a technology coalition (e.g. Meta, Google, Microsoft and others); international organisations; and an independent committee for evaluation and transparency. This shared governance is the condition of trust — for states, companies and civil society alike.

8. The investment plan (2026–2035)

Achieving a 5-to-10-fold gain in effectiveness requires a structured global investment programme of roughly **€1 billion in initial investment, then €1.5–2 billion per year**. Set against US$236 billion in annual profits from forced labour alone — and broader proceeds approaching US$500 billion — these amounts are modest: this is a change of priority, not a financial effort beyond reach.

Initial investment (2026–2030)

Category	Amount
Technology (platform + robust AI, language adaptation)	€200–500 M
Large-scale training (3–5 years)	€120–400 M
Infrastructure deployment	€100–200 M
Total initial	≈ €1 billion

Target annual budget (from 2030)

Category	Amount / year
Infrastructure & international coordination	€150–350 M
Victim support (often underfunded)	€600 M – €2 bn
Total annual	≈ €1.5 billion / year

A balanced funding split

Contributor	Share
States	40%
Technology companies	30%
International institutions	20%
NGOs / foundations	10%

Without clear costing, governments underestimate the scale of the effort, companies downplay their responsibility, NGOs remain underfunded, and policies stay largely symbolic. That is precisely why only 1–2% of victims are rescued today.

9. What is asked of Heads of State

The challenge is no longer one of technical means, but of political coordination and structured investment. Heads of State hold the decisive lever.

- **States–Tech coalition:** create a strategic alliance between states (starting with the G7, in coordination with Interpol and Europol) and tech leaders, to set global standards, pool capabilities and accelerate implementation;
- **Platform accountability:** move from a voluntary approach to a structured framework: mandatory proactive detection, sharing of high-risk signals, independent audits;
- **Addressing root causes:** align action with the Sustainable Development Goals (poverty, inequality, discrimination), with the support of the ILO;
- **Massive capacity building:** train tens of thousands of actors, deploy in vulnerable countries, support NGOs;
- **Investment and law:** equip the fight with budgets comparable to anti-drug policies, treat trafficking profits as seizable criminal assets, and harmonise legal frameworks.

> *One can resist the invasion of armies; one cannot resist the invasion of ideas.* — Victor Hugo

The idea that this cause must become a major political priority is now irreversible. The only question is whether leaders will choose to be its architects, or merely the ones who delayed it.

10. What is asked of technology leaders

Your companies have built the world's digital infrastructure. Now essential drivers of global growth, they are also being exploited by criminal networks on an unprecedented scale. This creates a new responsibility — but also a historic opportunity: to transform these technologies of connection into global infrastructures of protection. This is not an innovation gap, but a challenge of deployment, adaptation and access across some fifty vulnerable countries.

A flexible commitment framework

- **Differentiated access to technology:** solutions adapted to constrained environments, tailored pricing models (credits, solidarity licences, targeted pro bono), low-bandwidth and offline-capable solutions;
- **Technological adaptation:** AI models for under-resourced languages, enhanced behavioural and network detection, simplified interfaces for field use;
- **Secure capacity sharing:** sharing of aggregated and anonymised signals, dissemination of best practice, provision of analytical tools;
- **Financial contribution:** participation in an International Innovation and Deployment Fund, indicative contribution of €20–100 million per company over five years;
- **Human capacity building:** training programmes (law enforcement, NGOs, judiciary), transfer of expertise, support for local training academies.

The value proposition

- **Strategic influence:** participation in shaping international standards and emerging regulatory frameworks;
- **Regulatory anticipation:** better anticipation of future requirements, reduced exposure to regulatory fragmentation;
- **Market positioning:** preferential access to public ecosystems in emerging markets, anchoring within national digital infrastructures;
- **Reputational leadership:** a shift from a defensive to a proactive posture, leadership on a critical global issue, strengthened credibility with ESG-focused investors.

Concretely, we propose a confidential high-level exchange (CEO / VP Public Policy / VP Trust & Safety), participation in a small group of founding partners, and a contribution to the initial structuring of the programme.

11. Ethical safeguards: effectiveness without drift

The technological ramp-up will be legitimate — and durable — only if it scrupulously respects fundamental freedoms. The more effective the tools, the more complex the ethical and legal challenges. Three risks must be addressed head-on, with explicit mitigation measures.

Risk	Mitigation measure
Infringements of individual liberties, over-surveillance	Judicial oversight, data minimisation and anonymisation, refusal of mass surveillance
Algorithmic bias and error, false positives	Strong human validation, independent audits, specialised AI co-designed with practitioners
Dependence on private actors	Shared international governance, open standards, independent transparency committee

The central challenge remains: to combat criminal networks effectively without sliding into excessive surveillance of populations. Safeguards are not a brake on effectiveness; they are its condition of legitimacy.

12. Conclusion: the time for commitment

History will remember not only what we knew, but what we chose to do — or not to do. Faced with a tragedy that deprives millions of human beings of their freedom, their dignity and often their future, silence is no longer an option. To allow suffering to continue when action is possible is already a form of abdication; inaction is not neutral — it carries a human, moral and historical cost.

Great leaders are distinguished by the passage from indifference to commitment. The tools exist, financial resources are globally available, and the diagnosis is unanimous. The only remaining obstacle is a decision: to structure and fund a coordinated global effort, with clear objectives, adequate means and credible accountability mechanisms.

> *The time is always right to do what is right.* — Martin Luther King Jr.

The world is not waiting for another diagnosis. It is waiting for commitment. It is waiting for a coalition, now.

It is possible to free one million victims from modern slavery and to save one million human lives per year. If we want to, today.