Brain-be 2.0
Belgian Research Action through Interdisciplinary Networks
POLICY BRIEF

Policy Brief n° 5

BE-FORINTEL - BUILDING THE FOUNDATIONS OF A FORENSIC INTELLIGENCE TOOL IN BELGIUM: The Feasibility of a Forensic Intelligence Tool in Belgium

This feasibility study examined whether Belgium can realistically implement forensic intelligence (FI) tools that convert forensic traces into actionable intelligence for policing. Drawing on eight expert interviews and a national survey of 51 practitioners across forensic science, policing, law, government, and IT, one clear result stands out: among three tool types, traditional cross-case forensic data analysis is viewed as by far the most feasible, useful, and legally secure option in the short to medium term. Over 80% of survey respondents judged this tool both realistic and legally acceptable, and interviewees described it as a natural extension of existing laboratory practice rather than a radical reform. By contrast, more integrated tools that link police and forensic databases, or create holistic views, are seen as aspirational but heavily constrained by data-protection law, governance gaps, and technical fragmentation. The central finding is therefore that Belgium can move concretely toward FI today by strengthening and systematizing the cross-case analytical work performed in its forensic laboratories.

Context and question(s) of research

FI aims to move forensic science from a purely case-by-case, evidential role towards a proactive intelligence function, where traces (such as DNA, fingerprints, ballistics, chemical profiles, and digital artefacts) are analyzed across cases to reveal patterns, link series, and support strategic decision-making (Ribaux et al., 2003; Ribaux & Wright, 2014). International examples show that FI can help tackle case linkage blindness by uncovering connections that remain hidden when cases, agencies, or datasets are siloed (Baechler et al., 2012; Morelato et al., 2014). At the same time, implementing FI raises complex questions around data protection, proportionality, and governance, particularly in jurisdictions with strong privacy frameworks.

Belgium represents a challenging but promising environment. Its justice and policing systems are decentralized. This means there are separate local police zones, federal investigative services, and multiple forensic laboratories at various levels. Data is distributed across different platforms, identifiers and coding systems, and thus is governed by strict laws, including the Belgian Data Protection Law (2018) which implements the Law Enforcement Directive (EU 2016/680) and the Law on Police Services. These then create both a legal basis for specialized police databases (Article 44/11/3) and firm boundaries on how personal and biometric data may be processed and combined. Within this context, our study asked how experts and practitioners assess the feasibility, usefulness, and risks of three FI tools: traditional forensic data analysis, information-sharing and forensic integration, and a holistic data-view tool. This policy brief focuses on the main result that cuts across all data sources: which tool is considered realistically implementable today?

Main findings

Both interviews and survey responses converge on a single, clear conclusion: traditional forensic data analysis define by systematic cross-case comparison of the existing forensic traces within and across laboratories is the FI tool that Belgium can implement first. Survey data show near-unanimous support: 41 out of 51 respondents judged this tool useful, similarly, 41 considered it realistic to implement in Belgium, and 40 believed it to be legally and ethically secure. These are the strongest scores across all three tools, and they come from a sample dominated by forensic practitioners (but also including police, legal, policy, and IT experts).

When asked to explain why this tool stands out experts explained that forensic laboratories already conduct scientific comparisons of traces within individual cases. In addition, magistrates can authorize cross-case comparisons under current law, and laboratory information systems are structured around such trace analysis. In practice, therefore, a traditional FI tool largely formalizes and strengthens work that is already being done: making cross-case comparison more systematic, standardized, and timely, rather than inventing an entirely new process. Despite this promise, experts noted that this

tool requires investment in staffing, coding harmonization, and laboratory information management systems, but does not demand major legal reform or a new national platform linking all police and justice databases.

By contrast, respondents were more cautious about tools that integrate forensic and police data in shared platforms, and especially about holistic. While these more ambitious tools were understood to be useful in principle, concerns about legal compliance, governance, role definition, access control, cybersecurity, and political acceptability increased sharply. Practitioners pointed to persistent data silos, incompatible systems, unclear data controllership, and differing security clearances as major obstacles. Many stressed that combining multiple sensitive datasets into a single environment would require new authorizations, strong oversight structures, and significantly more resources. As a result, they framed such tools as longer-term goals rather than realistic near-term options. Taken together, the central empirical message is that Belgium does not face an "all-or-nothing" choice between no FI and a fully holistic fusion center. There is concrete, widely supported entry point: scaling up traditional forensic cross-case analysis into a structured FI capability embedded in existing laboratory workflows.

Conclusion and recommendations

In practical terms, policymakers should priorities investments that allow laboratories to turn existing data into more systematic intelligence products: reinforcing laboratory staffing and analytical capacity; harmonizing coding schemes and identifiers across laboratories; improving laboratory information management systems; and creating clear procedures for generating and disseminating cross-case linkage reports. These steps respond directly to experts' concerns about workload, fragmentation, and data quality, while staying comfortably within current legal boundaries.

At the same time, the strong but more cautious interest in information-sharing and integrated tools suggests that Belgium should prepare the ground for the next phase. This includes working toward common case identifiers that can link forensic and police records without duplicating personal data; establishing governance arrangements that clearly distinguish data controllers from processors; and designing access-controlled, auditable interfaces rather than unconstrained data pools. Any future move toward more integrated systems will also require sustained training for magistrates, police, and forensic personnel on interpreting FI outputs and applying data-protection principles in practice.

The core policy message is therefore incremental. Belgium can and should develop FI, but it should begin by formalizing and scaling the traditional forensic analysis that practitioners already trust. Doing so will deliver visible benefits for investigations in the short term, demonstrate the value of FI in the Belgian context, and create the technical and organizational foundation needed for more ambitious integration in the future, all while respecting the strict privacy and proportionality standards that underpin the Belgian and European legal order.

Read more

- Harvey, D. L., Madjlessi, J., Kumar, K., & Vandeviver, C. (2026). Enhancing criminal network disruption through forensic intelligence: A scoping review [Preprint].
- Harvey, D. L., Vander Beken, T., Kumar, K., & Vandeviver, C. (2026). Feasibility of forensic intelligence in Belgium: A mixed-methods assessment of legal, organizational, and technical constraints [Preprint].
- Harvey, D. L., Geeraert, J., & Vandeviver, C. (2026). Observability and disruption in criminal networks: A simulation study of forensic intelligence [Preprint].
- Harvey, D. L., & Vandeviver, C. (2026). Examining observability in forensic-enhanced criminal networks: Evidence from empirical network reconstruction [Preprint].
- Harvey, D. L., & Vandeviver, C. (2026). The added value of forensic intelligence in criminal network analysis: Evidence from empirical network reconstruction [Preprint].
- Klymentiev, R., Harvey, D. L., Rocha, L. E. C., & Vandeviver, C. (2025). A systematic review and Bayesian meta-analysis of co-offending characteristics. Nature Human Behaviour, 9(10), 2135–2152. https://doi.org/10.1038/s41562-025-02244-z
- Vandeviver, C. (2023). The future of big data policing for law enforcement agencies [Lecture].

Information

Harvey, Dayle
University of Ghent
e-mail: dayle.harvey@ugent.be

Vandeviver, Christophe
University of Ghent
e-mail: christophe.vandeviver@ughent.be

***BRAIN-be 2.0**: BELSPO (the Public Planning Service Science Policy) organises a research programme designed to strengthen the scientific basis of federal public policy and the strategy and potential of the Federal Scientific Institutions (FSI) since 2012.*

More: www.belspo.be/brain-be