View this email in your browser

GANNDALF

NextGen Collaborative Cybercrime Investigation Framework

4th Newsletter

Building the EU's NextGen investigation framework against advanced forms of cyber threats and cyber-dependent crimes.



GANNDALF is an EU-funded Horizon Europe R&D project designed to empower Law Enforcement Agencies (LEAs) and the wider judicial ecosystem in detecting, investigating, and preventing advanced cybercrime.
The project develops a secure, modular collaboration framework with privacy-aware data sharing, AI-powered decision support tools, and a customizable sandbox for collaborative investigation.

Beyond technology, GANNDALF promotes policy innovation, professional training, and citizen engagement through its Cyber Hygiene 2.0 approach, helping society recognise, report, and resist cyber threats more effectively.

Learn more

Discover GANNDALF's Use Cases!

See GANNDALF in action!



How can innovative technologies support real-life cybercrime investigations?

Our second GANNDALF project video takes a closer look at the project's use cases, showcasing how AI-powered tools and advanced technologies can support law enforcement agencies in tackling different cybercrime challenges.

Discover how GANNDALF's solutions can enhance investigations, improve collaboration and support more effective responses to emerging cyber threats.

Technical & Cybersecurity
Tools to help Law Enforcement Agencies detect, analyse, investigate and respond to cyberattacks, strengthening the resilience of public-

Cross-border Cooperation
Secure information exchange and coordinated investigations between law enforcement agencies across different countries, supporting effective

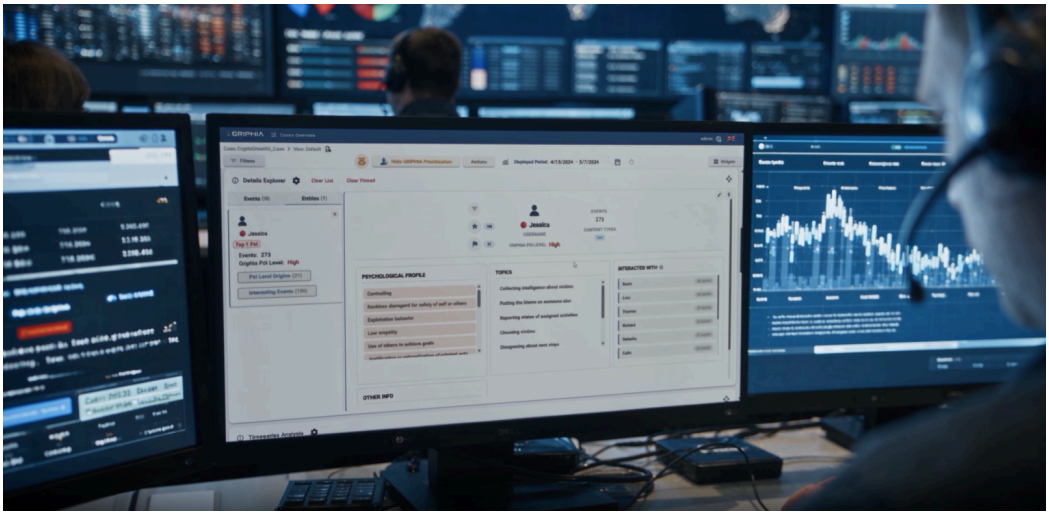
Training & Awareness
Multilingual training and practical exercises for investigators, together with GANNDALF's Cyber Hygiene 2.0 approach to strengthen cybersecurity awareness among

safety infrastructure and critical systems.

international cooperation.

professionals and citizens.

Explore All Use Cases



GANNDALF Technology Highlights

GANNDALF Portal
One workspace to run, follow and share cybercrime investigations.

Security Infusion (SecInf)
Monitor infrastructure, detect threats and investigate security incidents.

Scenario Building Tool
Create realistic scenarios, practise responses and capture lessons learned.

Human Swarm Teaming (HST)
Identify cyber threats in near real time with the support of an AI swarm.

Explainable AI (XAI)
Make AI findings easier to understand and assess through accessible explanations.

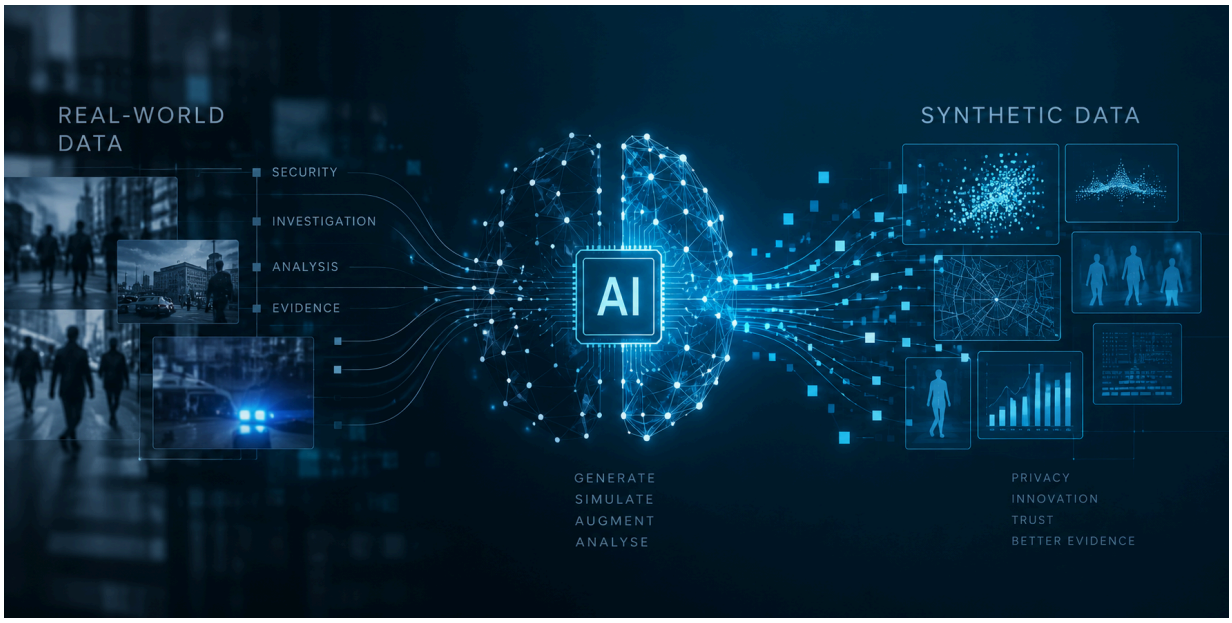
Forensics Visualization Toolkit (FVT)
Connect related alerts to identify incidents and understand their links.

Discover all GANNDALF technologies and explore how they support cybercrime investigations.

Research & Insight

SYNTHETIC DATA IN RESEARCH ON INVESTIGATIVE TECHNOLOGIES PART 2: WHAT GENERATION DOES NOT SETTLE

By Pablo Trigo Kramcsák — Vrije Universiteit Brussel (VUB)



Part one set out why research on investigative technologies generates its own data, and the rule of preference that follows: real personal data require justification where synthetic data would serve. The rule rests on the assumption that synthetic data fall outside data protection law. This part asks whether they do, and what follows if they do.

Synthetic data and anonymisation as distinct operations

Synthetic records generated under appropriate constraints do not correspond to identifiable individuals. The dataset is sampled from a model of a distribution rather than transcribed, masked or transformed from existing records, and the resulting rows describe individuals who do not exist. Information of that character does not relate to an identified or identifiable natural person in content, purpose or effect, and it does not, in itself, appear to fall within the material scope of the Regulation.

Anonymisation and generation are frequently treated as variants of a single technique, although they operate differently. Anonymisation starts from real records and alters them, scrambling or masking the features that would otherwise identify the

people behind the original data. It removes or generalises attributes until the residual link to the data subject may be regarded as insignificant. Generation follows two routes. Rule-based simulation and expert authorship involve no personal data, subject to the possibility that authored scenarios inadvertently incorporate real identifiers. A generative model fitted to a real dataset retains a statistical representation rather than the records themselves, and each output constitutes a draw from that representation.

Three qualifications apply. First, the conclusion depends on the construction of the generator: a model that overfits or is otherwise insufficiently constrained may memorise and reproduce source records, in which case the outputs correspond to identifiable individuals. Second, synthetic data do not prevent inference attacks. Third, the dataset and the generator raise separate questions. The European Data Protection Board has taken the view that a model trained on personal data is not anonymous merely because it does not retain records in directly retrievable form, and that reasoning would extend to generative models.

TheBoard's anonymisation guidelines (for public consultation)support this reading, since the relative approach they adopt makes anonymity a function of the position of the data holder rather than a property the dataset carries with it. An inference engages the 'No Inference' criterion only where it is specific and meaningful, which requires that it relate to the original dataset rather than to general knowledge or to the population at large, and that it be capable of affecting the rights of a data subject. The Board also observes that querying synthetic data may permit conclusions to be drawn concerning a particular individual and that a meaningful inference of that kind violates the criterion.

What it does not settle

A determination that artificially generated material falls outside the scope of the GDPR resolves a question about that material alone, and leaves several issues open.

Other obligations remain in place. Data protection law is one regime among several bearing on the development and deployment of investigative technologies, and a conclusion reached under it does not necessarily travel. Requirements concerning dataset quality and representativeness, non-discrimination, and procedural fairness in the decisions such systems inform attach irrespective of the status of the underlying material. A developer that generates its training material accordingly substitutes one set of obligations for another rather than escaping scrutiny, and the obligations so acquired are arguably the more demanding, since representativeness must be established against a distribution the developer has itself modelled.

Risk also moves rather than disappearing. The assumptions that make simulated material safe at the level of the identified person are the same assumptions through

which historical enforcement patterns enter a dataset containing no individual record. A generator fitted to where policing has concentrated will reproduce that concentration, and it will do so in a file that names nobody. The resulting harms fall on populations rather than persons, and data protection law reaches populations only obliquely.

There is also what generation simply cannot supply. A benchmark built to balance classes says nothing about prevalence in the setting where the system will actually run, which leaves the operational false-positive burden unmeasured. The mechanism that produced a file constrains what questions can properly be asked of it, and an analyst who ignores that mechanism may draw inferences the data do not support.

Using synthetic data well

Artificially created datasets have an important place in research on investigative technologies. The comparison that matters is not with an ideal dataset. It is with the arrangement generation would displace, in which operational records stay with the authorities holding them, under regimes that do not reach research consortia, and the incidents of interest are too rare to provide an evidential base. Against that, an artificially generated dataset can at least be published and re-run by people with no stake in the result, and without that possibility no claim about detection performance can really be contested. The limitations set out above are therefore conditions on use rather than objections to it. They require the assumptions built into a generator to be made explicit and open to challenge, representativeness to be demonstrated rather than presumed, and performance figures to be interpreted in light of the prevalence that can reasonably be expected in the setting in which the system will operate.

Read Part 1

GANNDALF’s upcoming pilot in València is making the news!

In 2027, València Local Police will coordinate an operational pilot simulating a cyberattack against its Integrated Security and Emergency Centre (CISE).
The exercise will bring GANNDALF partners together to test innovative European solutions designed to:

- Detect and assess cyber threats.
- Support risk and vulnerability analysis.

- Improve collaborative investigation and decision-making.
- Coordinate incident containment and system recovery.
- Strengthen the continuity of essential police services.

The pilot will be conducted in a controlled environment using simulated scenarios and synthetic data.
The initiative has already received coverage from the City Council of València, EFE Comunitat Valenciana and several regional media outlets.

The results will contribute to the final evaluation of GANNDALF's tools and to recommendations concerning their potential future use by European law enforcement agencies.

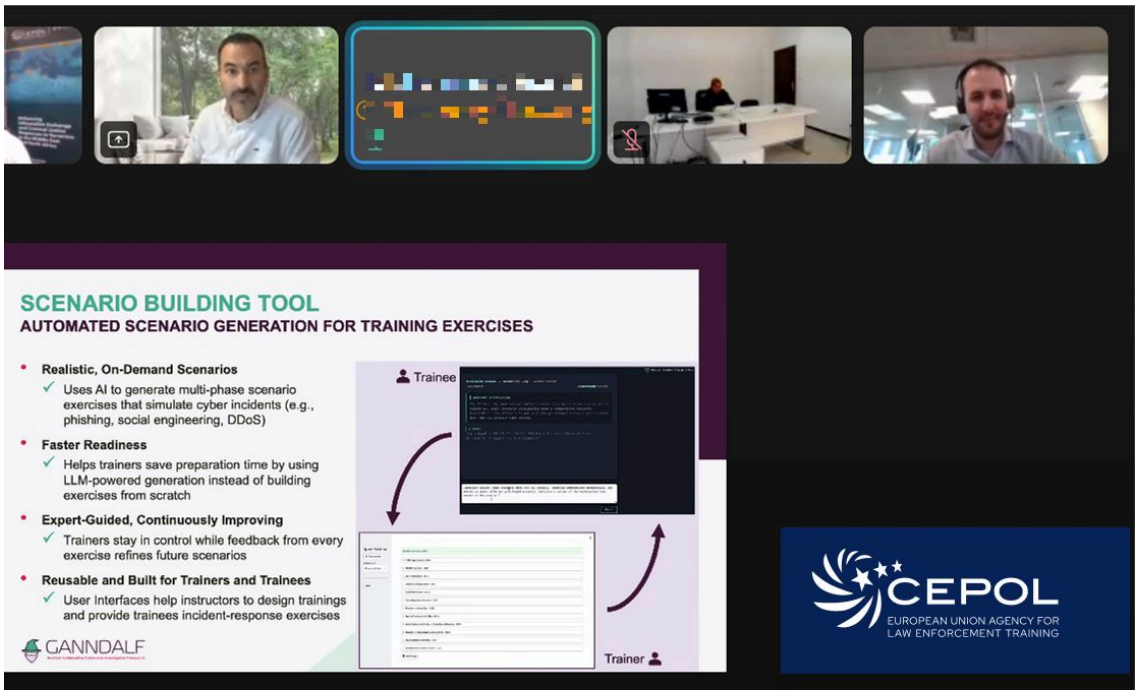
Read the coverage:

- Official announcement – City Council of València
- EFE Comunitat Valenciana
- Valencia Plaza
- València Extra
- Actualidad Valencia

Dissemination highlights

GANNDALF CONTRIBUTES TO THE CT INFLOW II SEMINAR

September 2026



GANNDALF recently took part in the **EMISA Seminar Research and Science CT INFLOW II**, presenting some of the project's solutions and their potential value for law enforcement agencies.
The session prompted an engaging discussion on key challenges for the responsible use of AI in investigations, including:

- Preventing AI-generated hallucinations from misleading investigators or compromising digital evidence.
- Ensuring that AI remains a decision-support tool under meaningful human supervision.
- Enabling secure cross-border information sharing while respecting national sovereignty.
- Exploring sovereign, on-premises deployment of collaborative investigation environments.
- Maintaining human review and clear institutional responsibility when AI-supported analysis identifies potential criminal activity.

These questions lie at the heart of GANNDALF's work to develop trustworthy, secure and operationally relevant technologies for fighting advanced crime.

Read more

From Criminal Evidence to Conclusions with GRIPHIA

September 2026

GRIPHIA, developed by GANNDALF partner AEGIS IT RESEARCH, has been featured on the European Commission's EU Innovation Platform, highlighting its potential to support law-enforcement authorities in tackling complex digital investigations.
GRIPHIA combines advanced forensic techniques with investigative psychology to process and connect fragmented digital evidence, helping investigators identify relevant entities, uncover hidden relationships and prioritise suspects or events.
Among its key capabilities are identity attribution and entity resolution, evidence correlation, analysis of text, audio and metadata, detection of emotional and behavioural indicators, and visualisation of relationships and investigative timelines.
Within GANNDALF, GRIPHIA is being further developed and integrated into the project's Crime Psychology Toolbox, where it will contribute to several investigative use cases and help transform complex digital evidence into actionable investigative insights.

This recognition by the European Commission represents an important step in bringing GRIPHIA's innovative capabilities closer to the European law-enforcement community.

Discover how GRIPHIA is helping turn complex digital evidence into actionable investigative insights and explore its role within GANNDALF.



Read more

3rd Plenary Meeting - Day 1: Training

October 2026



GANNDALF partners gathered in Lisbon for a new round of collaboration, knowledge exchange and hands-on work.
The first day focused on cybersecurity, training and the operational needs of Law Enforcement Agencies (LEAs), with external LEAs also joining the training. In parallel, technical partners held dedicated sessions to connect GANNDALF's technological developments with real-world investigative challenges.
Stay tuned for more updates from Lisbon and discover how GANNDALF is turning innovation into practical solutions for law enforcement!

Read more

GANNDALF concludes its 3rd Plenary Meeting in Lisbon!

October 2026



Three days of training, technical discussions and collaboration have brought the GANNDALF consortium together in Lisbon to strengthen cooperation and drive the project forward.

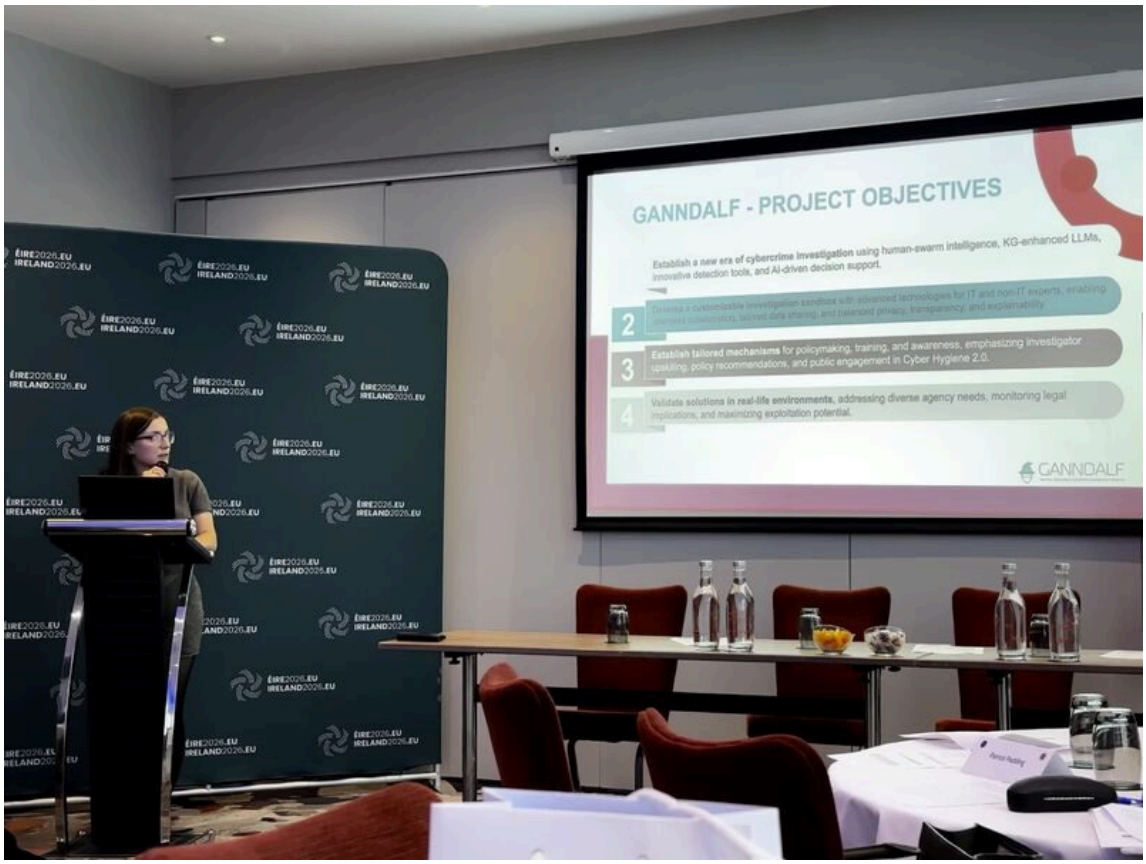
The final day focused on reviewing key deliverables, assessing progress and preparing for the upcoming project review, ensuring that the consortium remains aligned on its objectives and next steps.

A big thank you to Polícia Judiciária, INOV and all GANNDALF partners for their valuable contributions, active participation and continued commitment to the project.
We leave Lisbon with fresh insights, stronger collaboration and a shared ambition: **turning innovation into practical solutions to combat cybercrime across Europe.**

Read more

Connecting with European Law Enforcement at ENLETS

October 2026



On 29–30 October, the **Polish Platform for Homeland Security** presented GANNDALF at the **ENLETS NCP Face-to-Face Meeting** in Limerick, Ireland.

The meeting brought together European law enforcement and security experts to exchange knowledge, explore new technologies and strengthen cooperation.
PPHS introduced GANNDALF's main objectives, raising awareness of the project and its upcoming activities among European law enforcement stakeholders.

Another great opportunity to increase the project's visibility and connect with the European security community.

Read more

Barcelona Cybersecurity Congress 2026

November 2026



València Local Police presented GANNDALF at the Barcelona Cybersecurity Congress 2026 with the presentation **"Cyber Resilience of Emergency Coordination Centres from a Law Enforcement Perspective."**

José Luis Diego (Police Inspector and Chief of Staff to the Chief Commissioner) and Rubén Fernández (Police Officer and Project Manager) shared the end-user perspective behind the GANNDALF pilot led by València Local Police, focusing on the protection of the city's Emergency Coordination Centre and the critical infrastructure supporting emergency calls and dispatch services.

The presentation highlighted how GANNDALF technologies will be validated through realistic cyberattack scenarios.

The session also highlighted the importance of bridging the gap between European cybersecurity research and the operational needs of law enforcement agencies.

Read more

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement No. 101167951. The website reflects only the view of the author(s) and the Commission is not responsible for any use that may be made of the information it contains.



GANNDALF

NextGen Collaborative Cybercrime Investigation Framework

*Copyright (C) *|CURRENT_YEAR|**

Want to change how you receive these emails?

You can update your preferences or unsubscribe

