25 Years of OLAF - the Office's Digital Transformation and Some Reflections on What Lies Ahead

Konstantinos Bovalis, Georg Roebling *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

In today's fast-changing world, the issue of digitalisation – or "tech" – is rapidly moving up the agenda. This observation also very much applies to the anti-fraud domain. On the occasion of the 25th anniversary of the European Anti-Fraud Office (OLAF) in 2024, this article provides a retrospective of the progressive digitalisation of work at the Office. Arriving at today's "digital first" paradigm has been a long journey since OLAF's humble digital beginnings in 1999. The authors also review the parallel evolution of OLAF's legal framework for data collection and data processing, and they offer some reflections on further digital challenges ahead.

AUTHORS

Konstantinos Bovalis

Head of Unit
European Commission / European Anti-Fraud Office (OLAF)

Georg Roebling

Head of Unit
European Commission / European Anti-Fraud Office (OLAF)

CITATION SUGGESTION

K. Bovalis, G. Roebling, "25 Years of OLAF - the Office's Digital Transformation and Some Reflections on What Lies Ahead", 2024, Vol. 19(4), eucrim, pp306–315. DOI: https://doi.org/10.30709/eucrim-2024-023

Published in
2024, Vol. 19(4) eucrim pp 306 – 315
ISSN: 1862-6947
https://eucrim.eu

I. Introduction

The last 25 years, which the European Anti-Fraud Office (OLAF) looks back on with pride, have witnessed many changes in the world around us. However, few have been as far-reaching and consequential as the pervasive digitalisation of virtually all aspects of our modern societies, including, notably, the work life. The work of fraud busters is of course no exception, and this applies both to the fraud and its busting.

This article first explores how the evolving legal framework governing OLAF's preventive and investigative work has supported and exerted an influence on OLAF's digital transition over the years. Secondly, it provides a practical overview of OLAF's digital transformation. And thirdly, we reflect on some of the digital challenges ahead.

II. OLAF's Evolving Legal Framework and Digital Evolution

OLAF has undergone several stages of its legal framework. The following examines OLAF's digital work within the initial legal framework, i.e., the OLAF Regulation 1073/1999[1] (hereinafter referred to as the "1999 OLAF Regulation"), and the current legal framework based on Regulation 883/2013[2], as amended notably by Regulation 2020/2223[3] (together referred to as "the current OLAF Regulation").

The analysis is built upon three main areas: First, the access to data that OLAF collects from a variety of sources via different means. Second, the processing of data following their acquisition. And third, we describe the digital setup in which OLAF performed its work under each legal framework. All these elements combined make up what we understand as OLAF's digital transformation.

1. Digital operations under OLAF's initial legal framework – the 1999 OLAF Regulation

OLAF's initial legal framework established by Regulation (EC) 1073/1999 was inevitably still a product of the twentieth century. Even though the dawn of the digital age was already on the horizon, the initial OLAF Regulation did not contain many, let alone exhaustive references to the issues we would today associate with digitalisation.

a) Access to data

In one key respect, the 1999 OLAF Regulation was already crafted in a sufficiently forward-looking manner to pave the way for the digital transition: regarding the type of data the Office would have access to. This is evidently a fundamental precondition for the Office to effectively carry out its mandate in a digital environment. As Advocate General *Francis Jacobs* observed in 2002 in the *EIB* case. [4]

> If OLAF were not empowered to access documents and data, take copies, ensure that documents and data are secured where necessary, and ask for oral information, its ability to uncover fraud and other irregularities would be severely limited.

The issue of accessing data, including electronic data was clearly set out in the 1999 OLAF Regulation in relation to **internal investigations**. In such instances, OLAF access was not limited to (paper) documents, but also covered other types of information. Pursuant to Art. 4(2) of that Regulation, OLAF was empowered to

"take a copy of and obtain extracts from any document or the contents of any data medium held by the institutions, bodies, offices and agencies and, if necessary, assume custody of such documents or data to ensure that there is no danger of their disappearing."[5] This innovative provision already considered the concept of data to which OLAF was conferred a right of access. With data underpinning virtually all forms of digitalisation, this terminology laid the groundwork that would allow the OLAF Regulation to adjust flexibly to the evolving digital landscape.

As concerns **external investigations**, Art. 3 of Regulation 1073/1999 incorporated the provisions of Council Regulation No 2185/96 concerning on-the-spot checks and inspections carried out by the Commission.[6] The Regulation's Art. 7(1) established that inspectors shall have access, like national inspectors, "to all the information and documentation on the operations concerned".

The use of the two words "information and documentation" already implied that the concept of information was to be distinguished from a traditional document. Upon closer inspection, it becomes evident that the term "information" is to be understood very widely, and notably encompasses all possible forms of data: Art. 7 of Regulation 2185/96 provides a long list of examples as to what such information may comprise, including "computer data".[7]

Also elsewhere, the 1999 OLAF Regulation used a broad concept of the term "information", encompassing "documents" and "data". The term "information" was also used in this sense in Art. 7(2) and (3) of Regulation 1073/1999 expressing the duty – incumbent on both Member States and Community institutions, bodies, offices, and agencies – to let OLAF know of possible cases of fraud, corruption, and other illegal activities.

OLAF access to a wide variety of data, as described, has not substantially changed over the last 25 years. Rather, subsequent revisions of the OLAF Regulation have specified and strengthened this access to certain data categories which have been deemed essential to anti-fraud investigations.

b) Data processing

Article 3(3) of Regulation 2018/1725[8] setting out the data protection rules applicable to the EU institutions, bodies, offices and agencies provides a good summary of what such processing may consist of: any operation or set of operations which is performed on data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The 1999 OLAF Regulation did not lay down in any detail how, where, and under which conditions the data collected by the Office should be processed. Notably, the question of *data storage* was not at all addressed in that Regulation.

However, as concerns *data analysis*, the 1999 Decision creating the Office[9] established in Art. 2(5)(b) that the Office shall be responsible for any other operational activity of the Commission in relation to the fight against fraud, including the collection and analysis of information. However, the Decision did not add any further conditions for the conduct of such analysis.

c) Being digital 25 years ago

In the years prior to the foundation of the Office in 1999, the administrative world in which it was embedded was based on digital databases with limited functionalities and split in scope. These were in essence the IRENE database (IRregularities, Enquiries, Exploration) for irregularities reported by the Member States, and

Pre-IRENE, the then UCLAF internal case management database, which contained information on cases not reported by the Member States.

These databases suffered from weak performance, incompleteness of records, user-unfriendliness, limited querying capabilities (in turn preventing reporting), and a lack of standardisation related to the descriptions of fraud and irregularities. Interconnection was out of the question. As a result, the databases were not used systematically within the Office and a lot of information was still kept on paper or in electronic spreadsheets on local disc drives. Digital information maintained this way, mainly took the form of unstructured documents processed manually before being printed for further circulation (on trolleys being pushed from one office to another), reviewed, approved, and signed by hand.

During the Office's first on-the-spot checks, the amount of work carried out was typically expressed in meters (of physical file storage to plough through), not terabytes. And although digital forensics equipment existed and was occasionally used at the time, the pride and joy of the intelligence unit was a high-performance scanner that easily weighed 25kg and could process several thousand pages per hour.

Remote access to OLAF hosted systems and their data was not possible, and even from within the Office, desktop applications installed on the bulky personal computers of this still premature digital era were needed to enable access to local IT systems and applications. Access to the Internet was slow and subject to staff queuing behind the very limited number of computers connected to it. National and European authorities had barely begun implementing new data protection rules established by Regulation 95/46/EC.

2. Digital operations under OLAF's current legal framework – the 2013 OLAF Regulation (as amended in 2020)

The current OLAF Regulation still mentions the terms "documentation, information and also data" in various places, including the crucial clarification that this applies "irrespective of the medium on which it is stored."

However, today's approach is more consistent in the sense that the term "document" matches the definition given in Art. 3(a) of Regulation No 1049/2001, i.e., content (no matter the medium, written or digital) related to a subject matter (therefore carrying a specific meaning), whereas the term "data" is used as a complement of the above to denote a unit of raw material which does not carry a specific meaning. References to "personal data" should be read as information "related to an identified or identifiable natural person" as per Art. 3(1) of Regulation 2018/1725.

a) Access to data

The by now well-established OLAF access to a wide set of data in internal and external investigations has been **clarified and extended** in a number of directions in recent years. First of all, Art. 6(1) of the current OLAF Regulation establishes that the Office shall have, under certain conditions, access to "any relevant information in databases held by the institutions, bodies, offices or agencies" even prior to the opening of an investigation. Secondly, pursuant to Art.7(3a), OLAF also has access to certain data concerning bank accounts, including – in cases where this is strictly necessary for the purposes of the investigation – the record of transactions. Thirdly, Arts. 3(5) and 4(2a) confirm, as a matter of principle, Office access to data on privately owned devices that are used for work purposes.

One of the most substantial changes over the last quarter of a century relates to OLAF access to relevant data via a **digital forensic acquisition**. In the context of internal investigations, such acquisitions of data held by the institutions, bodies, offices, and agencies may occur in or without the presence of the data owner.

Such operations are typically among the most privacy-invasive investigative measures which OLAF is empowered to undertake.

The possibility of such digital forensic acquisitions in internal investigations actually already existed prior to the entry into force of the 1999 OLAF Regulation.[10] This situation established by case law was then codified in Art. 4(2) of the 1999 OLAF Regulation and in Art. 7(1) Regulation 2185/1996, which also applies to external investigations. However, a quarter of a century ago, digital forensic acquisition was still a new and relatively rare investigative measure compared to today, mainly because of the low level of digital readiness in administration and businesses. In this sense, investigative practices in connection with digital forensic acquisition have changed profoundly.

In 2016 OLAF adopted Guidelines on Digital Forensic Procedures for OLAF Staff.[11] These Guidelines are binding and set out which procedural steps and technical precautions must be observed by the Office. They were confirmed by the ECJ in *Vialto*.[12] In substance, OLAF's digital forensic actions have always been carried out with potential use of the data as evidence in judicial proceedings in mind. Therefore, the Guidelines adhere to internationally accepted standards of digital forensic acquisitions (e.g., chain of evidence, documentation, and non-alteration of data).

The European courts have also established certain boundaries which apply when OLAF is collecting data. A good illustration is the Order of the General Court in the *LG* case[13], which indicates that the principle of legal professional privilege may also apply in the context of anti-fraud investigations in a similar way as it does in the anti-trust domain.

b) Data processing

In the same vein, the current OLAF Regulation remains largely silent on the conditions under which the Office may process data (in the wide sense presented above). The only exception is a reference in Art. 12g(2) (in the context of OLAF's cooperation with the European Public Prosecutor's Office) to managing OLAF's data in a **case management system**. Notably, the OLAF Regulation as such does not specify where the Office should store its data, e.g., on a server hosted locally or in the cloud.

Nonetheless, when designing an in-house **data storage** system, the Office needs to take confidentiality requirements into account so as to prevent leakages. This results, first of all, from Art. 10(1) and (2) of the current OLAF Regulation. Further legal constraints in that respect arise from the European data protection rules pursuant to Regulation 2018/1725. Art. 8(3) of the 1999 OLAF Regulation already explicitly spelled out that the Office had to comply with data protection rules, and that aspect has naturally not changed, as illustrated by Arts. 1(3)(e) and 10(1), (2) and (4) of the current OLAF Regulation.

In implementing Regulation 2018/1725, the Commission has adopted internal rules[14] concerning the processing of personal data by OLAF in relation to the provision of information to data subjects and the restriction of certain of their rights in accordance with Art. 25 of that Regulation. Those internal rules note in Recital 4 that in order to prevent unlawful access to or transfer of data to persons who do not have a need-to-know, OLAF stores personal data in a secured electronic environment.

Similarly, the OLAF Regulation is essentially silent on the ways in which OLAF can **handle** the data in its possession. Provisions of this kind can more often be found in sectoral legislation, such as the successive amendments of Regulation 515/97 on mutual administrative assistance in customs and agricultural matters.[15] These provisions have evolved substantively over the last 25 years.[16] On that basis, assistance has practically moved from exchanges of letters and then digital communication to the creation of large repositories with transaction level customs data hosted and managed by OLAF. Given the sensitivity of these data,

the legislature has foreseen a number of restrictions as to who can access the data and for what purpose; restrictions that of course also affect OLAF's analytical and operational work.

Interestingly, Art. 2 of Regulation 515/97, as amended, contains relevant definitions of the important terms of "operational analysis" and "strategic analysis": **operational analysis** is understood as:

> the "analysis of operations which constitute, or appear to constitute, breaches of customs or agricultural legislation, involving the following stages in turn: (a) the collection of information, including personal data; (b) evaluation of the reliability of the information source and the information itself; (c) research, methodical presentation and interpretation of links between these items of information or between them and other significant data; (d) the formulation of observations, hypotheses or recommendations directly usable as risk information by the competent authorities and by the Commission to prevent and detect other operations in breach of customs and agricultural legislation and/or to identify with precision the person or businesses implicated in such operations".

By contrast, **strategic analysis** is defined as:

> "research and presentation of the general trends in breaches of customs and agricultural legislation through an evaluation of the threat, scale and impact of certain types of operation in breach of customs and agricultural legislation, with a view to subsequently setting priorities, gaining a better picture of the phenomenon or threat, reorienting action to prevent and detect fraud and reviewing departmental organisation. Only data from which identifying factors have been removed may be used for strategic analysis."

The coordination tools available to the Office provided for by Regulation 515/97 have subsequently been extended to a range of other sectors, such as the enforcement of intellectual property rights[17], export of cultural goods[18], transit of dual-use items[19], trade in drug precursors[20], the supervision of explosives for civil uses[21], manufacturing of and trafficking in firearms[22] as well as the EU's restrictive measures in response to Russia's actions in Ukraine in 2014[23].

But of course, the definitions and conditions for data access and handling set out in Regulation 515/97 only apply within the scope of the aforementioned instruments. By contrast, the current OLAF Regulation contains no equivalent rules. Yet, it is without doubt in relation to the various types of data processing operations that the most important developments have occurred over the last 25 years. OLAF is involved in a constant effort to extract and aggregate data from different sources, its own repositories and external databases, to clean and transform them in terms of format and upload them to data warehouses for processing and intelligence analysis.

When handling or processing personal data, the Office is naturally bound by **data protection** rules.[24] There is no doubt that the processing of investigative data, as long as it relates to the matter under investigation, is in principle necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body, in the sense of Art. 5(1)(a) of Regulation 2018/1725.[25]

The internal 2018 Commission Decision implementing Regulation 2018/1725 mentioned above[26] also sets out the applicable data protection regime in more detail for the specific investigative context. It addresses, for example, such issues as the period during which OLAF may retain investigative data (in principle for 15 years after dismissal or case closure) and the rights of data subjects. It includes transparency obligations and refers to OLAF's dedicated Data Protection Officer.

Within those boundaries, the European courts have accorded OLAF a certain discretion as to which processing operations may be required in the context of an investigation, as can be exemplified by the *Vialto* case relating to a digital forensic acquisition by OLAF.[27] In this case, the appellant had objected to the collection of data by OLAF forensic analysts, which the company considered unrelated to the project in question. At issue was the production of a digital forensic image of certain data on a digital storage medium to enable the data to be indexed. This indexation would in turn enable keyword searches using specific forensic computer software in order to identify the documents relevant for the OLAF investigation. The ECJ confirmed on appeal that the production of such a digital forensic image of all data stored on certain digital media was a legitimate intermediate step in the examination of those data.[28]

c) Progressive digitalisation

Even before the current OLAF Regulation was adopted, the Office had begun its digital transformation, i.e., the integration of digital technology in the practical implementation of the business process, so that the latter could be performed timely, efficiently and effectively. This did not happen overnight; it was a progressive effort to develop information systems, such as case management systems, organise the internal operational processes and manage information.

In these early years of the 21st century's digital revolution, digitalisation of business processes did not follow a holistic approach but, with the benefit of hindsight, appears more like a struggle to respond to fundamental challenges of this period.

- **Digital-first**: It may seem evident today, but 15 to 20 years ago, (re)designing business processes using digital means instead of paper circulation was a change to people's working culture. From today's perspective, the first efforts to apply this principle look almost clumsy, as operational bureaucracy was simply reproduced in digital terms. On the positive side, end users' experience improved, data were easier to collect and process, reporting to management was enhanced in quality, and security and data protection aspects were reinforced. The replacement of the legacy IRENE and Pre-IRENE databases with a new case management system (CMS) was an example of OLAF's shift towards a more digital way of organising document/record management based on electronic workflows, integrated search and increased security. Nevertheless, missing features, such as remote secure access to, effective reporting and digital document signing in the CMS were still to be implemented in the years that followed.

  Probably the ultimate effect of embracing a wider use of digital technologies was the established certainty that "digital is here to stay" and technology will determine the quality and effectiveness of administrative and operational activities of the Office.

- **Governance or "do it your own way"**? In the software development process of this era, known and pressing needs were implemented first, and emerging ones were tackled in subsequent phases. This resulted in information systems resembling digital patches of incoherent modules, difficult to maintain and further evolve. The Office prioritised the flexibility to develop digital applications quickly and within available budget over a coherent approach that would first map all business needs and respond to them in order of priority. This inefficient way of building up information systems was tackled with the adoption of IT development and project management methodologies (Rational Unified Process and PM^2)[29] to ensure a holistic response to automating business needs, resulting in a solid and scalable digital product able to address current and future requirements. Although these methodologies standardised the digital delivery process, they did not solve the issue of scattered IT developments and responsibilities in different units across OLAF. As was standard practice at the time, IT governance and decision-making were decentralised, creating digital silos.

- **Who's in the driving seat, IT or business?** That said, digital initiatives were still driven by IT. OLAF units and their staff involved in core investigative/operational activities, representing the business interest, tended to leave the design of IT systems to the IT experts. Involvement from the business side was limited and mainly at ideation or inception phase. IT project management followed a cascade model; broadly described business requirements were implemented in IT systems based on an incomplete understanding of the IT side for the actual business needs. This was spotted when completed digital end-products were found to only partially incorporate the business logic and outcomes. Escalation to management and internal reviews gave rise to stricter governance, with the business side beginning to assume responsibilities throughout the whole lifecycle of an IT project, from determining the business needs the IT system should address, to periodical evaluation of intermediate IT deliveries and acceptance testing before putting the information system in production mode.

d) Digital transformation in full swing

Over the last ten years, digital technology has exploded into every facet of people's work and private lives. OLAF has been no exception and has reached a mature stage of its own digital transformation journey. To achieve its strategic objectives, OLAF had to: build business capabilities for detecting, preventing, and investigating fraud; support anti-fraud policies by operating trans-European IT systems; collect, manage, and analyse data to produce intelligence; collaborate and exchange with stakeholders; all while ensuring security and trust. At the heart of this entire endeavour have always been data and OLAF's intention to transform itself into a data-driven organisation, i.e., to manage its data assets in such a way as to facilitate or even completely automate decision-making related to investigative activities.

For digital transformation to become a reality, certain digital capabilities should be in place as necessary preconditions or enablers:

- **Digital, data, and security governance:** Governance is the necessary condition for digital initiatives and operations to thrive and survive long term. It should cover, end to end, all types of business categories and their processes, technologies, services, and collected information within the responsibility of OLAF. Governance is organised in tiers to align with different expectations related to decisional power and accountability – starting with the top, where decisions are made on strategic alignment, portfolio prioritisation, policies and critical procedures, resources and risk, and where innovation is steered; to lower levels, which deal with projects, systems, changes, user support, and operations. An equally important function of governance is to set the principles shaping digital work, i.e., digital-by-default for all new business processes, one-stop-shop for access to data, reuse-first when it comes to developing a new information system, security-by-design to ensure that security is considered early in the design of any software application, etc., and to ensure they apply horizontally and establish a homogenous digital landscape across the Office.

- **Modern digital culture and workplace:** The digital transformation of business is doomed if the people who run businesses do not embrace the relevant changes. Considering that change in a work context is often synonymous with disruption, the first to steer change is management, who should mentor and lead by example and communicate to general staff the positive effects of change initiatives via awareness-raising campaigns and training sessions. A digitally-rich environment is also required, well-adapted to the specific requirements of a business, such as security and privacy, mobility, and remote access; this includes corporate and interconnected applications for resources, document, mission, time, financial, procurement management, collaboration with internal and external stakeholders. The cost of such transformation should not be neglected, as technology evolves fast and (especially) equipment is depreciated (financially and technologically) within a few years. The pace of technological transformation should be carefully assessed with view to the return on investment and be kept

proportional to benefits produced. The Office is involved in such a continuous effort, by taking part in relevant corporate Commission IT initiatives and whenever necessary developing local/on-premises digital solutions best suited to its own needs (business or security related).

- **Digital transformation of business processes and data:** In the recent years, OLAF's digital transformation took off. Specifically, this concerned redesigning and streamlining processes within the Office and introducing the technical means to automate as much as possible. An example is the OLAF Case Management (OCM) system, which replaced its predecessor CMS and organises the lifecycle of cases throughout their different phases – i.e., selection, investigation, and monitoring – using features such as fully automated workflows based on manually or automatically generated activities and tasks, certificate-based user authentication, digital document signing and timestamping, remote access, integrated reporting, etc. OCM exports certain datasets to another internal environment (GET Intelligence), which is interconnected with other OLAF and Commission data sources to combine, analyse, and produce intelligence for analysts and investigators.

- **Innovation:** OLAF has long been using cutting-edge digital technologies in areas such as digital forensic examination and operational analysis in its own data and Open Source Intelligence (OSINT) environments. Although OLAF is not a research or technological organisation, whose sole purpose would be to produce innovation, the Office is open to using innovative digital technologies to improve the quality and speed of investigations and maximise impact in the anti-fraud domain. Nowadays, the Office is exploring how to benefit from the most influential example of innovation, Artificial Intelligence (AI), which is expected to influence and accelerate the way certain administrative and investigative tasks are conducted. In pursuit of innovation, a "right to fail" should be accepted, as failures feed future activities in the form of lessons learnt.

III. Looking Ahead, or What Does the Future Hold?

It comes as no surprise that there has been a paradigm shift in the way OLAF works when you compare its digital operations today with the situation 25 years ago, when the Office was first created. Digital processes are now at the core of its activities.

Yet we also need to acknowledge that investigations carried out by the Office can invade the privacy of those investigated. It goes without saying that the Office fully respects the applicable, stringent rules on data protection, and these go a long way towards ensuring an adequate balance between privacy and the effectiveness of investigations. But looking at current digital developments, the question arises whether OLAF's legal framework itself should evolve in lockstep with this digital transformation.

That said, the experience of the last quarter of a century has also shown that several regulatory mechanisms combined are able to largely guarantee an adequate protection of fundamental rights, privacy, and due process:

- Firstly, the legislative framework was relatively modern to start with; the digital era was already on the horizon as the 1999 OLAF Regulation was taking shape. This in mind, the legal text could incorporate certain aspects, even if it is not always very explicit. This is most noticeable in the above-described way that the term "data" was given centre stage as the basis of all of OLAF's digital work.

  Moreover, it is also likely that the 1998 *Tzoanos* judgement[30] that preceded OLAF's establishment by one year had opened the door to the concept of digital forensic operations, probably the most privacy-sensitive OLAF operation of all. The legal language of Art. 4(2) of the 1999 OLAF Regulation, including the use of the term "any data medium", is unusually detailed compared to other provisions and a clear

testimony to the fact that the Union legislature intended to provide a basis for this key digital operation in the new regulation.

- Secondly, as a matter of regulatory technique, there is much to be said in favour of not overregulating technical details at the level of a basic regulation. This could lock in existing technologies and thus hinder the uptake of future innovations. The sections above show through how many digital transformations the Office has gone in the past years. Rather, implementing acts which are at least binding on the administration can often be updated in a more agile manner. The *Guidelines on Investigation Procedures for OLAF Staff*[31], which are regularly updated, and the aforementioned *Guidelines on Digital Forensic Procedures for OLAF Staff* are good examples of this approach.

- Thirdly, the OLAF Regulation naturally does not exist in isolation, but is firmly embedded in the EU's wider regulatory framework. This includes, for the present purposes, in particular Regulation 2018/1725 on data protection, the EPPO Regulation 2017/1939[32], and the AI Act[33]. In many respects, OLAF's digital practices are conditioned by these important legal acts, making it unnecessary for all issues to be separately addressed in the OLAF Regulation.

- Last but not least, jurisprudence from Luxembourg safeguarding the rights of individuals and companies in a large variety of cases will always be a driver for regulatory innovation.

This finding of a broadly adequate overall legal framework applicable to OLAF's digital operations notwithstanding, one can always legitimately ask where there is room for improvement.

The following section contains three examples, all taken from the context of OLAF's ongoing digital transition. They illustrate the need to continuously reflect on the appropriate level of prescriptive detail i Union legislation, in light of the invasive nature of some of OLAF's digital operations, especially to the privacy of natural persons.

1. Processing of cloud-based data by OLAF

First of all, it is clear that increasing amounts of data are no longer stored on a specific device or in a local network environment (work-related or otherwise), but in a cloud configuration hosted and operated by private companies. There are two elements of concern associated with the well-established technological trend of cloud use:

- *OLAF access to data stored in the cloud for investigative purposes:* OLAF Regulations do not include specific provisions for services delivered by and data hosted in the cloud; this means that the cloud is to be considered a typical digital technology, storing data subject to access or acquisition by the Office. The associated challenges are both procedural, i.e., data managed by a third party (cloud provider) who is unrelated to the investigation, but also technical, i.e., special tools needed to get access to and download cloud-based data, bandwidth restrictions, security, etc. A possible approach would be to include cloud-related provisions in revised guidelines (e.g., on digital forensic) and in operational and technical procedures driving investigative work.

- *Use of the cloud for OLAF-operated information systems and data:* The technological shift to the cloud has been widely embraced by the IT of the Commission for applications related to office automation, but also more generally for IT system development, in the latter case by applying the "cloud-first" approach which means that new information systems should be designed in such a way that they can be deployed in the cloud, whereas existing ones should be assessed for technical transformation to the cloud.[34] OLAF might, at some point in time, develop a cloud-specific policy following a careful assessment of its exposure to and potential use of the cloud to benefit from this technology's scalab-

ility, flexibility, and availability whilst minimising risks related to security, vendor lock-in, and limited visibility in data processing.

2. OLAF work on artificial intelligence

Like many other modern administrations, OLAF is also in the process of reflecting on to what extent the potential of new tools based on Large Language Models (LLM)/artificial intelligence could be harnessed to make OLAF's operations more efficient and more effective.[35] These deliberations are of course undertaken in full compliance with the AI Act, applicable data protection rules, and the Charter of Fundamental Rights of the European Union. It is obvious that AI tools will always be limited to a support role in anti-fraud prevention and investigation. The objective of the prudent use of AI by anti-fraud authorities must be to render the decision-making of human anti-fraud investigators more efficient and effective, and never to replace it.

However, from a regulatory perspective, OLAF's administrative investigations are not easy to categorise under the AI Act. *Prima facie*, OLAF's administrative processes cannot be considered "law enforcement" for the purposes of identifying which use of an AI tool has to be considered high-risk.[36] From the point of view of assessing AI-related risks, it seems more adequate to assimilate OLAF's administrative investigations with "administrative proceedings by tax and customs authorities", which are not generally considered high-risk under the AI Act.[37]

3. OLAF access to relevant data

Lastly, the question of how effectively OLAF can protect the financial interests of the Union in the digital era to some extent depends on the access that OLAF has to the right sets of data. But where to find that data depends not least on how spending and the corresponding reporting obligations are organised.

The Recovery and Resilience Facility (RRF) introduced a novel *modus operandi* for Union expenditure, which contributed significantly to the rapid disbursement of funds. In implementing the Facility, the Member States, as beneficiaries or borrowers of funds under the Facility, shall take all the appropriate measures to protect the financial interests of the Union and to ensure that the use of funds in relation to measures supported by the Facility complies with the applicable Union and national law, in particular regarding the prevention, detection, and correction of fraud, corruption, and conflicts of interests. To this effect, the Member States shall provide an effective and efficient internal control system and the recovery of amounts wrongly paid or incorrectly used. Member States may rely on their regular national budget management systems.[38]

From a data perspective, the hybrid control approach taken in the RRF poses challenges in terms of data availability. Each Member State has put their own reporting mechanisms in place to meet the RRF requirements. These fragmented data structures inevitably do not make it easier for the Office to investigate any irregularities, raising the question of how this could be remedied.

IV. Conclusions

OLAF's digital journey over the past quarter of a century was marked by the need to align its legislative and operational configuration with the rapid technological advancement of the digital landscape. As a result, that period witnessed a shift of paradigm towards the today well-established data-driven and digital-first principles.

As the digital revolution is still in full swing, especially with the advent of artificial intelligence, there is a strong case to maintain an overall regulatory approach where references in OLAF legislation to data access/

handling remain high-level. Likewise, legislation should include provisions on digital aspects in a technologically neutral manner; specificities related to digital tools and processes should be formalised separately to allow for changes following the dynamic nature of information technology. Personal data protection matters are adequately addressed by the applicable general legislation. Operational/business related processes should be subject to working arrangements with the stakeholders or internal operational procedures. Overall, this carefully balanced approach has proven to be an efficient and flexible way to deliver OLAF's core businesses and to innovate, whilst adequately protecting fundamental rights and privacy.

We should also acknowledge that advancements in technology have a direct impact on the effectiveness of OLAF's operations. Fraudsters are making wide use of the latest technology to commit fraud smarter and faster, covering up their tracks. OLAF should not only technologically follow and be efficient and effective in detection and evidence production; especially when it comes to prevention we should be technologically mature to analyse relevant big amounts of data and produce intelligence which would allow, as appropriate, OLAF, the other European anti-fraud actors or the active national anti-fraud authorities to take up action as early as possible.

Unfortunately, technology has a cost, especially when it serves extraordinary forensic and analysis needs delivered under strict security requirements for the sensitive data OLAF manages. In the view of the authors, necessary financial provisions should be made to ensure a sound technological environment. Similarly, OLAF like many other anti-fraud authorities will have to continue invest to digitally educate staff members on how to lawfully reap all possible benefits technology can bring to their professional mission.

Last but not least, we are witnessing the – inevitable and important – arrival of self-thinking software and machines such as AI in support (but never in control) of anti-fraud activities. We need to acknowledge that these are not only offering a powerful support, but also come with risks. The use of state-of-the-art technologies, especially AI, within OLAF's digital ecosystem, should be subject to scrutiny and assessment for compliance with the relevant legislation and organisation's policies.

---

1. Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ L 136, 31.5.1999, 1.↩
2. Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248, 18.9.2013, 1.↩
3. Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, OJ L 437, 28.12.2020, 49.↩
4. *AG Jacobs*, Opinion of 3 October 2002 in Case C-15/00 *Commission vs. EIB*, at para. 159.↩
5. Emphasis added.↩
6. Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, 2.↩
7. See on this point also ECJ, judgment of 28 October 2021 in Case C-650/19 P, *Vialto*, para. 70.↩
8. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, of 21.11.2018, p. 39.↩
9. Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-fraud Office (OLAF), OJ L 136, 31.5.1999, 22.↩
10. See the example in the judgment of the Court of First Instance of 19 March 1998 in Case T-74/96, *Georges Tzoanos v Commission of the European Communities*, paras. 319-322, relating to facts arising prior to the adoption of the 1999 OLAF Regulation.↩
11. The Guidelines are available at: <https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?file-name=guidelines_en_bb84583638.pdf> accessed 7 February 2025.↩
12. ECJ, *Vialto*, *op. cit.* (n. 7), paras. 70-74.↩
13. GC, 20.5.2021, Case T-482/20, *LG and Others v Commission*, paras. 51-62.↩
14. See Commission Decision 2018/1962 of 11 December 2018, OJ L 315, 12.12.2018, p. 41.↩
15. Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, OJ L 82, 22.3.1997, 1.↩
16. See *E. Porebska*, "Paving the Way for Improved Mutual Assistance in the Context of Customs Fraud", (2016) eucrim, pp. 52-55.↩

17. Art. 36 of Regulation 608/2013 of 12 June 2013 concerning customs enforcement of intellectual property rights, OJ L 181, 29.6.2013, 15.↩
18. Art. 6 of Regulation 116/2009 of 18 December 2008 on export of cultural goods, OJ L 39, 10.2.2009, 1.↩
19. Art. 19 of Regulation 428/2009 of 5 May 2009 on setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, OJ L 134, 29.5.2009, 1.↩
20. Art. 11 of Regulation (EC) No 273/2004 of 11 February 2004 on drug precursors as amended by Regulation 1258/2013, OJ L 41, 18.2.2004, 1, and Art. 27 of Council Regulation (EC) No 111/2005 of 22 December 2004 laying down rules for the monitoring of trade between the Community and third countries in drug precursors as amended by Regulation 1259/2013, OJ L 22, 21.1.2005, 1.↩
21. Art. 14 of Directive 2014/28/EU of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses, OJ L 96, 29.3.2014, 1.↩
22. Arts. 19-20 of Regulation 258/2012 of 14 March 2012 on Implementing Article 10 of the UN Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, OJ L 94, 30.3.2010, 1.↩
23. Art. 3 of Regulation 833/2014 of 31 July 2014 on restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 229, 31.7.2014, 1.↩
24. For an overview of the applicable data protection rules, see <https://anti-fraud.ec.europa.eu/olaf-and-you/data-protection_en#:~:text=OLAF%20maintains%20an%20independent%20register,conditions%20of%20the%20processing%20operations> accessed 7 February 2025.↩
25. See also in this sense the judgement of the General Court of 20 July 2016 in Case T-483/13 *Athanassios Oikonomopoulos v European Commission*, para. 60.↩
26. *Op. cit.* (n. 14).↩
27. GC, 26 June 2019, Case T-617/17, *Vialto*, para. 68; ECJ, 28 October 2021, Case C-650/19 P, *Vialto*, paras. 65-75.↩
28. In this context, the ECJ also made an analogy to anti-trust investigations and referred to its judgment of 16 July 2020 in Case C-606/18 P, *Nexans France*, para. 63.↩
29. See European Commission, "PM² Methodologies", <https://pm2.europa.eu/index_en>Project Management Methodology>, accessed 7 February 2025.↩
30. *Op. cit.* (n. 10).↩
31. The Guidelines are available at: <https://anti-fraud.ec.europa.eu/document/download/3dc10699-df07-4782-ae0d-232cd698286c_en?filename=gip_2021_en.pdf> accessed 7 February 2025.↩
32. Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, 1.↩
33. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 2025/1689, 12.7.2024.↩
34. This approach calls for any new or upgraded information systems to be cloud-native, i.e., to have the potential of being easily put in the (private or public) cloud.↩
35. For a more detailed discussion of the use of AI-based tools by anti-fraud investigations see G. *Roebling and B. Necula*, "Reflections on Introducing Artificial Intelligence Tools in Support of Anti-Fraud", (2024) eucrim, 206-214.↩
36. See section 6 of Annex III of the AI Act, *op. cit.* (n. 33).↩
37. See in particular Recital 59 AI Act; similarly Recital 42 as concerns prohibitions.↩
38. Art. 22(1) of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, OJ L 82, 18.2.2021, 17, as amended.↩

* Authors statement

This article only reflects the authors' personal opinions and cannot be attributed to the Institution that employs them.

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union