

Internal Investigations “à la Française”

In France, an internal investigation can introduce an array of key challenges for in-house and outside counsel who will need forensic technology experts to navigate new data challenges and ensure their internal investigation obligations are aligned with new guidelines released by the France National Bar Council (CNB).

“An internal investigation can introduce an array of challenges for in-house and outside counsel”

“A threat to the democratic pact and harmful to the proper functioning of the economy.” These are words the French Anti-Corruption Agency (AFA) has used to describe the impact of corruption on Europe and the global economy. Issued with the enactment of the Sapin II law, France’s position on corruption—and its government’s intentions to ramp anti-corruption efforts—has aligned with that of the U.S., United Kingdom and other leaders on the global stage.

In the years since Sapin II was formalised into law, businesses in France have begun to implement corruption prevention programmes and the whistleblowing mechanisms required of companies that fall under the law’s jurisdiction. Similar to the U.S. Department of Justice and Yates Memo guidelines, one of the key aspects of these corruption prevention efforts is the implementation of internal investigations. This is a relatively new concept for French corporations and has spurred significant legal and cultural shifts in how corporations and the government address corruption.

In June 2020, the France National Bar Council (CNB) issued guidelines¹ to help lawyers understand the ethical, practical and defensibility standards for internal investigations. These built upon earlier guidelines issued by the AFA and the National Financial Prosecution Office (PNF)² in 2019, which outlined the

¹ https://www.cnb.avocat.fr/sites/default/files/cnb_guide_the_french_lawyer_and_internal_investigations.pdf

² [https://www.agence-francaise-anticorruption.gouv.fr/files/files/EN_Lignes_directrices_CJIP_revAFA%20Final%20\(002\).pdf](https://www.agence-francaise-anticorruption.gouv.fr/files/files/EN_Lignes_directrices_CJIP_revAFA%20Final%20(002).pdf)

“Forensic technology experts are often needed to prepare and perform the investigation”

implementation of the judicial agreement in the public interest (CJIP), or the “French DPA,” and the requirement that any company seeking to enter into a CJIP conduct an internal investigation.

Notable in the CNB’s standards is the recommendation that companies use a “forensic service provider than can host all the data in France and enable a review of the information and documents that match the request made by the foreign authorities in France.” Document redaction is also mentioned as an important measure to preserve data protection and confidentiality for employees and third parties who are not directly targeted by the investigation or whose written authorisation is difficult to obtain.

A Challenging Landscape

In any jurisdiction, an internal investigation can introduce an array of challenges for in-house and outside counsel. They are often high-stakes, highly sensitive data collection and review matters involving massive volumes of documents and tight turnaround times. In France, lawyers may face additional unique difficulties and must now follow the new CNB guidelines. Below is an overview of the key challenges that may arise in an internal investigation driven by a CJIP.

- **Cultural barriers:** The intensity and depth of an internal investigation is a big shift in thinking for French organisations and lawyers. While this type of probe is widely considered a regular cost of doing business in common law countries like the U.S or the UK., it is not in the French legal system. Self-investigation and self-reporting are not part of the French culture and judicial system, and therefore successfully tackling such a task will be an uphill battle for many.
- **GDPR and privacy:** Simultaneously fulfilling discovery obligations for an internal investigation and complying with data privacy law will require special care. Companies/data custodians, and potentially the French data protection watchdog, may ask for detailed information regarding what data will be collected, where it will be stored, for how long, who’s going to access it, what security measures will be taken, how private information will be excluded and how data will be deleted after the investigation. Pre-filtering steps to identify and exclude private information from the review set, sometimes at a very early stage, has become the norm. Involvement of a bailiff to oversee certain steps in anticipation of potential claims from data custodians may provide some additional guarantee that no private information was illegitimately accessed.
- **Cross-Border Considerations:** The French Blocking Statute, which was originally defined to prevent sensitive data belonging to French organisations from being transferred abroad in response to a U.S. e-discovery proceeding, may have implications for internal investigations that develop into self-reporting to foreign authorities. The 2019 Gauvain Report from French MP Raphael Gauvain, asserted that the French Blocking Statute should be strengthened and reinforced. If that happens, the result would need to be seriously taken into consideration when contemplating data disclosure to foreign authorities. Counsel must understand the French Blocking Statute’s existing framework, and impending changes, to ensure any document review strategies and document production formats used in internal investigations are compliant now and in the future. To stay on the safe side, teams must ensure data is processed, hosted and reviewed in-country to narrow down the data set by excluding out irrelevant documents and redacting sensitive information as required before any international transfer may occur.
- **Technology Complexities:** Possibly the most glaring barrier for French legal teams performing internal investigations is technology. Because internal investigations have not been a commonplace occurrence in the region, most companies do not have the proper processes and tools in place for dealing with them. Technology is essential for streamlining the work of mapping relevant information sources, tracking legacy data, executing legal holds and making data available (in a decrypted format) for the investigation. Even among companies where the processes and technology exist, there’s often a gap between the information technology team and the legal/compliance teams leading the investigation. As organisations undertake internal investigations, they will need to establish clear lines of communication, coordinate between various teams and ensure everyone understands and agrees with the data workflow.

The Role of Forensic Technology Experts

Given the large volume of electronically stored information (ESI) at stake in an internal investigation, forensic technology experts are often needed to prepare and perform the investigation alongside outside counsel. The importance of forensic expertise has been emphasised by the CNB. Collecting data from the company servers and employee devices and processing and uploading data into an e-discovery platform so data can be organised, searched and tagged efficiently is a nuanced process that requires a degree of expertise to maintain chain of custody and ensure defensibility of the investigation’s findings.

Counsel facing current or impending internal investigations should consider the following areas where digital forensic expertise may be needed:

- Educating the various stakeholders on what an internal investigation may involve from a data standpoint;
- Defining the scope of the investigation by identifying potentially relevant data sources;
- Ensuring data are preserved and gathered in a forensically-sound, independent and defensible manner and handled securely throughout the investigation;
- Planning for document review resources;
- Translating a legal strategy into technical steps that follow best practice data collection approaches and data filtering and searching techniques;
- Holistically addressing unstructured data as well as structured data such as financial transaction records and accounting information to help understand the full picture;

- Verifying that searches are thorough and conducted using full indexing and advanced searching technology, including across deleted data;
- Defensibly and strategically applying advanced analytics and predictive coding approaches such as the continuous active learning (CAL) methodology to speed up the review process and keep costs under control;
- Leveraging technology to apply data filtering as required and remove or redact sensitive information subject to protection under GDPR and the French Blocking Statute.

Conclusion

The French civil law system is moving toward similar approaches used in the U.S.’s common law system. Digital forensics investigation is not a new practice area, and forensic technologies and approaches have been extensively relied on in common law countries to ensure facts are properly investigated while mitigating data risks and keeping costs under control. Counsel will need a strong combination of global experience and local expertise to navigate new data challenges and ensure their internal investigation obligations are aligned with new guidelines and fulfilled in a timely, defensible and cost-effective manner.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

THOMAS SELY

FTI Consulting Paris
 Managing Director
 +33 (0)1 47 03 68 12
 thomas.sely@fticonsulting.com