Execution of search and seizure warrants in criminal matters in respect of electronic data held by persons bound by professional secrecy rules

Professionals of the financial sector in Luxembourg have, in the past, regularly been confronted with search and seizure warrants (*ordonnance de perquisition et de saisie*) in respect of electronic data held on the professional's computer servers which is potentially related to criminal matters under investigation.

For reasons mainly of expediency and efficiency, the investing magistrate and the police have on occasions tended not only to seize the data effectively useful for the ongoing criminal investigation, but to have a copy made of the whole (or a large part) of the professional's electronic database in order to be able to extract from such database the information sought at the premises and with the computer resources available to the police. Data not required for the purpose of the criminal investigation is thereafter supposed to be deleted.

It is clear that, whilst certainly facilitating and speeding up criminal investigations, such measures are not only questionable from the perspective of criminal procedural rules, but also raise serious concerns from a professional secrecy point of view.

In this context, a landmark decision was rendered on 2 April 2014 by the council chamber (*chambre du conseil*) of the Luxembourg District Court quashing the warrant issued by an investigating magistrate to seize (*i.e.* to copy) the entire database of a law firm in the context of a criminal investigation relating to a client of the firm for the purpose of mining such database for any information pertaining to the matters under investigation.

It must be said that this decision was rendered in a somewhat specific context insofar as it relates to data seized from a law firm where, in addition to ordinary professional secrecy rules, more specific protection of client data applies, such as the client-attorney privilege, in particular in criminal matters pursuant to which clients' files relating to ongoing criminal cases can under no circumstances be seized by the judicial authorities.

However, the general principles that can be derived from the council chamber's decision should in our view also apply to electronic data held by persons other than lawyers, such as professionals of the financial sector, where such data is subject to professional secrecy rules. Such principles can roughly be summarised as follows:

- While the investigating magistrate has, in principle, the authority to order any investigative measures he deems useful to ascertain the truth as to the subject matter of an ongoing criminal investigation, when seizing data potentially subject to professional secrecy rules, be it in paper or electronic form, such investigating magistrate must, pursuant to Articles 33 and 65(4) of the Code of criminal procedure, take all necessary measures to protect such professional secrecy, which means that he must take all necessary steps to ensure that the data seized is limited to data which is relevant for the ongoing criminal investigation.

- The seizure of an entire database, in situations where it is clear from the start that the majority of the information contained in such database is of no relevance for the ongoing criminal investigation, cannot be justified for reasons of expediency, efficiency or other practical reasons, but the seizure must be limited to such data which is specifically identified in the search and seizure warrant, as it is the case for documents in paper form. This is all the more the case in situations where such steps cannot be justified by exceptional circumstances or a particular urgency. Thus, the investigating magistrate and the delegated officer of the police must select the documents and the data to be seized at the premises where the search is made, even where such documents and data are in electronic form.

- In the same manner as for tangible assets such as documents seized in paper form, an inventory must be established of the documents and data seized in electronic form and the report produced on such search and seizure must show that this requirement has been met. In case an inventory cannot be established immediately, the documents and data seized must be sealed until such inventory can be made. A failure to establish such an inventory constitutes a breach of the rights of defence of the persons involved.

This decision should effectively put an end to the highly questionable practice of the seizing and copying of the entire contents of computer servers held by persons bound by professional secrecy rules, although it remains to be seen how the principles derived from the council chamber's decision will effectively be put in practice in the future

In any event, and in particular following this decision, persons bound by professional secrecy rules, in case of an attempt by the police to seize their entire database, should formally contest the legality of such seizure and ensure that such challenge is duly recorded in the report produced on the search and seizure, in order to avoid the risk of breaching professional secrecy rules.

For further information please contact:

Ari Gudmannsson
Dispute Resolution
Of Counsel
Tel: +352 40 78 78 223
ari.gudmannsson@arendt.com