CERHA HEMPEL
CEE NEWSLETTER
Czech Republic

DAWN RAID THREATS IN THE DIGITAL ERA

Every year, digital technologies play a greater and more significant role in how businesses interact with one another. Nowadays, most business processes have more or less been digitalised. Paper documents and archives are being replaced by emails and electronic data storage solutions. Using modern technologies to process digital data offers a substantial increase in efficiency and accessibility to data and information on the one hand and such use of technology radically reduces the time needed to obtain data on the other. Operating in a digital environment has become indispensable in order to keep pace with the ever-accelerating exchange of information affecting the way business is conducted today. Digitalisation, however, in spite of its many undeniable advantages, brings a number of risks, which may at first go unseen.

One of the situations where the digital environment of the company, if handled and organised improperly, might prove to be very harmful includes on-site inspections conducted by competition authorities searching for evidence otherwise inaccessible, so-called dawn raids.

Due to technological progress, searching for digital evidence has now become an integral part of every dawn raid and the inspecting authorities have been quick to adapt to this development. As massive amounts of electronic information are exchanged daily via email accounts, smartphones, social networks, and other means of communication, and because such information is often stored for a long period of time at several locations (on in-house servers, cloud services, etc.), the digital form of the information can make what is already an unpleasant intervention even riskier for the undertaking being inspected.

Below we set out the main disadvantages posed by digital environments with respect to dawn raids conducted by competition authorities.

Volume of accessible data

The power to conduct a dawn raid is usually based on the essential right of the inspecting authority to investigate business records which are on or accessible from the business premises regardless of their form.

Since storing digital data, unlike hardcopy documents, is rather effortless, business IT systems usually contain large volumes of machine-readable structured data which will all become accessible to the authority irrespective of whether it is located on the company's servers or stored on cloud services physically present outside the inspected premises.

Therefore, the volume of electronic data and its structure may significantly broaden the potential source of evidence the inspection authority will gain access to when compared to hardcopy documents. Even though the authority is still bound by the scope of inspection and thus cannot examine documents without any relevance to this scope, the risk of discovery of incidental evidence in the course of the inspection is much higher.

Electronic data is easier to search

As stated above, the machine-readability of digital data makes the entire search by the authority more efficient. Special search systems used by the authorities may give more comprehensive search results when compared to scanning

through single hardcopy documents. The system will tag all documents containing the key words used by the authority to search the extensive quantity of information. The tagged documents may be closely investigated by the inspectors afterwards. Given the limited duration of on-site inspections, the authorities can never go through as many hardcopy documents as they can digital data.

Beware of metadata

Unlike physical documents in hardcopy form, information valuable for the inspecting authority is not limited to the content of the document alone, but, in the case of digital data, it also relates to information such as the document's origin, author, time of creation and alteration or who accessed the document. Such information may also be part of the document in the form of metadata, *i.e.* data providing information about other data.

Less control over electronic data

The digital environment presents the opportunity to share documents easily via digital mediums and messaging apps. More copies of respective documents may be made in this way and even if a document on one digital medium is destroyed permanently, it can be present on other digital media or leave some traces of its existence detectable by special forensic software used by the authorities. In addition, even if the only existing copy of the respective digital document by a standard procedure is deleted, it may still be recovered by special software; something that cannot be done with hardcopy documents once destroyed.

Fishing expedition

Based on the reasons above, digital environments may seem unequivocally advantageous to the benefit of the inspectors. However, the authorities are facing challenges connected to digital data searches as well. It is disputed almost every time by the undertaking that evidence discovered by chance during the search is the result of a "fishing expedition", which is a practice generally prohibited for lack of reasonable suspicion justifying the raid in the first place.

However, the courts in the Czech Republic recently ruled that if the competition authority accidentally discovers evidence of a different violation of competition law during the dawn raid, it is entitled to seize such documents and use them as evidence. These new court decisions are not favourable for an undertaking that is the subject of a dawn raid as it makes it more difficult to dispute the new evidence by claiming it was the result of a fishing expedition.

IT systems complexity

A significant number of companies use modern and complex IT systems. These systems require trained staff, expertise and equipment, and these are services which a not insignificant number of companies outsource to a third party service provider. With respect to dawn raids, it is essential for the undertakings to understand that it is their obligation to provide the authorities with assistance and access to their IT system. Therefore, the presence of trained staff is necessary during the inspection. If such staff are not available (e.g. because the contractor of outsourced IT services is unavailable), the authority may claim that the undertaking is demonstrating its unwillingness to cooperate and impose a huge fine.

In light of the above, it is evident that the establishment of proper rules for data management, including the creation of a data map, routine document destruction, rules for employees, etc., are a key factor for the success of every competition compliance programme.

Authors

Mgr. David Kučera and Mgr. Michal Horký

For more information

JUDr. Petr Kališ, Ph.D.
Managing Partner Czech Republic
petr.kalis@cerhahempel.cz
Tel: +420 221 111 711

Media owner and publisher: **CERHA HEMPEL Rechtsanwälte GmbH**, Parkring 2, A-1010 Vienna | Tel: +43 1 514 350 Fax: +43 1 514 35 35 | email: office@cerhahempel.com | Although this newsletter was created with the greatest of care, we nevertheless do not accept any responsibility whatsoever for its content being correct, complete or up to date **| Visit us at www.cerhahempel.com |**
CERHA HEMPEL Austria Belarus Bulgaria Czech Republic Hungary Romania Slovak Republic