Dawn raids in Poland – tighter rules on the gathering of electronic evidence

Kluwer Competition Law Blog
October 19, 2017

Piotr Skurzyński, Maciej Gac (Hogan Lovells)

Please refer to this post as: Piotr Skurzyński, Maciej Gac, 'Dawn raids in Poland – tighter rules on the gathering of electronic evidence', Kluwer Competition Law Blog, October 19 2017, http://competitionlawblog.kluwercompetitionlaw.com/2017/10/19/dawn-raids-poland-tighter-rules-gathering-electronic-evidence/

On March 7, 2017, the Polish Court of Competition and Consumer Protection, the ("**CCCP**"), issued an important judgment regarding the powers of the Polish Competition Authority, the ("**PCA**"), to search IT systems and hardware (e-mails and hard disks) during dawn raids (the Order of the CCCP of 7 March 2017, XVII Amz 15/17). This judgment significantly changes the landscape for antitrust inspections in Poland by limiting the excessive use of the PCA's investigative powers. It also confirms the need for the protection of legal professional privilege ("**LPP**") within antitrust inspections, and creates the grounds for further debate on its possible scope.

According to the provisions of the Polish Act on Competition and Consumer Protection, the ("**ACCP**"), the PCA enjoys similar powers to conduct inspections and obtain evidence of antitrust violations as stipulated under EU law. However, as recent PCA practice showed, the ACCP's provisions on antitrust inspections were broadly interpreted as far as the collection of electronic evidence was concerned. These provisions were regarded as empowering the PCA, not only to review IT systems and hardware at the premises of the inspected undertaking, but also to copy entire data carriers and/or e-mails found at the place of inspection (without its previous selection) with a view of their subsequent search at the premises of the PCA. In many cases the PCA obligated the undertakings subject to the inspection not only to provide the specific data covered by the scope of the inspection, but also to disclose any e-mails and/or hardware containing information which could potentially exceed it. The PCA regarded a failure to do so as a refusal to submit to the inspection, or as an act of obstruction, and this often resulted in severe financial penalties. For instance, in the *Polkomtel* case in 2011, the refusal by the undertaking to disclose a hard disk containing the entire e-mail correspondence of a number of its employees for the purpose of its subsequent analysis by the PCA within its premises, was regarded as an act of obstruction of the inspection. This, as well as other acts of obstruction, resulted in a financial penalty of 33 million EUR imposed on *Polkomtel*.

The above practice was criticized by various scholars and legal practitioners. It was considered as the PCA's abuse of their inspection powers, resulting in the limitation of the right of defence, as well as the right to the privacy of the undertakings subject to the antitrust inspection. Even though the courts often decrease the amount of the fines imposed in these cases, they have never contested the PCA's approach with regard to searching electronic evidence.

The PCA's practice was also different from the European Commission's approach to the collection of electronic evidence. When it comes to dawn raids conducted by the European Commission, if the selection of documents relevant for the investigation is not yet finished at the envisaged end of the on-site inspection at the undertaking's premises, the copy of the data set still to be searched may be sealed and collected to continue the inspection at a later time. However, if the Commission wants to continue the inspection in its own premises, it shall invite the undertaking to be present when the sealed envelope is opened and during the continued inspection process. Otherwise, the Commission is obliged to return the sealed envelope to the undertaking without opening it or to ask the undertaking to keep the sealed envelope in a safe place to allow the Commission to continue the search process at the premises of the undertaking in the course of a further announced visit.

The recent groundbreaking judgment issued by the CCCP overrules the PCA's previous practice applied, among others, in *Polkomtel* case. Even though the CCCP did not contest the PCA's general right to request access to electronic evidence, the method of its execution has been limited by the CCCP.

During the inspection assessed by the CCCP in its judgment, the PCA's employees made copies of three hard disks belonging to the company's CEO, as well as the entire e-mail correspondence of the company's CFO. Before being copied, the data (hard disks and e-mails) was neither analysed, nor selected by the inspectors. The copies were sealed and taken to the premises of the PCA with a view to their further analysis. The company lodged a complaint to the CCCP claiming that by copying such a large quantity of information, without its previous selection at the company's premises, the PCA: exceeded the scope of the inspection, obtained access to information covered under the LPP, violated the company's right to a defence and privacy, and violated the prohibition to conduct a search outside the premises of undertaking without its previous consent. As a result of the company's complaint, the questioned data was sealed and prevented from search until a judgment was issued by the CCCP.

Although due to procedural reasons, the CCCP eventually rejected the complaint, in the grounds of the judgement it analysed, in detail, the PCA's practice concerning the complete copying of the hard disks (without its prior selection) for the purpose of its further analysis at the PCA's premises.

Firstly, the CCCP underlined that the PCA's right of inspection was an important limitation to the individual's right to privacy and, as such, should be interpreted narrowly. Otherwise, as the CCCP claimed, the existing guarantees of the right to privacy would have had only an "*illusory character*." Based on this approach, the CCCP maintained that the provisions of the ACCP, granting the PCA the right to request information during an inspection, had to be understood as obligating the PCA to strictly select and request only that information which fell within the scope of the inspection. Similarly, while making copies of the information/documents, the PCA had to limit itself only to that which was relevant for the purpose and scope of the inspection. In the opinion of the CCCP, there should have been no difference in the PCA's approach depending on the information carrier, i.e. electronic, or paper, since, in both scenarios, the PCA was able to select only that content which might have been relevant for the case.

Secondly, as the CCCP pointed out, in order to ensure the appropriate protection of an undertaking's right of defence, and its right to privacy, the selection of information had to be conducted at the undertaking's premises and in the presence of its representative. Otherwise, the inspection itself, understood as the selection of evidence, making copies of documents and preparing notes, would have had to be conducted outside the premises of the undertaking which would have been contrary to the provisions of the ACCP. In the opinion of the CCCP, the analysis of hard disks and e-mails construed an inspection in itself (at the moment the PCA was confronted with evidence) and could not have been regarded as a mere technical activity; therefore, performing it in the absence of the inspected undertaking would have undermined its right of defence.

The above approach of the CCCP to the question of the scope of an inspection and the position of the inspected undertaking seems to draw a clear line between those inspections allowed under the ACCP, and prohibited "fishing expeditions". By obligating the PCA to select evidence at the premises of the undertaking, and copy only that information which was relevant to the case, the CCCP has limited the possible abuse of the PCA's right to inspection. Moreover, the CCCP emphasized the need for the protection of undertakings which were the subject of the inspection, and confirmed that a right of defence should not be a dead letter, but had to be manifested at each stage of any antitrust proceedings.

Apart from setting the limits for the PCA's collection and analysis of electronic evidence, the CCCP also referred to the issue of the LPP. The CCCP confirmed that the LPP required protection during antitrust inspections and would be put at risk if certain data were to be collected (e.g. hard disks, e-mail correspondence) without its previous selection at the premises of the inspected undertaking. Moreover, the CCCP held that the legal basis for the protection of the LPP should be the one set out within the Code of Criminal Procedure. Even though the CCCP did not elaborate on the scope of the LPP (in particular, whether it should be limited to correspondence with an external attorney, or whether it should also cover communication with the company's internal lawyer), it provided the grounds for further debate on this issue in Poland. This is because, as various Polish scholars underline, the current construction of the LPP in Polish antitrust law, i.e. the absence of any specific provisions on the LPP in the ACCP, and the need to apply provisions of the Code of Criminal Procedure correspondingly, could lead to a situation in which the scope of the LPP under Polish law would be broader than in EU law. This would result from the fact that the Code of Criminal Procedure does not make a distinction between external and internal lawyer communication for the purpose of the LPP; therefore, it can theoretically cover both external and internal legal advice.

The analysed judgment is a turning point in inspections conducted by the PCA. It clearly states that the PCA's current practice, according to which electronic data was copied without prior selection and taken from the premises of the inspected undertaking for further analysis in the PCA's premises, is no longer permissible. Moreover, the appropriate protection of the LPP also requires the selection of electronic data at the undertaking's premises before the data carriers, which can potentially contain information covered by the LPP, are copied and taken by the PCA. Finally, according to the analysed ruling, it cannot be excluded that the scope of information covered by the LPP would be broader under Polish law than under EU law. Even though the CCCP does not give an answer to this issue, its reference to the provisions of the Code of Penal Procedure in order to assess the LPP creates the grounds for a broader interpretation of the LPP's scope in Poland.