Concurrences
Antitrust Publications & Events

HERBERT SMITH FREEHILLS

CARTELS WORKSHOP :
AN ADVANCED SEMINAR ON SUBSTANTIVE AND PROCEDURAL EU DEVELOPMENTS

2nd Cartels Workshop: An advanced seminar on substantive and procedural EU developments

Workshop II - Procedural Issues, Thursday 21 January 2021

Interview with Aymeric de Moncuit (CJEU)

*by Daniel Vowden (Herbert Smith Freehills)**

***Aymeric de Moncuit** (Référendaire, CJEU) has been interviewed by **Daniel Vowden** (Partner, Herbert Smith Freehills) in anticipation of the **2nd Cartels Workshop**, to be held online with a series of 2 webinars on Wednesday, January 20th and Thursday, January 21st.*

Registrations & Program here

** The views and opinions expressed in this document do not necessarily represent those of the speakers' institution or clients.*

Daniel Vowden: **The General Court provided important guidance in 2020 on the powers of the Commission to conduct dawn raids. While in principle these powers are not unlimited, in practice they are exceedingly broad. Are they too broad? Do you believe that the evidential threshold the European Commission must satisfy to conduct a dawn raid has been set at an appropriate level?**

Aymeric de Moncuit: I would make three points in response to this.

Firstly, it is true that the powers of the Commission to conduct dawn raids, while not unlimited, as they are strictly circumscribed in Article 20(2) of Regulation 1/2003, are broad in their content. The Court recalled recently in *Prysmian* (C-601/18) that such powers did not have to be interpreted narrowly (para. 58). In practice, the powers of the Commission to collect data and review documents have evolved considerably with the use of Nuix, the forensic search tool used by DG COMP. As far as I understand the functioning of this tool, all the evidence collected is indexed in its system irrespective of its relevance to the investigation or of the presence of privileged documents. The review on the basis of keywords and in the presence of the response team only takes place at a subsequent stage, at the Commission or at the company's premises. In *Nexans*, the Court accepted that Regulation 1/2003 does not impose an obligation to carry out a prior examination of the documents copied to ensure that they fall within the scope of the inspection decision (paras 56 and 64) and confirmed the legality of the seizures carried out by Nuix.

Secondly, are these powers too broad? I would say that they are not. However, this does not mean that these powers cannot be exercised too broadly by the Commission while conducting an inspection. During the entirety of the inspection, the Commission must make sure that it does not exceed the subject matter and purpose of the inspection. As held by the Court, in *Dow Chemical* (97/87), the decision authorizing the inspection has to "clearly indicate the presumed facts which it intends to investigate" (para. 45). In practice, this means that the Commission must state what it is looking for and that it cannot gather evidence that does not relate in one way or another to the subject matter and purpose of the infringement referred to in the decision. The inspection is possible "only for those documents coming within the scope of [its] subject-matter" (Deutsche Bahn, C‑583/13, para. 60 et seq.). In this latter case, the Court pointed out that the Commission cannot go on "fishing expeditions".

Thirdly and lastly, has the evidential threshold the European Commission must satisfy to conduct a dawn raid been set at an appropriate level? Allow me to address this question separately, as I understand it does not directly relate to the "powers" of the Commission but to its "competence" (construed in a very broad sense) to adopt an inspection decision. In this respect, it must be noted that the Court's control on whether the evidence in possession of the Commission was sufficient to be the ground for an inspection is very strict. For instance, in *Nexans* (T-135/09), the General Court held that even if he Commission had grounds to suspect an infringement relating to high-voltage underwater and underground electrical cables, it did not have sufficient grounds for ordering an inspection covering all electrical cables (paras 93 and 94). In *České dráhy* (T-325/16), the General Court annulled the Commission decision in so far as it concerned routes other than the Prague-Ostrava route and conduct other than the alleged predatory pricing practices. More recently, in the *Intermarché/Casino* case (T-255/17), the General Court held that the evidence put forward by

the Commission was not sufficient to suspect an exchange of information between Intermarché and Casino during a public meeting. In this case, it is worth noting that the General Court asked the Commission, by way of measures of organization of procedure, to produce all the indicia used as a basis for adopting the inspection decision and carried out a thorough review of each one. So, even if, as recalled in *Intermarché/Casino* (paras 189-190), the Commission only has to produce "indicia" and not proper "evidence" to justify an inspection, the General Court is very vigilant as regards the probative value of these indicia.

Do parties subject to an unannounced inspection have access to sufficient judicial remedies to protect their fundamental rights?

The European legal system is somewhat singular in that it does not contain a specific judicial remedy to contest the "conduct" of an inspection in itself, while such a remedy has been incorporated in several Member States' legal systems (including France), in line with an increasingly protective jurisprudence from the European Court of Human Rights. In practice, judicial reviews of the conduct of inspections are carried out in the context of actions for annulment against the final sanction decision adopted by the Commission. However, judgments concerning those final decisions are generally rendered several years after the inspection.

Admittedly, this may be thought of as regrettable given that the EU legal system is generally more protective of defence rights than Member States' legal systems. Generally, parties go before the Court to argue their national legal system does not offer the guarantees entrenched in EU primary law, not the reverse. However, I would not say that the provisions of Regulation 1/2003 governing the conduct of inspections do not comply with EU fundamental rights and notably the right to an effective remedy (Article 47 of the Charter). This question came up recently in the *Intermarché/Casino* case: the parties raised, under Article 277 of the TFEU, a plea of illegality against Article 20(4) of Regulation 1/2003, in that this article does not contain a specific judicial remedy to challenge the conduct of the inspection. The General Court dismissed the plea. It found that businesses subject to an inspection have, in practice, several ways to challenge the conduct of this inspection (para. 88 of case T-255/17). As stated above, they may challenge the final decision, but they may also contest the conduct of the inspection by appealing the inspection decision. This may be the case where the Commission uses an out-of-scope document to adopt a new inspection decision (See *Deutsche Bahn*, T-289/11, paras 138 to 160). Businesses may also challenge a decision sanctioning their obstruction during the dawn raid, or, more generally, any act meeting the case-law requirements for "reviewable acts" which the Commission adopted in the course of the inspection, including a decision rejecting an application for protection of a privileged document. It is even possible to obtain the suspension of operation of certain measures taken by the Commission through an application for interim measures.

In *Intermarché/Casino*, the General Court further improved this protection by confirming the possibility for an undertaking to request the protection of documents covered by privacy and to challenge the Commission's potential refusal (paras 94 and 95 of case T-255/17). The General Court also confirmed in *Intermarché/Casino* that an application for interim relief may be made when the Commission rejects a protection request based on legal privilege. (paras 96 and 97 of case T-255/17).

Thus, while each of these judicial remedies does not, on its own, make it possible to carry out a complete judicial review of the merits of all measures taken in the course of the inspection, their combined use makes such a complete judicial review possible, in line with the requirements of the European Court of Human Rights.

There have recently been a number of high-profile court judgments considering privacy rights in the context of antitrust enforcement proceedings, including the conduct of dawn raids. Such inspections are by their nature highly intrusive. How is the correct balance to be struck between guaranteeing privacy rights, including those of employees, and ensuring antitrust agencies have adequate means to detect and prosecute cartels?

Before the boom of the internet, most of the evidence seized from cartels was contained in notebooks or in meeting minutes recorded on paper. Most of the "classic" cases concerning cartels are thus based on "smoking guns" contained in paper documents. Back when I was a case handler for the French Competition Authority, most of the evidence was located in email inboxes. However, I have the impression that over the last few years the way professionals communicate has drastically changed. As you say in your final question, "business is transacted through new channels, including social messaging platforms and networks". It is nevertheless possible for the Commission to conduct searches in this new IT environment. The Commission's explanatory note on inspections indicates that searches of the IT environment also apply to private devices and media that are used for professional reasons (the 'bring your own device' (BYOD) trend) (para. 10).

Does the seizure of personal information breach, in itself, the right to privacy? Even if the powers of inspection conferred on the Commission by Article 20(4) of Regulation 1/2003 vis-à-vis an undertaking constitute an interference with the latter's right to respect for its privacy, (including respect for private premises and correspondence), inspections may be conducted when they are necessary and proportionate to the aim pursued. In my opinion, the correct balance is struck primarily by verifying that the decision is not arbitrary inasmuch as it is necessary to detect and pursue an infringement. The EU Courts may be called upon to review a decision adopted under Article 20(4) of Regulation 1/2003 for the purpose of ensuring that it is in no way arbitrary, that is to say, that it has not been adopted in the absence of facts capable of justifying an inspection. As I said above, this is what the General Court actually did in *Intermarché/Casino*, where it requested, by way of measures of organization of procedure, that the Commission produce all the evidence relied upon to adopt the inspection decision and carried out a thorough review of each one.

Moreover, while the interference with privacy rights may not, in itself, justify the annulment of the whole inspection because, as you suggest, inspections are, by their very own nature, intrusive, this does not rule out the possibility for undertakings to challenge the seizure of a specific document on privacy grounds. As explained above, the General Court, made this possibility clear in *Intermarché/Casino*. However, it must be borne in mind that the undertaking subject to the investigation needs, in order to activate this remedy, to make a specific request to the Commission in the course of the inspection.

Therefore, the jurisdictional protection given to businesses subject to inspection appears to me as a complete one, even though issues related to the respect for privacy rights may increase in

the future given the progressive blurring of lines between private and professional life. The right to disconnect (*droit à la déconnexion*) is a striking illustration of this blurring of boundaries. But, as is often the case, society changes faster than the law and it always takes time for the law to adapt.

We have witnessed the progressive digitisation of the workplace, a trend accelerated by reformed work practices caused by the COVID-19 pandemic. Business is transacted through new channels, including social messaging platforms and networks, and relevant digital evidence can be voluminous and heterogeneous in nature. Are the Commission's practices and procedures suited to the challenges of the digital world?

As I mentioned in my response to your third question, the Commission considers that it enjoys access to private devices and media that are used for professional reasons (due to the BYOD trend) when they are found on the premises. Personal mobile phones are typically requested along with any company phones, and the same applies to laptops and tablets. With these devices, inspectors have access to exchanges on social media and apps, personal email and chat rooms. A number of recent cases have relied to a significant extent on exchanges of that nature, which have provided renewed and almost unlimited sources of evidence in antitrust inspections. It is likely that due to the pandemic and the development of remote working future inspections will increasingly rely on digital evidence such as, for instance, phone connections and data related to localization. This brings me to two comments.

Firstly, as you rightly point out, the digitization of the Commission's inspection procedure gives rise to issues of "volume" and "heterogeneity". As mentioned in the ICN scoping paper on "Big Data and Cartels", the potential gathering of large sets of data exacerbates issues regarding the treatment of privileged or confidential information or the protection of privacy/personal data, notably in the context of reinforced regulation on this matter. As noted by the OECD recently, "since digital searches enable access to a great amount of information during unannounced inspections, incidental evidence issues may come up more often" [DAF/COMP/GF(2018)7, 23 October 2018]. Heterogeneity raises other issues: arising from the fact that the Commission forensic tools designed to guarantee the seizure of emails may not be yet perfectly suited to seizing messages on social messaging platforms and networks like Facebook or WhatsApp, let alone messages on less popular applications such as Telegram, on which data are very safely encrypted. Evolution on these matters will hinge on budgetary means allocated to improving forensic search tools and, potentially, the reactions of courts called upon to adjudicate on massive seizures of data by competition authorities. Up to now, the EU courts have upheld the legality of the Commission's practices as regards seizures of digital data.

Secondly, the localization of data servers may also raise issues in the future. As is stated in the ICN scoping paper on "Big Data and Cartels", many competition authorities, including the Commission as I understand it, adopt an "access approach": data that is accessible to the company has to be rendered accessible to the investigators, and failure to do so may result in charges of obstruction and possible prison sentences and/or fines (depending on the jurisdiction). Other competition authorities adopt a "location approach", whereby they can only search for data located within the premises or in specific places provided for under the search warrant. The latter approach may not allow data stored on clouds to be seized.

It remains to be seen what legal questions and challenges arise in the future regarding these diverging approaches.

To hear more, see the Program, and register for the conference for free below:

REGISTER FOR THE CONFERENCE

The views and opinions expressed in this document do not necessarily represent those of the speakers' institution or clients.