Dawn Raids and the Role of Forensic IT in Antitrust Investigations

by

Jan Polański*

CONTENTS

I. Forensic IT
II. European Union
  1. Legal framework
  2. Forensic IT in practice
III. Poland
  1. Legal framework
  2. Forensic IT in practice
IV. Digital investigations or investigations with a digital element?
  1. Full forensic images
  2. Pre-selection procedures
  3. On-spot pre-selection and continued inspections
  4. Dawn raids outside business premises and/or dawn raids by non-antitrust officers
V. Pre-selection procedures: a needed development or a mistake?
  1. Scope of the dawn raid
  2. Analysing digital evidence as an 'act of searching'
  3. Just the minimum?
  4. Pre-selection and legal privilege protection
  5. Pre-selection and private information
VI. Alternatives
VII. Conclusion

* Counsel to the Head of the Polish Office of Competition and Consumer Protection (UOKiK), Antitrust Department. The views expressed in this article are the author's own and do not necessarily reflect those of the Polish Office of Competition and Consumer Protection (UOKiK).

Article received: 2 March 2020, accepted: 30 April 2020.

Abstract

While digital markets attract much attention of the antitrust community, important developments also take place in relation to the way antitrust investigations are handled and evidence is preserved. More and more enforcement actions of antitrust authorities rely on the ability to find and preserve digital evidence of an illegal activity. This article focuses on recent case law developments in relation to the approach to forensic IT in antitrust enforcement and investigates whether enough leeway is left to the antitrust authorities to properly discharge their powers. The article focuses on the procedural developments at the EU level and in one EU national jurisdiction, i.e. Poland. The article concludes that the current approach to forensics in antitrust does not allow to use available capabilities to a full extent. A proposal is made for an alternative approach, which would benefit effective antitrust enforcement and due process.

Resumé

Si les marchés numériques suscitent une grande attention de la part de la communauté antitrust, des évolutions importantes ont également lieu en ce qui concerne la manière dont les enquêtes antitrust sont menées et dont les preuves sont préservées. De plus en plus d'actions des autorités antitrust sont fondées sur la capacité à trouver et à préserver les preuves numériques d'une activité illégale. Le présent article se concentre sur les développements récents de la jurisprudence concernant l'approche de l'informatique juridique dans l'application de la législation antitrust et examine si les autorités antitrust disposent d'une marge de manœuvre suffisante pour exercer correctement leurs pouvoirs. L'article se concentre sur les développements procéduraux au niveau de l'UE et dans une juridiction nationale de l'UE, la Pologne. L'article conclut que l'approche actuelle ne permet pas d'utiliser pleinement les capacités disponibles. Une proposition est faite pour une approche alternative, qui bénéficierait d'une application efficace de la législation antitrust et d'une procédure régulière.

Key words: computer forensics; dawn raids; digital investigation; due process; evidence; forensic IT; inspections, searches.

JEL: K21, K42

I. Introduction

When the police raid the premises of a suspected murderer, the task is typically simple: find the murder weapon. Yet, searches may still require going through each piece of furniture to find what is looked for. Antitrust offences,

however, do not leave easily traceable tracks or smoking-guns. Collusion may come down to a simple: '*yes, let's do it*'. In consequence, the hunt for evidence in antitrust cases typically starts with a search for the only thing that could have been left by perpetrators: a note, memo or written communication. Still, in the age of information it is the digital world in which traces of one's actions are more often left. To no surprise, 'forensics', which has been known to criminal investigations for decades, made a huge entry into the realm of antitrust enforcement in the form of computer forensics (forensic IT).

At the same time, as liability for hardcore antitrust infringements is hard to refute, more actions have recently started to aim at questioning procedural aspects of antitrust investigations (Van der Woude, 2019). Against this backdrop, concerns have been voiced that there is a risk that if case law on procedural issues becomes too harsh, antitrust enforcement might become ineffective (Van der Woude, 2019).

This article aims at discussing whether recent case law developments concerning dawn raids and the preservation of digital evidence leave proper space for the use of forensic IT in antitrust enforcement. As a secondary objective, the article is intended to investigate whether any adjustments could be introduced to European antitrust to foster the use of forensic IT. The article focuses on EU and Polish law. The EU perspective serves as a reference point for most European jurisdictions. The Polish perspective serves as an example of a national jurisdiction in which judicial developments significantly changed the way forensic IT is used in antitrust investigations.

In the article, I first discuss in layman terms the role of forensic IT in antitrust investigations (Section II). After doing so, I focus on how forensic IT has been used in antitrust investigations at the EU level and on a national (Polish) level (Section III and Section IV). This analysis is followed by observations on the feasibility of the current approach to forensic IT (Section V) and then by an analysis on whether restrictions on the use of forensic IT in antitrust investigations are warranted (Section VI). Finally, I provide alternatives to the current approach (Section VII).

II. Forensic IT

Forensics in general aim at collecting and analysing pieces of evidence throughout the investigation. Such pieces of evidence may include various objects, for example blood samples, body tissues, fingerprints. Collecting such evidence may not be easy. Evidence may not be well preserved when investigators arrive at the crime scene, due to, for instance, the passage of

time. Evidence might also not be easy to locate, as among 'relevant evidence' (e.g. pieces of hair of the murderer) many pieces of 'non-relevant evidence' may too lie at the crime scene (e.g. pieces of hair of someone who happened to be present at the crime scene before the crime took place).

After evidence is collected the job is not yet done. Blood or tissue samples alone say nothing and require further analysis in laboratories to establish their basic properties. When the basic properties are known, the process is still not over – once, for example, the blood type is known one must further investigate how this information fits within the broader picture of the investigation. In other words, forensics is a complex task.

Forensic IT is not much different in that respect. It aims at fostering investigations by collecting and analysing digital evidence. To collect such evidence, one must first locate it. Once evidence is located, it must be collected and preserved in a way which prevents distortions. Finally, the collected evidence must be analysed.

Here, ordinary forensics and forensic IT become harder to compare. Let us assume that the investigators managed to recover from the crime scene five fingerprints. Is that many? In quantitative terms probably not, just five objects. Still, probably enough to move the investigation from the crime scene to laboratories for further analysis. Let us then assume that the investigators managed to find at the investigation scene two data carriers. Is that many? Probably not. On the other hand, a modern data carrier may store hundreds or thousands gigabytes of information. Does it say much to the layman? Probably the layman will know that an electronic document will carry a weight of approximately 200 kilobytes and that a holiday photo he or she made requires some 2 megabytes of storage capacity. And that his or her smartphone may store up to 32 gigabytes of data. Still, how much is that really and how easy or hard is it to analyse such a volume of data? The layman uses the 'search' option in his or her laptop and mailbox every day, and it works well. Also, a file is a file, is that not the case? Should then forensic IT experts make searches instantly or move their investigation to a lab, same as other forensic experts do? This question plays a fundamental role on how the analytical process is organised and will remain the main area of interest in this article.

While forensic IT may play a role before investigators arrive at dawn raid locations, its role becomes more visible once search teams start their work. In consequence, the forensic process becomes closely connected with dawn raids (inspections, searches).[1] Typically, antitrust investigators will gather digital evidence during dawn raids and, hence, the forensic IT process will usually

[1] Various terms are used under European antitrust laws to refer to actions which aim at finding evidence at premises belonging to suspects or other parties. In this article terms such as 'dawn raid', 'inspection', and 'search' are used interchangeably, unless they refer directly to EU

take place at least partly at the searched location, where evidence is located (**on-spot inspection**).

However, as mentioned before, some part of the forensic process may take place after investigators leave the searched location, for instance, in a lab or other adapted environment. As far as it concerns European antitrust investigations, such further actions may in consequence be taken within so-called '**continued inspections**', or **outside the framework of inspections** altogether. In the former case, the searched party will typically be able to use his or her main right of a searched person, i.e. be present when investigators conduct the continued inspection. In the latter case, all actions are taken outside the framework of an inspection, meaning typically that the investigators take actions behind closed doors.

While forensics aims at discovering evidence and establishing case facts, it also has another facet. As forensic IT plays an important role during dawn raids, questions arise when the forensic process ends, or rather, which forensic actions should take place within the framework of a dawn raid and which can be taken later. In other words, does the role of forensics in the dawn raid end once evidence is collected or should the forensic process (e.g. analysis of digital evidence) continue within the framework of the dawn raid? Also, what constitutes 'evidence' – is it the collected data or data that was subjected to some sort of further selection?

To conclude, same as with evidence such as blood samples and body tissues, **digital evidence must be first found, collected, and preserved** from distortions.[2] **Then it can be analysed** in order to establish its true relevance for the investigation. In case of non-digital evidence, it should be clear for a layman that typically such analysis will take place outside the crime scene or searched location. There is no rush or any other reason to run on a regular basis, for instance, blood tests at locations where blood samples have been found. The case of digital evidence might be less clear-cut from the point of view of a layman. One could say that any piece of digital evidence is simply stored in a specific way, same as documents can be stored in folders and then folders in a filing cabinet. There are at least three options to approach the issue of analysing digital evidence in antitrust investigations: (a) do it 'on the spot'; (b) do it outside the searched location, but still within the framework of an inspection (continued inspection); (c) do it outside the searched location and outside the framework of an inspection. As is further discussed, all three approaches are known to European antitrust enforcement.

---

or Polish law. In the latter case, the article follows the terminology used under the applicable body of law.

[2] On the stages of this process see also: OECD, 2018a, p. 5–7.

III. European Union

1. Legal framework

According to Regulation 1/2003, the European Commission may inspect undertakings in connection with its powers to enforce Article 101 and 102 TFEU.[3] The European Commission may also inspect other premises.[4] Inspections at the premises of undertakings do not require *ex ante* judicial authorisation, while inspections at other premises do require approval of relevant national courts. An inspection can be started based on a written authorisation or a formal decision issued by the European Commission, in the latter case the inspected entity is obligated to submit to the inspection. In any case, the European Commission has to specify the subject matter and purpose of the inspection. The European Commission is not in a position to (forcefully) overcome opposition to its inspections, but it may call national authorities to provide such assistance.[5] The inspected entity has a right to challenge the inspection decision.[6] However, the inspected entity cannot challenge 'measures implementing the decision' (*i.e.* specific actions taken during the inspection), until an infringement decision is adopted. This is because the implementing measures do not constitute a 'decision' and hence remain outside the remit of EU courts.[7]

During an inspection, the European Commission is empowered inter alia to 'examine the books and other records related to the business, irrespective of the medium on which they are stored' and to 'take or obtain in any form copies of or extracts from such books or records'.[8] It was argued in the past that the manner in which the European Commission interprets its inspection powers amounts to conducting a search, but the European Court of Justice dismissed such arguments, pointing out that the European Commission is not in a position to use force and that, without an effective power to look through each piece of furniture and all documents, its inspection powers would become illusory.[9]

---

[3] Article 20 of the Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 04.01.2003, p. 1–25.

[4] Article 21 Regulation 1/2003. For instance, houses in which managers reside.

[5] Article 20(6) Regulation 1/2003. This does not preclude the possibility of fine imposition for the obstruction of the inspection.

[6] Article 263 TFEU.

[7] GC judgment of 14 November 2012, Case T-135/09 *Nexans*, ECLI:EU:T:2012:596.

[8] Article 20(2) Regulation 1/2003.

[9] ECJ judgment of 21 September 1989, Joined cases 46/87 and 227/88 *Hoechst*, ECLI:EU:C:1989:337, para. 27.

2. Forensic IT in practice

Since the early nineties the dawn raid teams of the European Commission have included trained IT personnel, and since 2006 the European Commission has been using forensic IT hardware and software.[10] As the European Commission is not empowered to seize evidence, it makes forensic images of datasets, which are then reviewed to select relevant information. According to the European Commission, the review process typically takes place at the premises of undertakings, and undertakings' representatives are entitled to 'shadow' the members of inspection teams. Also, according to the European Commission, the selection process typically takes less than a week, and hence appears limited time-wise.[11] Occasionally, the process may continue at the premises of the European Commission within the framework of a 'continued inspection'. In such a case, the European Commission invites the inspected undertaking to be present during the continued inspection. It is unclear whether on-spot selection takes place also when premises other than those of an undertaking are inspected (e.g. the home of an executive). Once the selection process is finished, relevant information is put into the case file, while any other information is wiped from the data carriers used during the selection procedure.

The procedure outlined above sparked controversy and became subject to judicial review. While it has been clear since *Hoechst* and *AM&S* that the European Commission may examine each document, but is not in a position to investigate the contents of documents covered by legal professional privilege, the practice of preserving large datasets was challenged by one of the undertakings subject to the *Power Cables* investigation.[12] The same party also contested the practice of conducting selection procedures at the premises of the European Commission.

As regards the first claim, the inspected undertaking pointed out that by making a full forensic image of a data carrier, the members of the inspection team exceeded the powers envisaged in Article 20(2) of Regulation 1/2003. The inspected undertaking argued that the European Commission is only allowed

[10] OECD, 2018b, p. 4.

[11] As pointed out in Section II, a single data carrier can store vast amounts of information. The same applies to business mailboxes. Taking into account that antitrust infringements are typically committed by groups of individuals, it can be reasonably assumed that at the initial stages of investigations, antitrust authorities collect a number of datasets which corresponds to the number of suspects (individuals) or exceeds it. In consequence, the amount of data subject to such a pre-selection can be expected to be considerable, making the process of selection *de facto* very quick (and, possibly, closer to a cursory analysis rather than an in-depth one).

[12] 46/87 and 227/88, *Hoechst*; ECJ judgment of 18 May 1982, Case 155/79 *AM&S*, ECLI:EU:C:1982:157; Case T-449/14 *Nexans*.

to 'copy' materials that were already examined (and within the scope of the inspection decision). Since the European Commission made a forensic image of a whole data carrier (a computer hard drive), it 'copied' also information which (allegedly) was not covered by the inspection. According to the inspected undertaking, such an interpretation would also mean that the European Commission could very well make forensic images of the undertaking's whole IT system to review them later at the premises of the European Commission.[13]

The General Court concluded that making a full forensic image of the data carrier served the purpose of a further selection of information. The General Court pointed out that making forensic images falls within the scope of powers given to the European Commission under Article 20(2) (b) and (c) of Regulation No 1/2003.[14] Also, the European Commission did not put the generated forensic images directly into the case file, without examining them first.[15] In consequence, the General Court did not find the actions of the European Commission controversial or beyond the scope of its powers.

As regards the claim that by conducting a continued inspection the European Commission acted unlawfully, the General Court pointed out that neither Regulation 1/2003 nor the inspection decision specified that the European Commission had to conduct its actions at the premises of the inspected undertaking. The General Court also pointed out that the fact that the continued inspection had started one month after the on-spot inspection, was in line with the law. The inspection decision did not define the end date of the inspection, and while this did not mean that the inspection could last indefinitely, the inspected undertaking did not argue that the period of one month was excessive.[16]

The judgment of the General Court has been appealed by the inspected undertaking and is not final at the time this article is written, but nevertheless provides important insights on how the EU first instance judicial body approaches the powers of the European Commission. Firstly, the General Court does not see any problem with making full forensic images. Secondly, the General Court does not see as problematic the practice of continued inspections – it was sufficient for the court to see that the inspection decision had not precluded such a procedure and that there is nothing precluding such an approach under the applicable legislation. The Advocate General concurred with this position.[17]

---

[13] Case T-449/14 *Nexans*, para. 35.

[14] Case T-449/14 *Nexans*, paras. 54–55.

[15] Case T-449/14 *Nexans*, para. 58–59.

[16] Case T-449/14 *Nexans*, paras. 68–69.

[17] Opinion of AG Kokott delivered on 12 March 2020, Case C-606/18 P, *Nexans*, ECLI:EU:C:2020:207, paras. 29–100. The Advocate General stated inter alia (para 61) that

IV. Poland

1. Legal framework

The Polish legal framework surrounding dawn raids is overall similar to the EU one, but holds some important differences, which are outlined below.

Firstly, under Polish law the Polish Competition Authority is empowered to conduct **inspections** and **searches**. Since 2014, inspections and searches are regulated on their own, each constituting a different type of dawn raid (before 2014, searches could only take place within inspections, meaning that the competition authority had to first start an inspection, and that relevant national legislation concerning inspections at business premises applied also to searches).[18]

The main difference between inspections and searches is that during searches the members of dawn raid teams are not dependant on the cooperation on the part of the undertaking, which in practical terms means inter alia that in case of encountering opposition, they are in a position to make copies of documents and data carriers by themselves and do not need to rely on the undertaking's cooperation.[19] The Polish Competition Authority may issue on its own written authorisations for its officers to conduct inspections. To conduct a search, on the other hand, a court authorisation is needed.

Apart from that, however, many of the inspection powers are also available during searches, meaning, for instance, that the searched undertaking can be asked to give access to its IT systems and can be fined for refusing to do so (apart from that, the searching officers may obviously attempt to gain such access on their own or seize IT equipment, as the power to seize is also available). The Polish legislation mentions explicitly continued inspections and envisages that to conduct such an inspection the agreement on the part of the inspected undertaking is needed. When it comes to searches, the applicable legislation remains silent on the possibility of conducting a 'continued search'.

Contrary to EU law, Polish law provides a legal remedy to question the actions taken by the investigative team during inspections and searches

respect for the rights of undertakings does not mean that the European Commission's powers must be interpreted narrowly per se, but rather, interpreted and applied in such a way that respect for those rights is guaranteed. In consequence, the limitations to which the exercise of the European Commission's powers is subject are not an end in themselves, but serve to ensure that those rights are respected.

[18] Inspections are covered by Article 105a of the Polish Competition Act (Act of 16 February 2007 on competition and consumer protection, consolidated text: Journal of Laws 2019, item 369; hereinafter: PCA) and searches are covered by Article 105n PCA.

[19] Article 105o PCA.

('acts of inspecting' and 'acts of searching'), even if they do not constitute decisions on their own. In practical terms this means that the inspected or searched undertaking (and any other entity whose rights have been affected) may challenge these actions immediately or shortly after they take place. In consequence, Polish legislation provides rights which go far beyond what is possible under EU law.

Another difference in comparison with the EU system is the fact that Polish antitrust investigations typically take place in two stages, which are split apart more visibly than in the EU procedure. These stages are: (i) preliminary investigations; (ii) full antitrust investigations. There are no parties to preliminary investigations and, in consequence, no party has access to the file at this stage of the investigative process. Preliminary investigations serve the purpose of gathering information and evidence, and they never end with a decision, they rather constitute a procedural framework within which the Polish Competition Authority can use (some of) its powers. Case files for both types of investigations are separate and only relevant pieces of evidence become part of the case file of a full antitrust investigation. Dawn raids can be conducted both in preliminary and full antitrust investigations, but in practice preliminary investigations are generally the framework for searches. This is because undertakings have to be formally notified when full antitrust investigations are initiated (and so the surprise effect of a dawn raid ceases to exist). In consequence, evidence collected during dawn raids by the Polish Competition Authority is typically first put into the file of a preliminary investigation. As mentioned before, the issue of whether something becomes part of the file turned out to be relevant for the General Court in its analysis of the forensic IT procedure followed by the European Commission, and hence it seems relevant to bear in mind this characteristic of the Polish antitrust procedure.

Apart from the general power to search premises of undertakings, the Polish Competition Authority can also initiate searches conducted by the police. In such a case the search is conducted by police officers (assisted by antitrust officers) and may take place in any type of premises (houses, business premises, public premises).[20] This type of a search is conducted according to the national criminal procedure and most of the provisions concerning searches conducted on its own by the Polish Competition Authority do not apply.[21]

[20] The roles are, therefore, reversed as during ordinary antitrust searches it is police officers that assist antitrust officials.

[21] For instance, under Article 105n PCA, the Polish Competition Authority may always fine an undertaking which opposes entry. However, in case of Article 91 PCA, a searched entity can be fined, but only if the police were asked to search business premises (Article 106(2)(4) PCA)

Since the Polish Competition Authority mostly uses forensic IT in case of searches, the remaining part of this discussion refers to searches, not inspections within the meaning of the Polish legislation.

2. Forensic IT in practice

What makes the Polish case interesting is the fact that the Polish Competition Authority used to employ on a regular basis an approach to forensic IT which was different to the one followed by the European Commission.

While it seems that since the early days the European Commission has been conducting on-spot selection of information, at least for some time this was not the case for the Polish Competition Authority. In consequence, during searches antitrust officers were first locating relevant data carriers (e.g. laptops of executives) and then preserving them, by making forensic images. As mentioned before, the Polish Competition Authority was empowered to (physically) seize data carriers, but it was typically not done so, and data carriers were returned to their holders, as forensic images were made.[22]

Consequently, at the initial stages of dawn raids, the situation was overall similar to the one in the investigations conducted by the European Commission. Still, once forensic images were ready, the situation was changing as the Polish Competition Authority did not consider forensic analysis to constitute an 'act of searching'. The search was aimed at finding relevant data carriers, not putting them under forensic analysis. This meant that once forensic images were generated, searching officers were typically leaving the searched location. The forensic analysis of generated forensic images could have been conducted behind closed doors. Little is known in relation to how legal professional privilege issues were handled in case of an analysis taking place behind closed doors – until 2017 no publicly known case law developed nor were there any soft law acts issued.[23] As regards privacy concerns, it should be borne in mind that as it has been pointed out earlier, dawn raids in Poland typically take place within the scope of preliminary investigations and that only relevant pieces

or the searched entity belongs to a group of individuals indicated in the Polish Competition Act (Article 108(2)(2) PCA).

[22] The power to seize granted to the Polish Competition Authority is of a limited character. Items can be seized, but only for 7 days. Such a limitation is not applicable in ordinary searches conducted under Polish criminal law; in consequence, the powers of the Polish Competition Authority are more restricted in that respect.

[23] However, it follows from the information made public in the judgment of the Competition and Consumer Protection Court of 7 March 2017, ref. no. XVII Amz 15/17 (*Calypso I*), which is also discussed further on, that potentially privileged information was not passed on to the case teams.

of evidence are then moved to the case file of a full antitrust investigation. In other words, privacy concerns (if any) could possibly arise only *vis-à-vis* the authority, which anyway was empowered to conduct the investigation.[24]

The landscape of how the Polish Competition Authority handles forensic IT significantly changed in 2017, when the authority decided to raid the premises of undertakings in the Polish fitness sector.[25] During a search at one of the locations, the searching officers located three electronic devices. Forensic images of the devices were made and saved on data carriers which remained at the disposal of the searching officers. The devices were returned to the undertaking, and the data carriers with forensic images were put into envelopes, which were then sealed. The envelopes were taken outside the searched location and transported to the premises of the authority.

The searched undertaking turned to the court alleging that the contents of the data carriers had been analysed outside its premises and without its representatives having the possibility to be present during this analysis.[26] The authority, on the other hand, refuted the allegations that the data carriers had been analysed, stating that the data carriers have remained sealed at its premises. Still, the authority also argued that any analysis of forensic images does not constitute 'an act of searching', rather a technical operation which is taken outside the framework of a search.

The court dismissed the case, pointing out that no action had been taken in relation to the forensic images and therefore there is no room to dispute the actions taken by the searching officers. The court also pointed out that making full forensic images was in line with the law. While the General Court concluded in the case discussed earlier that making full forensic images was covered by the general power to make copies, the Polish court opted for a different legal ground available under Polish law and pointed out that generating such images amounted merely to 'securing evidence'.[27]

Still, although the court dismissed the case, it also decided to further elaborate on the forensic IT procedure employed by the Polish Competition Authority. The court pointed out that while it dismisses the case, it might have been of a different opinion, had the authority started to analyse the forensic images. The court declared that such an analysis might constitute 'an act of searching', that the analysis should take place at the premises of the

[24] See also further comments in Section VI. For a wider discussion on data protection issues, see: Geradin and Kuschewsky, 2013.

[25] Judgment of the Competition and Consumer Protection Court of 7 March 2017, ref. no XVII Amz 15/17 (*Calypso I*).

[26] *Ibidem*.

[27] Article 105f PCA.

searched undertaking, and that the representatives of the undertaking should be afforded the possibility to be present during this process.[28]

Neither of the parties appealed the ruling. However, the case re-emerged a few months later when the searching officers returned to the premises of the undertaking to acquaint themselves with the contents of the forensic images and to conduct a selection procedure similar to those conducted by the European Commission. This led to three more complaints lodged with the court by the undertaking.[29] The undertaking pointed out, in essence, that the actions of the searching officers lacked a legal basis as, according to the undertaking, the search had ended a few months earlier when the officers had left the searched premises. The undertaking also pointed out that it had received a search report (which allegedly meant that the search had ended), and that in any case its rights had been infringed due to the lengthiness of the search.

However, the court pointed out that while the search report had clearly showed the date on which the search had started, it had not contained any indication of the end date of the search. The court also acknowledged that the search authorisation had not contained any fixed end date of the search, merely an estimation on when the search would possibly end. Furthermore, by returning to the premises, the authority followed the ruling of the court which had been given a few months earlier. The court again dismissed the complaints lodged by the undertaking, pointing out that the search was not over. The court confirmed that the search lasted a considerable amount of time, but concluded that considering the circumstances of the case, the search was not excessive. The case was further appealed by the undertaking, but the Court of Appeals followed the reasoning presented by the court of first instance.[30]

In consequence of the discussed case, the Polish Competition Authority changed its procedure in relation to forensic IT and started engaging on a regular basis in on-spot selection of information. In 2019, the Polish Competition Authority issued a soft law document on searches conducted at the premises of undertakings. While the soft law document makes a reference to the selection procedure, it does not do so in unequivocal terms. The document says rather that the searching officers 'may' decide to collect datasets

[28] As mentioned before, the relevant Polish legislation does not mention 'continued searches' at the premises of the authority; it only provides a clear legal basis for 'continued inspections'. Since the relevant national legislation provides a clear legal base in case of inspections, and does not provide it in case of searches, the court concluded that all 'acts of searching' need to take place at the premises of the searched undertaking.

[29] Judgment of the Competition and Consumer Protection Court of 3 October 2017, ref. no XVII Amz 121/17 (*Calypso II & III*); judgment of the Competition and Consumer Protection Court of 10 October 2017, ref. no XVII Amz 124/17 (*Calypso IV*).

[30] Judgment of the Court of Appeals of 8 February 2018, ref. no VII AGz 268/18 (*Calypso IV*).

larger than containing only information which will be used for the purpose of the investigation, and that they '*may*' engage in a selection procedure.[31]

It is not publicly known how the Polish Competition Authority would approach searches delegated to the police and conducted e.g. in the homes of executives. It is also unclear whether the Polish courts would expect the Polish Competition Authority (or police officers) to engage into any selection procedures in such cases. This issue is further discussed in the next section.

V. Digital investigations or investigations with a digital element?

As mentioned in Section II, the forensic IT process can be divided into at least two phases: (i) evidence collection and preservation; (ii) evidence analysis.[32] It seems reasonable to say that the effective use of forensic IT would include collecting and preserving all digital evidence found at the location, and that an effective analysis would be an analysis that leads to uncovering all relevant facts of the case, that is, discovering 'the truth' about what happened. However, this is also precisely the point where things become blurry. Against this backdrop, it is worthwhile to look at how the case developments at the EU and national levels may affect the actions of antitrust authorities.

1. Full forensic images

In the first place, it is interesting that the issue of generating full forensic images has been debated in courts both at the EU and national (for the purpose of this discussion Polish) level. It is also interesting to see that in both cases the courts arrived at the same conclusion namely that generating full forensic images is in line with the law.[33]

The practice of generating full forensic images (or in fact also partial images, but containing large datasets) seems to be reasonable both from the point of view of the searched entity and forensic IT. Supposing that no forensic images could be made, the investigating authority would need to come up with another way of preserving evidence, and the only one which appears

[31] UOKiK (Polish Competition Authority) (2019). *Wyjaśnienia dla przedsiębiorców – przeszukania* (*Guidelines for undertakings – UOKiK's searches*), Section 2.7.

[32] One could also think of other stages, e.g. evidence presentation, but this stage appears to be of a more technical and marginal character.

[33] The European Court of Human Rights arrived at a similar conclusion, see: ECHR judgment of 14 March 2013, Application no 24117/08, *Bernh Larsen Holding*.

viable in such a case is to temporarily seize the data carrier.[34] In case of devices which are not easily dismantled this would require seizing a whole device. In extreme cases, such as data stored on servers, this could mean seizing whole servers, even if the investigators were only interested in a few mailboxes. When it comes to the forensic IT perspective, on the other hand, some of the reasons for generating forensic images were properly outlined by the European Commission.[35]

In general, there seem to be no meaningful reasons not to allow the generation of (wide) forensic images of data. It should be clear that during a dawn raid, the investigating officers are in a position to examine all documents, pieces of furniture, and rooms. Without such a power dawn raids would be an illusion.[36] In consequence, the position of the General Court, which concluded that the European Commission may generate forensic images, so that it can examine and copy documents, seems appropriate.[37] A Polish court arrived at a similar conclusion, but using a different legal basis available under national law, which does not appear to be problematic.

Another issue is whether full forensic images can (or should) be treated as evidence or whether the contents of such images should be subject to some sort of pre-selection.

---

[34] Either for the time of pre-selection (which may adversely affect the effectiveness of the procedure) or until the investigation is over.

[35] Case T-449/14 *Nexans*, para. 52.

[36] To explain this point further, one can imagine a search conducted by the police at the premises of a murder suspect and the suspect saying: 'since you are suspecting me of a knife murder, you are not empowered to search this drawer as it contains only kitchen hammers'. Unless inspecting or searching officers are empowered to look through the premises, their powers are nothing more than a form of a request for information which simply takes place 'on the spot'.

[37] I strongly disagree in that respect with M. Michałek, who argued that the practice of generating wide forensic images should be utterly prohibited on proportionality grounds, as allegedly it is extremely intrusive, see: Michałek, 2015, p. 210. Dawn raids are 'intrusive' by their very nature and, as mentioned above, the powers of inspection would be illusory, if antitrust officials were not in a position to examine each piece of furniture and other objects. This is even more true in case of authorities which are empowered not merely to 'inspect', but to 'search', and are authorised to do so by relevant courts. In fact, M. Michałek admits that due to effectiveness considerations such a ban seems less probable. I also disagree with M. Michałek insofar as she takes as the basis of her position the conclusion reached by the European Court of Human Rights in the judgment of 3 June 2012, Application no 30457/06, *Robathin v Austria*. The aforementioned case concerned a search of the premises of an individual who was also a practicing lawyer, i.e. very specific circumstances. In comparison, the approach taken by the court in the *Bernh Larsen Holding* case quoted earlier was much different, this includes also a statement made by the court that more leeway may be warranted in case of business premises which belong to a corporate entity.

2. Pre-selection procedures

While the courts seem positive about pre-selection procedures, it is not that clear what should be the product of such procedures. It seems fair to assume that the pre-selection process might prevent putting into the case file information which is covered by legal professional privilege. However, a pre-selection procedure as something meant to protect legally privileged communication implicitly requires the raided entity to be present, so that the privilege can be invoked. Still, while such an approach may seem understandable, it does not logically require a pre-selection being made by the investigators. If some information is legally privileged, it is rather for the entity using the privilege to invoke it. To be invoked, the privilege does not require a full-blown pre-selection procedure, rather locating files covered by the privilege and disposing them.

Pre-selection appears to be even less clear when it comes to information which is not legally privileged. If one assumes that the only thing that can be put into the case file are things that are (literally) indicated, in the inspection decision or search authorisation, as 'issues' which provided grounds for the inspection or search, then such an approach does not appear workable.

To explain this, let us return to the less 'digital' world of ordinary forensics. Let us assume that the police conduct an investigation in the area of organised crime. The police raid premises of an accountant who knowingly provides services which facilitate the execution of criminal activity. At the premises, the police find a ledger. The ledger contains dozens of entries made on a regular basis and some hand-written notes on blank pages. Three pages are torn out and a few pages are damaged with their top corners being cut out. The police officers go through the names included in the ledger, but do not recognise any of the names as belonging to any of the investigation suspects, apart from one which had been recorded in an entry at page five. Page five of the ledger is one of those with cut corners. The notes included in the ledger appear to be mostly some private notes, reminders, and doodles, but some are hardly legible, and some are clearly written in some exotic language.

What constitutes 'evidence' then, and what should be preserved for the investigation? Is it the single entry at page five of the ledger? Or maybe the whole page five which includes the entry? Or maybe rather all pages with cut corners? On the other hand, cut corners might be just a coincidence and the whole ledger may include relevant entries with fake names instead of the real ones. Then the whole ledger might be relevant. Also, even if the fake names theory is not true, the ledger shows marks of some pages being torn out – something that might be relevant for the investigation. Furthermore,

the ledger includes passages that are illegible or unreadable for the police officers. Prudence indeed may justify seizing the whole ledger. In legal terms, however, this means that the investigators seize information which in objective terms might not be relevant for the investigation – it is the subjective element which warrants such an action.

As was discussed in the previous sections, the case of forensic IT in antitrust is in fact not that different. The Polish example shows in particular that the investigating authority might arrive at the conclusion that data carriers form a certain 'entirety' (same as the ledger) that only subsequently can be subject to analysis, which, however, is not part of the search.[38] The example of the European Commission might seem different at first sight, but on the other hand, it does not seem that the European Commission has adopted a significantly different approach when it comes to the substance of the issue. It is true that the European Commission engages in a pre-selection of information stored on data carriers, but it also points out in its public documents that it copies to the case files all evidence items in their 'technical entirety'.[39]

Still, it is highly arguable what constitutes a 'technical entirety'. The European Commission provides an example of an e-mail with attachments, still forensic images generated by antitrust authorities rather contain the contents of data carriers or specific mailboxes as a whole (*i.e.* files which are in fact a form of a table, a 'ledger' which contains further information) as some sort of 'technical entirety'. Typically, for the convenience of the user, forensic IT software can display such contents showing separate files or e-mails, but this does not mean that such e-mails exist on their own. In consequence, it could be very well argued that it is the mailbox ('the table') which constitutes a 'technical entirety'. The difference between choosing an e-mail (with some paragraphs not relevant), e-mail with attachments (with some attachments not relevant) and a file table with information on e-mails (with some information in the table not relevant) is not a difference in substance. In each case, the case file will contain information which is not literally connected to the issue which provided grounds for the dawn raid. On the other hand, in each case information is clearly obtained in connection with a dawn raid.

Likewise, if the inspection decision or search authorisation mentions that the dawn raid will take place because of a suspicion of price-fixing in the market for widgets, and the investigators encounter an e-mail which in one paragraph discusses price-fixing in the market for widgets and in another the price-fixing in the market for gadgets, then only information about widgets is

[38] After all, it is the data carrier that serves technical purposes, not some part of a binary pattern saved on it.

[39] European Commission (2015). *Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003*, para. 16.

truly relevant. Still, it is unreasonable (and technically cumbersome) to extract and put into the file just one paragraph of the message. This is also not what would be done in case of a simple letter.

It should also be said that preserving for the investigation a full forensic image or partial forensic image containing a larger dataset should not be easily dismissed as a forensic IT practice. Dawn raid teams typically include forensic IT experts, but are mostly comprised of staff better suited for legal assessments, not forensic analysis. While it might be more interesting for such officers (and for courts) to, for example, learn what was written in a given document or e-mail, it does not mean that in the digital era this is the only information that can be extracted from digital evidence. It should also be kept in mind that what is 'relevant' is in practice subjective. In fact, also the lack of information in relation to a certain period, or a change in the pattern of communication, might be relevant for the analysis (OECD, 2018a, p. 7, para. 30). Typically, only at the very end of the investigation, it can be known for certain what was actually needed to establish an infringement. Information on, for instance, the location of electronic devices at a given point in time might at first seem not connected with the investigated market practice, but with other evidence which refers to the dates of events and location of other devices, it can help proving that, for example, someone took part in a collusive meeting. Such an analysis might be, however, highly time-consuming and labour-intensive. Conducting such an analysis at a dawn raid location can be compared to conducting a surgery on the battlefield, which is obviously possible, but the chances for the patient to survive would be far greater if the surgery takes place in a proper environment.

3. On-spot pre-selection and continued inspections

Ultimately pre-selection always comes down to some form of a more in-depth analysis. Against this backdrop, continued inspections, which take place at the premises of an antitrust authority, offer surroundings far more favourable to forensic analysis than raided premises.

In the cases discussed in the preceding sections, the courts arrived at different conclusions when it comes to continued dawn raids. The EU court concluded without much hesitation that continued inspections are possible under EU law. The national (Polish) court concluded that under the applicable national law continued searches are not an option. It seems, however, that this difference is of little practical importance, as the Polish court did not offer any sophisticated reasons why not to allow continued searches; rather, it referred to the language of the applicable legislation and provided its interpretation in that respect.

As regards continued inspections themselves, there are few reasons to believe that they will not take place in the future. The main reason for that appears to lie not in the ruling given by the General Court and discussed in this article, but in the adoption of Directive ECN+.[40] The Directive replicates to a large extent the powers of the European Commission, but states also clearly that national competition authorities should be afforded the possibility to conduct continued inspections. Taking into account that national competition authorities will be in a position to conduct continued inspections, it seems unlikely that EU courts will find it reasonable to restrict the powers of the European Commission (which enforces Article 101 and 102 TFEU), with national competition authorities (which may enforce Article 101 and 102 TFEU) having this possibility.

Obviously, it can be argued that there is now a clear legal basis for continued inspections in Directive ECN+, and no such basis in Regulation 1/2003, and that, therefore, the European Commission should not be allowed to conduct continued inspections. However, taking into account the *effet utile* doctrine and cooperation between the European Commission and national authorities, it is rather unlikely that such an argument would be effective. The main reason for that is the fact that the powers of the European Commission would be then restricted, but in a very artificial way, since the European Commission is always in a position to simply ask the national competition authority to conduct an inspection for its purposes and assist the national competition authority in doing so. With Directive ECN+ adopted, there would be no real consequence of prohibiting the European Commission from conducting continued inspections. In fact, it can be said that by proposing Directive ECN+, the European Commission secured some of its own interests, without adopting any changes in Regulation 1/2003.

In consequence, it is more useful to think whether conducting pre-selection procedures during continued inspections is an optimal solution from the point of view of forensic IT. I think there are two reasons for which conducting such procedures is problematic.

In the first place, it should be remembered that depending on the depth of the analysis, making the selection might become a time-consuming process. As explained above, it is not clear what should be the final result of a pre-selection, as it is arguable what in fact constitutes evidence. It is also unclear when a continued inspection becomes too long. This issue was subject to legal review in both cases discussed in this article and, in each case, the court

[40] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, OJ L 11, 14.1.2019, p. 3–33.

decided that the length of the continued inspection was not unreasonable. The problem is, however, that without clear indication on how long the continued inspection may last, it might be hard to properly plan its stages in advance. On the other hand, the fact that the courts did not define any clear boundaries can be a positive development, since as long as an antitrust authority provides persuasive reasons to continue its actions, there are no reasons to believe a continued inspection will be deemed too long. Not having a statutory time limit may better serve a wide variety of cases encountered in practice and, in fact, also the interests of inspected entities as each case can be evaluated on its own.

The more important issue is the fact that a pre-selection will typically lead to some information being wiped. As mentioned earlier, data carriers may contain vast amounts of information, highly exceeding what could be effectively analysed by a human being even within a longer timeframe. A piece of information from a given data carrier may also be incomplete and may become understandable only when connected with other information in the possession of the authority.[41] Without analysing all information together it may turn out impossible to effectively secure and preserve information for the investigation.

Still, a continued inspection would typically be conducted with undertakings' representatives being present during the whole process and it is hard to imagine that all information at the disposal of the authority can be easily merged and analysed together, since it would also mean that, for example, each inspected undertaking would be looking through the e-mails of its competitor along with the investigating officers. In consequence, something which would be natural, effective, and recommended during an analysis behind closed doors, would most likely prove to be impossible during a continued inspection. Furthermore, since any not pre-selected information would be wiped at the end of the pre-selection, there would be no way back.[42] To conclude, continued inspections may affect the added value of forensic IT in a highly negative way and hence hamper effective enforcement.

---

[41] For instance, a mailbox may include an e-mail which at the first sight appears to have no apparent connection with the issues stated as the reason for the dawn raid (e.g. an e-mail stating: 'we have to finally hang out next week, I will fix some sandwiches' sent to an e-mail address created under some free-of-charge e-mail service). Without the context, it would be hard for antitrust officers to explain why such an apparently private e-mail should be included into the case file or even to realise that the e-mail is something relevant. However, an e-mail from a mailbox found at a different dawn raid location or information provided further on during the investigation might explain that the e-mail account of the addressee was used by another member to a price-fixing conspiracy and that the message meant that a collusive meeting should be set up, as one of the parties to the collusion wants to soon further raise prices.

[42] See also: ICN, 2014, p. 10.

4. Dawn raids outside business premises and/or dawn raids by non-antitrust officers

As mentioned earlier, antitrust authorities can be empowered to initiate, in one way or another, dawn raids outside business premises. The Polish example also shows that such dawn raids can be conducted by non-antitrust officers (e.g. the police) and under laws different than those applicable to antitrust officers (e.g. criminal law). This may lead to unexpected results, if conditions on the use of forensic IT by antitrust authorities become too tight.

Let us assume that an antitrust authority is empowered to collect evidence with the help of the police or other law enforcement agencies. However, those agencies when cooperating with the antitrust authority are supposed to act in accordance with their own procedural rules. For instance, in the Polish case, searches conducted by the police fall mostly under the criminal procedure, and according to the best knowledge of the author, they do not include selection procedures (which may also explain why the Polish Competition Authority did not engage on a regular basis in such procedures before 2017). In consequence, when police officers raid the premises of a person suspected of, for instance, distributing child pornography, they do not sit with the suspect at the searched premises and conduct a selection process, neither do they invite the suspect to their offices to do so during a 'continued search'.

It is also hard to imagine that police officers, who are not trained in antitrust, would be able to make any meaningful pre-selection before passing the collected evidence to the antitrust authority. On the other hand, if the courts expect a selection procedure within the context of searches conducted by the antitrust authority, it would be difficult to explain what warrants the imposition of more constraints on the officers of the authority than on the police officers.

Furthermore, on-spot pre-selection procedures are hardly reconcilable with conducting dawn raids at premises other than business premises, as it is hard to imagine that a selection process would be conducted in private homes over a number of days or weeks. While continued inspections provide an alternative, it is arguable whether it is a sensible one in practical terms. This applies in particular to the European Commission as the searched entity (e.g. an employee of the undertaking) would need to either travel to Brussels to make real use of the right to participate or incur significant costs in terms of legal fees.

In any case, it does not seem appropriate to prevent national authorities from using their powers and cooperating with other law enforcement agencies, especially insofar as such powers facilitate evidence collection in relation to liability under national laws (either the liability of undertakings or individuals,

with the latter currently not being even an option under EU law). Here, however, the situation becomes similar to the case of Directive ECN+ and the power to conduct continued inspection. As mentioned before, the European Commission may request national competition authorities to make use of their investigative powers for the purpose of its investigations, effectively circumventing any arguments that it cannot conduct continued inspections. When it comes to the national level, the national competition authority takes the role of the European Commission while non-antitrust law enforcement agencies take the role of an authority which might use a more effective (in some respects) investigative measure. In other words, restrictions put on the national competition authorities become artificial and hard to explain in a broader legal context.

VI. Pre-selection procedures: a needed development or a mistake?

From the forensic IT perspective, the applicable approach of antitrust authorities and the case law developments discussed above are ambiguous. On the one hand, the way evidence is collected respects the unique character of digital evidence, on the other, the idea of pre-selection procedures is something that from the perspective of forensic IT remains unnecessary or even harmful, as long as at the end of the day it leads to the destruction of the materials that had been previously preserved from tampering or destruction. Preserving evidence in its entirety provides the possibility to come back to it and re-assess evidence, if necessary. Conversely, disposing properly preserved evidence before the investigation is over, only to keep some smaller bits of information, appears to be wasteful or even dangerous.

Still, the forensic IT perspective is not the only thing that runs the investigation, and there are at least a few groups of arguments which are raised to justify or demand a pre-selection procedure and wiping out everything that at the time of the pre-selection did not appear to be needed.

1. Scope of the dawn raid

The first argument that can be inferred from the cases discussed earlier assumes that antitrust officials may only take information that is clearly and in fact directly connected to the investigation. This argument also assumes that there is a legal basis to take and attach to the case file only this kind of information, and that to do something more would be to act *ultra vires*.

In my opinion, this is not correct. First of all, and especially from the point of view of the wording of Regulation 1/2003 and Directive ECN+, the powers of antitrust authorities when it comes to examining and copying are wide and provide no clear indication of what exactly may and may not be examined and copied. In fact, this is precisely this issue and the effectiveness of dawn raid powers which first led EU courts to say that the European Commission may examine each document and inspect each piece of furniture, and then also to say, in the case discussed above (this applies to the General Court), that full forensic images can be generated.

It can be argued though, that powers granted to the antitrust authority should be read along with the purpose of the dawn raid. Still, as shown earlier, this is in fact not true as in practice copying irrelevant information takes place anyway, mostly due to the fact that doing otherwise would be impractical or unwelcome because of technical reasons.[43] In other words, there is no universal rule of not copying irrelevant information. At best, there is a principle (which can be weight against other principles) of not copying dispensable information. Such a principle, however, would rather fall under the 'limited to a minimum' argument discussed further, not the 'scope' argument discussed in this section.

In my opinion, the problem with the 'scope' argument is also that it is in practice not a meaningful argument. Let us assume that an antitrust authority would copy to the case file some information which ultimately turns out to be irrelevant for the case in question. The authority would be then able to analyse such information. However, it is unclear what previously not present benefit would that bring to the authority. When it started the dawn raid, the authority was already in a position to examine each document one by one irrespective of its medium, and it could very well encounter this specific information.

A distinction should also be made between factual knowledge and legally admissible evidence. Once a dawn raid starts, it is unavoidable for the authority to learn of many issues that are in fact not at all relevant for the investigation. The whole pre-selection procedure involves reading thousands of pieces of information, which *prima facie* have no direct connection with the grounds for the dawn raid, sometimes including even evidence of other infringements. Still, even if such evidence is copied, it is worth nothing, since the dawn raid concerned a specific investigation. It seems more straightforward to conclude that such evidence is not admissible beyond the scope of the investigation (obviously unless some other legal circumstances make it admissible).[44]

[43] In consequence, it is common to include into the file entire documents, even if only certain passages of such documents hold relevant information.

[44] For instance, a new inspection decision is issued or an *ex post* judicial authorisation for the use of evidence is given. It should be clear that during an ordinary dawn raid such *ex post* authorisation could very well be granted, if something not covered by the warrant is found

To conclude, it is unclear what specific damage and what legal interest is protected by requiring a pre-selection procedure and copying only bits of information. The authority may still obtain factual knowledge on matters not connected to the issue which provided grounds for the dawn raid. If, on the other hand, things go further and some information is attached to the case file, it does not necessarily mean that it should be admissible in another investigation.

There is finally the relevance and 'technical entirety' problem, discussed earlier. The relevance of certain information for the investigation is highly subjective and difficult to assess at the early stage of the investigation. It may be easily argued that preserving for the investigation a forensic image of a whole data carrier (*e.g.* a laptop hard drive) goes beyond what is necessary. After all, courts are used to see specific pieces of evidence when hearing appeals from infringement decisions (e.g. specific emails or documents). However, at the early stage of the investigation things might be different. If one aims at collecting only basic information then maybe a full forensic image is not indispensable, however, the digital age leaves far greater possibilities than simply examining the contents of e-mails. In consequence, a full forensic image might very well constitute relevant information in its 'technical entirety', not shredded into pieces.[45]

What appears to be a problem with digital evidence in antitrust investigation is what I would call the 'filing cabinet fallacy'. It might be tempting for some to say that electronic data carriers are nothing more than a certain type of a filing cabinet. A filing cabinet can store documents and when antitrust officials raided business premises in the past, they were expected to look through filing cabinets and pick relevant documents, not simply seize whole filing cabinets. This, however, is a fallacy as electronic data carriers are far more than simply filing cabinets capable of storing more documents than all filing cabinets in the raided location. If a document containing certain information is stored in a filing cabinet, it nevertheless preserves its entirety and its contents cannot

---

at the premises. It should also be recognised that once such a situation occurs, the authority cannot simply 'close its eyes' and pretend that nothing has been seen. It would be unreasonable to say that if an authority conducts a search in connection with e.g. human trafficking, it is not in a position to preserve evidence of a murder if, during the first search, evidence of another crime is found.

[45] To put the above-mentioned into layman terms, let us imagine that investigators find at a crime scene a jacket covered in blood ('technical entirety'). Obviously, samples of blood can be extracted from the jacket and analysed. Still, it is unlikely that once some blood samples ('relevant evidence') will be extracted, the jacket itself will be disposed of. After all, at the later stage of the investigation it may turn out that further analysis is needed as the jacket might have included blood stains of more than one person or other, previously unknown biological evidence.

be manipulated. Still, it is the data carrier (or rather, a certain pattern of a binary code which starts at point X and ends at point Y) which forms such an entirety, with specific bits of information being placed in a unique place in the memory and having their own properties. For instance, deleted data can be extracted from a data carrier (or a full forensic image of such a data carrier). Still, once such data is recovered and preserved in a new environment it is no longer 'deleted data'. The issue of how and when the data carrier has been used by the user is of interest in the digital world, while indeed it might be neither possible to extract data on how often drawers in the filing cabinet were opened nor that important to establish relevant facts.

Some pieces of information stored on a data carrier can be easily and quickly deemed to be relevant and can be extracted. Still, some pieces of information might require an in-depth analysis, cross-comparisons with evidence gathered in other searched locations. In my view, it is unreasonable to prevent the investigating authority from attaching to the case file an entire calendar or a ledger simply because some of its contents do not *prima facie* appear relevant. The ledger is attached as it forms an entirety and since some part of it contains relevant information, the entire ledger can serve as evidence. The issue with data carriers is that since they contain much more data, they may also contain more irrelevant data. Still, it is the nature of the digital age that data volumes grow exponentially. The bare fact that more irrelevant data can be potentially stored on a data carrier does not justify saying that the data carrier as an entirety cannot serve as evidence.

2. Analysing digital evidence as an 'act of searching'

In the Polish case discussed earlier, the court concluded that the fact that information can be stored on various mediums should not affect the way it is handled.[46] In consequence, if there is a document stored on a data carrier, it is the document that should be copied not the data carrier. In the same case, the court pointed out that the antitrust authority had been equipped with forensic software and hardware which could have been used to make a selection of information, and that in any case the authority could have requested assistance of external forensic experts to make a pre-selection.

In my opinion, such an approach amounts to the 'filing cabinet' fallacy mentioned earlier. To briefly expand on this, the fact that specific information can be extracted from a data carrier does not mean the data carrier is not connected to the investigation and cannot be copied in its 'technical entirety'.

[46] Ref. no XVII Amz 15/17 (*Calypso I*).

It should be clear that when searching officers encounter, at the searched premises, a notebook or ledger, they should be in a position to either seize them or copy them in their entirety. It is neither factually correct nor intuitive to say that searching officers 'search' a notebook when they flip pages.

Technical progress and new technologies made it possible for investigating authorities to generate forensic images of data carriers and to subsequently extract strings of information for presentation purposes, but this should not divert one's attention from the fact that, as discussed earlier, irrelevant information is always copied during a dawn raid.[47]

It should also be pointed out that basing legal arguments on factual capabilities of a given antitrust authority should not be encouraged. Antitrust authorities are empowered under applicable legislation to conduct searches, and it should be clear that a default option when it comes to securing evidence such as data carriers is seizing them. Obviously, if an authority is properly equipped, it may instead decide to make a full forensic copy of a data carrier. If financial resources allow it, then the authority may purchase equipment that provides opportunities which go further than generating forensic images. Still, such capabilities constitute a factual alternative and should not affect the normative level – the authority should always be able to choose the default option. Since seizing objects could be deemed to constitute a typical searching power, and presenting to the court physically seized objects a viable way of providing evidence, there should be nothing to prevent generating a full forensic image and preserving it as an entirety.

3. Just the minimum?

Another argument for conducting pre-selection procedures assumes that a pre-selection should take place since the authority should take only what is indispensable, as doing otherwise would entail going beyond what is necessary to conduct the investigation.

The problem with this argument is that it rests upon a principle rather than on any clear-cut rule. Principles by their very nature can be weighed against other principles, for instance, the effectiveness principle.

It can obviously be argued that some data covered by a full forensic image of a data carrier is not indispensable and, hence, should not be taken, for example, system files will rarely serve an important role in antitrust

[47] In consequence, if one agrees that such irrelevant information can be copied in case of physical evidence (e.g. a document with some information relevant and some information not relevant), there are in my view no meaningful legal reasons to take a different approach in relation to data carriers.

investigations. Still, while it can be argued that such data will likely not prove to be useful, separating it from other information might in practice prove to be more cumbersome than the benefits coming from such an operation.

Other arguments, such as those concerning unclear boundaries of what is relevant and what is not also apply, same as the 'technical entirety' issue.

If it is determined that data carriers cannot constitute a technical entirety and digital evidence on their own, the problem follows that any piece of information extracted from a data carrier can be argued to be irrelevant. While this is not a real issue when it comes to EU law (as discussed earlier, EU courts assume that 'decisions' on the relevance of information cannot be immediately challenged), national laws may differ. In practical terms, this means that each and every piece of information extracted from a data carrier can be argued before the court not to be indispensable for the investigation. Considering how much information electronic data carriers may store, it is questionable whether judicial systems can sustain such reviews and whether judicial bodies are, in fact, in a position to make well-advised decisions that something is irrelevant for the investigation. Moreover, as mentioned before, it is unclear why such a relevance judgment turns out to be advisable in relation to digital data carriers, while similar relevance judgments are not expected when it comes to pieces of documents. After all, same as only relevant information can be extracted from a data carrier, only relevant information can be copied from a document, with other information being omitted.[48] Still, it would be unreasonable to argue that only passages of documents can be copied.

4. Pre-selection and legal privilege protection

Pre-selection can be deemed to be necessary as a tool needed to properly protect legally privileged information. Indeed, if a full forensic image is generated and a data carrier subject to this process contains legally privileged information, then such information will be part of the forensic image. The pre-selection procedure may then serve as a tool to find and remove legally privileged information from the dataset which will be attached to the case file.

However, such a process is not without a cost, as any newly generated dataset will not form the 'technical entirety' identical to the one encountered at the raided premises.

Another issue is that a pre-selection procedure may not effectively reveal that some allegedly privileged information was in fact not covered by the privilege. For instance, during pre-selection, the antitrust officials may

[48] This is even more true in the area of antitrust law where case files are swamped with 'non-confidential' versions of documents with some information being omitted or blacked-out.

encounter some correspondence with an external lawyer and upon request decide not to take it. Still, once the dawn raid is over and case handlers start a full analysis of the evidence, the analysis may very well show that while the external lawyer sometimes provided legal assistance, he or she sometimes also facilitated collusion, which was discussed in some other communication by co-conspirators.[49] With the original forensic image already wiped there is no way to recover the previously preserved evidence. While this is not a fundamental issue and a problem in each investigation, it is something that cannot be discarded when it comes to effective enforcement and the proper use of forensic IT capabilities.

On the other hand, from the legal perspective, it is necessary to develop a procedure not to have legally privileged information available to the investigating authority at all times. A proposal in that respect is made in Section VII.

5. Pre-selection and private information

Similarly to the 'legal privilege' argument, the privacy argument assumes that pre-selection is needed to protect a specific kind of information, in this case private information. However, the important difference is that privacy is not subject to such strong legal protection as legally privileged information. While searching officers will only have a cursory look at information held to be legally privileged, nothing of a similar kind applies to private information. As explained earlier, it is clear that searching officers may go through each piece of furniture and enter any room (and this applies also to dawn raids at homes where the accumulation of private information might be higher than on corporate premises).

It should also be pointed out that pre-selection procedures are typically not about finding private information so that it can be excluded, but putting the antitrust authority in a position of looking for relevant pieces of information and making quick relevance judgments, so that as a by-product information held to be private is not taken. In fact, however, there is no obligation on the part of any antitrust authority to use forensic IT software or any specific e-discovery method. Looking at each piece of information one by one is a viable relevance judgment method, which ultimately leads to a list of pieces of information which seem more and less relevant.[50] In fact, this is precisely

[49] See a similar case outside the area of antitrust heard by the European Court of Human Rights: ECHR judgment of 18.03.2014, Application no. 24069/03, 197/04, 6201/06 and 10464/07, *Öcalan v Turkey*. See also: Andersson, 2018, p. 192.

[50] In consequence, I disagree with R. Polley who believes that even provisional copying of large data volumes is problematic, since an antitrust authority may then use broad search terms

what happens in the 'non-digital' world, as there is no way to use keywords or queries to search a room.

In consequence, it is not clear how exactly are privacy issues alleviated by excluding private information from a forensic image.[51] If privacy concerns arise, then that is so in relation to third parties, rather than antitrust authorities since the latter are anyway in a position to analyse the collected information. Still, concerns in relation to third parties can be mitigated either by not placing forensic images directly in the case file which is available to third parties (as it was discussed in relation to Poland) or by employing adequate access to file rules.

VII. Alternatives

There are two conflicting interests when it comes to the use of forensic IT in antitrust investigations.

From the point of view of forensics, it is always best to preserve data in its original form which was encountered at the time of the dawn raid. If data is stored on a data carrier that is found at the dawn raid location, generating a full forensic image of such a carrier ensures that the data comes in its 'technical entirety' without any interference. When it comes to analysing digital evidence, it is preferable to put evidence together to see the whole picture, rather than look at each piece of information in isolation. It is also preferable not to wipe properly preserved digital evidence, simply because a quick, week or two long, pre-selection process took place. Doing so is similar to destroying original evidence, once a few samples were extracted with no possibility of re-examination or showing once again step-by-step how samples were actually extracted from this specific piece of evidence.

From the point of view of the suspected entity, on the other hand, it is always best to prevent as much information as possible from being attached to the file. And indeed, such information should not be attached, if there

---

and artificially 'extend' the scope of the search. I believe that an antitrust authority could very well inspect each piece of information one by one, which in turn means that any keywords-related arguments are not well-founded. See: Polley, 2013, p. 13.

[51] It is also possible that private communication can serve as evidence of an antitrust offence (e.g. the antitrust authority knows about a certain collusive meeting at a specific location – at the same time a manager mentions in private correspondence with a spouse that he or she is attending a meeting at the very same location, confirming, therefore, indirectly that he or she took part in a collusive meeting).

are meaningful legal reasons not to do so. Legally privileged information constitutes the most important issue.

The question is whether both perspectives can be brought together, with both types of interests being properly addressed. In my opinion, it is possible to develop a procedure in which digital evidence is preserved and available for re-examination with proper fundamental rights safeguards being nevertheless in place.

It is possible, for instance, that once digital evidence is collected, evidence is not wiped until the end of the legal proceedings (administrative or judicial). Still, if such evidence covers, for instance, legally privileged information, then the first step is to locate such privileged information, either within the framework of a continued inspection or a separate procedure. Once such disputed information is located, all remaining information is released to the authority, so that it can analyse it in a way it finds suitable. The original digital evidence, however, is not wiped after the process. Rather it is sealed or deposited with an independent party (e.g. the court).

If during the investigation it turns out that the original digital evidence could have included something that should have been released to the authority, then the authority could request a re-examination of the original evidence. Likewise, if during judicial proceedings the court found it necessary to check a piece of information presented by the authority against the 'technical entirety' from which it had been extracted, it would be in a position to do so, which would also have a positive effect on due process.[52]

Depending on the type of jurisdiction and leeway available under applicable legislation, the approach outlined above may require legislative changes or may come about through case law developments. Overall, however, I believe that neither the language of Regulation 1/2003 nor Directive ECN+ prohibit such an approach, as they speak broadly about what may constitute evidence. The way evidence is then handled, especially in relation to legally privileged information, which may constitute a part of some piece of evidence, can be adjusted through soft law and judicial scrutiny. None the less, it should also be clear that legislative changes in the discussed area, in particular in relation to the procedure of re-examination of a sealed or deposited forensic image, would provide more transparency and legal certainty.

[52] While the issue of the authenticity of digital evidence has not been yet subject to much discussions in the area of antitrust, it is still an issue which has already appeared in the case law, see: CJEU judgment of 26 September 2018, Case C-99/17 P *Infineon*, ECLI:EU:C:2018:773, para. 57.

VIII. Conclusion

The hunt for digital evidence in antitrust cases will continue as more and more information on events and actions is preserved digitally. European antitrust enforcement adapted to the digital world by embracing forensic IT as a tool fostering investigations.

However, the way forensic IT is used is ambiguous and not always driven by the goal of making full use of the new capabilities. On the one hand, the unique nature of the forensic process has been recognised by allowing the generation of full (or wide) forensic images, so that they can be subsequently investigated. On the other hand, the true potential of forensic IT appears to be limited by an unwillingness to go beyond a simple transposition of the standards of the past to the new reality of digital investigations. With ever growing volumes of data, investigating authorities need sufficient time to analyse evidence and cross-reference it. In that regard, pre-selection procedures, which aim at making quick relevance judgments on specific pieces of information and on wiping all remaining information, are something that in my opinion puts an obstacle to making investigations truly digital and ripe for a new age of enforcement.

Since one of the interests served by pre-selection procedures is protecting legally privileged information, alternative ways of doing so can be developed. One of such routes would be to preserve originally collected digital evidence and have an option of re-examination, but at the same time to seal such original evidence or deposit it with a third party, if legally privileged information is covered by a given piece of evidence. More detailed rules on the admissibility of evidence would also be advisable. In consequence, antitrust authorities could make meaningful use of their capabilities to analyse and preserve digital evidence, but at the same time procedural rights of suspects would not be endangered.

Literature

Andersson, H. (2018). *Due Process Aspects on the European Commission's Dawn Raid Practices*. Hart Publishing, https://doi.org/10.5040/9781509920181.

Geradin, D. and Kuschewsky, M. (2013). *Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges*, Tilburg Law School Legal Studies Research Paper Series No 020/2013, https://doi.org/10.2139/ssrn.2341232.

International Competition Network (2014). *Anti-Cartel Enforcement Manual: Chapter on Digital Evidence Gathering*.

Michałek, M. (2015). *Right to Defence in EU Competition Law: The Case of Inspections*. Warsaw: University of Warsaw Faculty of Management Press.

Organisation for Economic Co-operation and Development (2018a). *Investigative Powers in Practice: Unannounced Inspections in the Digital Age* (DAF/COMP/GF(2018)7).

Organisation for Economic Co-operation and Development (2018b). *Investigative Powers in Practice – Contribution from the European Commission* (DAF/COMP/GF/WD(2018)25).

Polley, R. (2013). *Digital Evidence Gathering in Dawn Raids – A Risk for the Company's Rights of Defense and Fundamental Rights*. 20th St. Gallen International Competition Law Forum ICF.

Van der Woude, M. (2019). *Keynote Speech*, Chillin'Competition Conference.