Competition inspections in the digital age: Lessons from the recent case law

Yves Botteman
yves.botteman@nortonrosefulbright.com
Partner, Norton Rose Fulbright, Brussels

Yves is a Belgian/EU competition lawyer based in Norton Rose Fulbright's Brussels office. He focuses on EU and national merger control, as well as cartel and antitrust investigations. He is recognised for securing favourable outcomes in proceedings before the European Commission and national competition authorities. His litigation experience includes representing clients in high-profile follow-on damages and competition disputes in national courts. Yves advises clients on abuse of market dominance, distribution network design, and supply chain management. He has particular experience in the digital and publishing sectors, helping clients navigate the evolving regulatory landscape shaped by the Digital Markets Act and Digital Services Act. He also assists clients in developing antitrust-compliant sustainability collaborations while mitigating greenwashing risks. In addition, Yves provides practical, hands-on guidance on designing and implementing antitrust compliance programs and conducting audits at both the company and trade association levels. His industry experience spans renewable energy, news media and streaming services, consumer products, chemicals and agro-biotechnology, electric mobility, aviation, and aerospace.

Lisa Sopena
lisa.sopena@nortonrosefulbright.com
Associate, Norton Rose Fulbright, Brussels

Lisa Sopena is a Paris/Brussels-qualified antitrust and competition law associate in the Brussels office of Norton Rose Fulbright. Lisa advises on all aspects of EU competition law, including cartel investigations, abuse of dominance, merger control, foreign direct investment screening, regulatory matters and compliance programs. She has a particular focus on competition litigation. Lisa has successfully represented clients before the European Commission, national competition authorities and national courts, securing favourable outcomes, and has been involved in proceedings before the Court of Justice of the EU. Her experience spans a broad range of sectors including renewable energy, sports, digital markets, agriculture and food. Lisa gained experience in the antitrust and competition departments of leading international law firms in Brussels and Paris, as well as at the French Competition Authority (Legal Service) in Paris.

Abstract

Competition authorities are increasingly adapting their investigative methods to a business environment shaped by cloud computing, mobile devices, instant messaging applications and the growing use of AI. In the context of the ongoing revision of Regulation 1/2003, this article explores the legal and practical challenges facing both businesses and competition authorities in the digital age. It examines how these technological developments are transforming the detection of potential infringement and the conduct of competition inspections, and also analyses the recent case law illustrating how the EU Courts are seeking to strike a balance between effective competition enforcement and the protection of fundamental rights.

1. Over the past decade, competition inspections have undergone a profound digital transformation. As businesses increasingly rely on cloud-based storage, mobile devices, messaging applications and digital collaborative platforms to conduct their day-to-day activities, competition authorities have adapted their investigative toolbox. Yet the digitalisation of competition inspections is not without challenges and debate. As authorities gain access to ever-larger volumes of electronic information, questions have emerged on the appropriate scope and limits of their investigative powers and the safeguards necessary to protect fundamental rights. Issues relating to proportionality, the protection of personal data, legal professional privilege and the distinction between professional and private information have become prominent in both enforcement practice and litigation.

2. EU and national courts have been called upon to delineate the boundaries of competition authorities' investigatory powers and clarify the safeguards applicable. The European Court of Justice's (the "Court") recent judgment of 16 July 2026 in *Imagens Médicas Integradas (IMI) and Synlabhealth II* forms

part of this trend, raising questions surrounding the protection of personal data in the context of a dawn raid.[1]

3. This article explores how technological developments are reshaping competition investigations. It first examines the use of AI-driven and data analytics screening tools, before turning to the rise of mobile-device scrutiny during dawn raids. The article then analyses the evolving legal framework governing the collection of digital evidence, with a particular focus on how the EU Courts apply existing principles to the digitisation era, seeking to strike a balance between effective competition enforcement and the protection of fundamental rights. Finally, it considers the implications of these developments in the context of the ongoing revision of Regulation 1/2003.

4. The fast-changing digital landscape underscores the importance for companies and practitioners of ensuring that dawn raid preparedness, compliance programmes and data governance policies keep pace with the rapidly evolving reality of competition investigations.

I. Growing use of AI and data analytics: The *Michelin* case as a window into modern investigative techniques

5. The digitalisation of competition enforcement is not limited to the conduct of inspections itself; it is also shaping the inception of investigations. In this respect, the *Michelin* case provides valuable insights into the European Commission's (the "Commission") investigative toolkit and highlights the growing role of AI and data analytics in antitrust enforcement.[2]

6. The case, which concerned alleged price coordination in the market for replacement tyres for passenger cars and trucks in the European Economic Area (EEA), originated from the analysis of large volumes of publicly available information, including earnings calls. Using linguistic and statistical techniques, the Commission screened those public communications for recurring language patterns potentially indicative of price signalling or information exchange. In particular, it employed bigram frequency analysis – a technique used to measure the frequency of recurring two-word combinations in a text – to detect expressions associated with pricing intentions, market behaviour and competitors.

II. From laptops to smartphones and messaging applications: The rise of mobile-device scrutiny

7. While dawn raids traditionally focused on emails, paper records and desktop computers, competition authorities are now generally examining mobile devices and messaging applications as important sources of evidence.

8. The Commission's 2024 investigation into International Flavors & Fragrances (IFF) offers a useful example.[3] During an inspection carried out at IFF's premises, Commission officials reviewed certain employees' mobile phones and later discovered that WhatsApp messages containing business-related information exchanged with a competitor had been deleted after the inspection had commenced. Although IFF promptly acknowledged the facts and cooperated fully with the Commission, including by assisting in the recovery of the deleted messages, the case nevertheless highlights the heightened scrutiny that authorities now place on mobile communications during inspections.

9. The Commission's growing focus on mobile devices and messaging applications is also reflected in a more recent enforcement decision. In its 2025 *Delivery Hero/Glovo* decision, the Commission relied extensively on evidence derived from a wide range of communication channels, including emails, phone calls, but also WhatsApp messages and other instant messaging applications.[4] The decision revealed that senior executives used these platforms to coordinate no-poach arrangements and market allocation, and to exchange other commercially sensitive information.

10. More broadly, these investigations reflect the reality that modern business communications often take place through messaging and collaboration platforms such as WhatsApp, Teams, Slack and other similar applications. WhatsApp, for example, was originally designed as a personal messaging application but is today commonly used for professional

1 CJEU, 16 July 2026, *Imagens Médicas Integradas and Synlabhealth II*, joined cases C-258/23 and C-259/23, EU:C:2026:585.

2 GCEU, 9 July 2025, *Compagnie générale des établissements Michelin v. Commission*, case T-188/24, EU:T:2025:686.

3 Eur. Comm., decision C(2024) 4256 final of 24 June 2024, *IFF – deletion of data*, case AT.40882.

4 Eur. Comm., decision C(2025) 3304 final of 2 June 2025, *Food Delivery Services*, case AT.40795.

communications in many sectors and organisations. This evolution presents particular challenges because the boundary between professional and personal communications is often blurred, in particular with flexible working arrangements, remote working and the use of personal devices for professional purposes (and vice versa).

11. Beyond the specific infringements at issue, these cases illustrate how modern business communications increasingly take place outside traditional corporate email systems and how competition authorities are adapting their investigative techniques. Messaging applications have become a primary source of evidence capable of documenting anti-competitive conduct. Moreover, any attempt to delete potentially relevant information after the start of an inspection is unlikely to escape detection and may expose companies to significant risks. Importantly, as further discussed below, companies should bear in mind that even private devices may fall within the scope of an inspection where they are used for professional purposes.

III. Drawing limits to the collection of digital evidence?

12. The growing importance of digital evidence has not only expanded the scope of competition inspections but has also intensified the debate surrounding the protection of fundamental rights during dawn raids, in particular as authorities gain access to ever-larger volumes of digital information.

1. The *Meta* judgment

13. An important precedent for this debate is the General Court's 2023 *Meta* judgment.[5] In the context of an investigation into alleged abuse of dominance and tying practices, the Commission requested Meta to run an extensive keyword search across its internal systems using around 3,100 search terms, such as "for free," "advantage," "quality," or "looked at." The exercise generated more than one million potentially responsive documents, many of which allegedly contained sensitive personal information relating to employees and executives.

14. The case provided one of the first opportunities for the EU Courts to examine the legality of large-scale requests for information based on digital search terms. The General Court reaffirmed that the Commission enjoys broad powers to request information that it may reasonably consider necessary for the purposes of its investigation. The judgment is particularly noteworthy in this respect as the General Court upheld the Commission's request despite certain search terms being arguably vague and capable of capturing substantial volumes of irrelevant material. According to the General Court, the potentially broad nature of some search terms did not affect the overall legality of the request, provided that other search terms were sufficiently precise to satisfy the necessity requirement.

15. At the same time, the General Court acknowledged that extensive keyword searches may interfere with the rights to privacy and data protection protected under Articles 7 and 8 of the Charter of Fundamental Rights of the EU (the "Charter"), although such interference does not in itself render a request unlawful. In this context, the General Court attached particular importance to the safeguards implemented by the Commission, including the refinement of search terms during the procedure and the establishment of a virtual data room for documents containing sensitive personal data to be reviewed under controlled conditions. Under this procedure, the documents were accessible only to a limited number of Commission officials and Meta's counsel and were reviewed to determine whether they were relevant to the investigation and should therefore be included in the Commission's file. Meta's counsel were also given the opportunity to contest the relevance of documents and explain the reasons for their objections, with a dedicated mechanism in place to resolve any continuing disagreements.

16. Against this background, the *Meta* judgment suggests a willingness on the part of the General Court to accept increasingly sophisticated and data-intensive digital investigative techniques, even where they may capture significant volumes of irrelevant information or personal data, so long as the necessary safeguards designed to mitigate the impact on fundamental rights are in place. The underlying rationale is precisely to prevent competition authorities from engaging in impermissible "fishing expeditions," requiring them to define the scope of the requests by reference to appropriate material, geographic and temporal criteria.

17. A similar approach can be observed in the General Court's recent judgments in the context of a merger control investigation.[6] In these cases, the Commission required the parties to produce documents, including stored on personal devices and applications where these had been used at least once for professional purposes. While acknowledging that such requests entailed a serious interference with the right to privacy, the General Court held that the interference was justified by the objective of ensuring the effective enforcement of competition law and merger control rules. It emphasised that the requests were limited to specific custodians, covered a defined time period and relied on predefined search terms aimed at capturing

[5] GCEU, 24 May 2023, *Meta Platforms Ireland v. Commission*, case T-451/20, EU:T:2023:276; appeal proceedings pending under case C-497/23 P.

[6] GCEU, 3 June 2026, *Vivendi v. Commission* and *Lagardère v. Commission*, cases T-1097/23 and T-1119/23, EU:T:2026:355 and EU:T:2026:356; appeal proceedings pending under cases C-862/26 P and C-861/26 P.

the material and geographic scope of the Commission's identified competitive concerns. In addition, the Court attached importance to the existence of procedural safeguards, including the protection of confidential and privileged information, and the availability of judicial review. As a consequence, the General Court's rulings further illustrate the wide scope of competition authorities' powers to collect and review private information, including information stored on private devices used only occasionally, or even once, for professional purposes.

18. Whether this broad approach to digital evidence gathering, within the limits imposed by the prohibition of "fishing expeditions," will ultimately be upheld by the Court of Justice remains to be seen, however, as appeals are currently pending. The subsequent judgment in *IMI and Synlabhealth II* can therefore be seen as a continuation of this debate, this time in the specific context of emails and devices seized during national competition inspections.

2. The *IMI and Synlabhealth II* judgment

19. Much like in the *Meta* case, the Court was required to reconcile the broad investigatory powers of competition authorities with the rights to privacy and data protection. The Court confirmed that even professional communications exchanged through a company's email system are protected under Article 7 of the Charter, as they may contain personal information. Importantly, however, the Court reaffirmed that the existence of such personal data does not, in itself, prevent authorities from accessing or reviewing the information as competition inspections pursue the legitimate objective of enforcing competition law.

20. In reaching that conclusion, the Court recalled that competition authorities' investigatory powers are circumscribed by a number of procedural safeguards, designed to prevent abuse and arbitrariness, including the exclusion of non-business documents from the scope of the investigation, the protection of legal professional privilege and the requirement to provide reasons for the inspection decision. Relying on the case law of the European Court of Human Rights (the "ECtHR"), it further emphasised that prior judicial authorisation is not a prerequisite, provided that effective *ex post* judicial review is available to challenge both the inspection decision and the measures implemented during the dawn raid.

21. From an enforcement perspective, the judgment largely validates existing practices and seeks to preserve national competition authorities' ability to collect and review professional emails without prior judicial authorisation. The more novel—and potentially far-reaching—aspect of the judgment concerns access to data contained in employees' privately owned devices that are also used for professional purposes. The Court held that access to such data must, "*where appropriate*," be subject to prior review by a court or an independent administrative body to ensure proportionality. The Court recognised that such devices are likely to contain sensitive personal information, such as location data, photographs, internet browsing history and private communications. Access to such information may enable competition authorities to draw precise conclusions regarding an individual's private life and therefore result in particularly serious interferences with the rights to privacy and protection of personal data.

22. While the underlying objective is understandable, the judgment offers little guidance as to when prior review will be considered "appropriate." If the presence of personal data is the relevant criterion, should such review then become the norm whenever competition authorities seek access to devices used for both private and professional purposes? The Court's analysis is somewhat difficult to reconcile with the realities of modern working environments, as it focuses only on privately owned devices also used for professional purposes. In doing so, it creates a distinction with mobile devices owned by the employer and used by employees for both personal and professional purposes. In both situations, the device is likely to contain the same categories of private information and give rise to comparable risks for privacy and data protection. Arguably, the same level of protection should therefore apply, without distinction, to any mobile device used for both purposes, irrespective of whether it is owned by the employer or the employee.

23. Equally uncertain is what qualifies as an "independent administrative body" and at what stage the review should take place. Combined with the lack of harmonised rules governing competition inspections across the EU, these uncertainties make it difficult to predict the extent to which the judgment will affect inspection and enforcement practices.

IV. The ongoing revision of Regulation 1/2003: Expanding powers, strengthening safeguards

24. The balance between effective enforcement and the protection of fundamental rights is likely to remain a key source of debate, even more so in the context of the revision of Regulation 1/2003.

25. Regulation 1/2003 establishes the procedural framework governing the enforcement of Articles 101 and 102 of the

Treaty on the Functioning of the European Union (TFEU) by the Commission and underpins many of its core investigative tools, including requests for information, interviews and dawn raids. Following more than twenty years of application, the Commission launched a review of the framework in 2025 to assess whether these tools remain fit for purpose in an increasingly digital economy. The review is intended, among other things, to ensure that antitrust enforcement keeps pace with the realities of modern business practices and technological change.

26. A central theme of the reform is the possibility of adapting inspection powers to environments where relevant evidence is more commonly stored on cloud infrastructure, spread across digital platforms and accessible remotely. In particular, the Commission is considering the potential introduction of digital or partially remote inspections, which could enable competition authorities to access and review certain categories of information without being physically present at the inspected premises. While such mechanisms could improve efficiency and reduce disruption to businesses, they also raise legitimate concerns regarding data protection, confidentiality, trade secrets and rights of defence. As a result, many stakeholders have called for clear procedural rules and appropriate safeguards to accompany any expansion of digital investigative tools.

27. In this context, the *IMI and Synlabhealth II* judgment illustrates the types of tensions that are likely to be more prominent in the years ahead. If competition authorities are granted broader powers to conduct digital or partially remote inspections in the future, questions surrounding the collection, filtering and review of electronic information will become even more acute.

28. For that reason, any expansion of investigative powers will need to be matched by equally robust procedural protections. The protection of personal data, the preservation of legal professional privilege, the proportionality of data collection, the treatment of mixed personal and professional information and the availability of effective judicial oversight are likely to play a central role in shaping the future of competition inspections.

V. Lessons for companies and practitioners

– Antitrust scrutiny no longer arises only from complaints, whistleblowers or evidence uncovered during inspections. Competition authorities are increasingly using AI tools and data analytics to screen publicly available information for potential antitrust concerns. Statements made during earnings calls, investor presentations and industry conferences may therefore become the starting point of an investigation.
– While competition authorities customarily access and review large volumes of digital information during dawn raids, EU Courts signal that robust mechanisms ought to be set up to ensure that fundamental rights remain adequately protected.
– Dawn raid compliance programmes should ensure that employees are aware of the scope of an inspection, which may encompass cloud-based data, laptops, tablets, mobile phones and messaging applications—irrespective of whether the device is private or the messaging and social media apps are predominantly used for private purposes. Particular attention should be devoted to data retention policies and data integrity well before an inspection is about to start.
– Companies should therefore ensure that their dawn raid protocols include clear procedures for dealing with personal data, legally privileged material and mixed-use devices.
– Attempts to delete or alter potentially relevant information during or after an inspection has commenced are unlikely to escape detection and may give rise to significant additional risks.

VI. Conclusion

29. The broader lesson emerging from both the recent case law and the ongoing review of Regulation 1/2003 is that technological evolution almost inevitably requires procedural adaptation. As competition authorities seek to modernise their investigative toolkit and gain access to ever-larger volumes of information, the challenge for legislators and courts will be to ensure that enforcement remains effective without diluting the fundamental guarantees that underpin the legitimacy of competition investigations. ■