L’impact de la conformité au RGPD en droit de la concurrence

Nardi, Aline

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2024

Document Version
le PDF de l'éditeur

L'impact de la conformité au RGPD en droit de la concurrence

Aline Nardi[1]

ABUS DE POSITION DOMINANTE – MARCHÉS NUMÉRIQUES – COMPÉTENCE D'UNE AUTORITÉ DE LA CONCURRENCE NATIONALE POUR EXAMINER LA CONFORMITÉ D'UN COMPORTEMENT AU RGPD – COLLABORATION ENTRE AUTORITÉS DE LA CONCURRENCE ET AUTORITÉS DE PROTECTION DES DONNÉES

ABUSE OF A DOMINANT POSITION – DIGITAL MARKETS – COMPETENCE OF A NATIONAL COMPETITION AUTHORITY TO EXAMINE THE COMPLIANCE OF A CONDUCT WITH THE GDPR – COOPERATION BETWEEN COMPETITION AUTHORITIES AND DATA PROTECTION AUTHORITIES

L'accès et le traitement des données sont devenus des paramètres essentiels de la concurrence sur les marchés numériques. Bon nombre de ces données sont des données à caractère personnel. Ce faisant, les géants du numérique font une lecture particulière du RGPD pour promouvoir leurs intérêts. Cette dernière leur permet tantôt de faire circuler massivement les données à caractère personnel qu'ils détiennent au sein de leurs propres écosystèmes, tantôt de refuser à des tiers l'accès à ces dernières. Une telle pratique renforce la position dominante de ces entreprises sur les marchés numériques et leur permet d'en conquérir de nouveaux. Les autorités de la concurrence se sont récemment interrogées sur la conformité de ces comportements au droit de la concurrence et incidemment au RGPD. Si elles ne sont en principe pas compétentes pour apprécier la conformité d'un comportement au RGPD, même incidemment, la Cour de justice de l'Union européenne a récemment changé sa jurisprudence à ce sujet. Dans l'affaire Meta c. Bundeskartellamt, la Cour leur donne cette compétence, tout en établissant des garanties visant à préserver la compétence des autorités de protection des données. Si un tel arrêt entérine une collaboration déjà bien établie entre autorités dans plusieurs États membres, il promet surtout des analyses plus lucides des stratégies employées par les géants du numérique avec l'espoir de mieux garantir le bien-être des consommateurs européens.

Data access and processing have become essential parameters of competition in digital markets. Much of this data is personal data. Hence, digital giants have adopted a particular interpretation of the GDPR to promote their interests. This allows them both to circulate the personal data they hold on a massive scale within their own ecosystems and to deny third parties access to it. This practice strengthens the dominant position of these companies in digital markets and enables them to conquer new ones. Recently, competition authorities have questioned the compliance of such behaviour with competition law and, incidentally, with the GDPR. While in principle they do not have jurisdiction to assess whether a conduct complies with the GDPR, even incidentally, the Court of Justice of the European Union recently changed its case law on the subject. In Meta v. Bundeskartellamt, the Court gave them this competence, while establishing safeguards to preserve the competence of data protection authorities. While this ruling confirms the already well-established collaboration between authorities in several Member States, it also promises more lucid analyses of the strategies employed by the digital giants, in the hope of better guaranteeing the welfare of European consumers.

[1] L'auteur tient à remercier Antoine Delforge pour sa relecture attentive de la présente contribution.

INTRODUCTION

À l'ère des *Big Data*, l'accès aux données et leur traitement sont devenus un paramètre clé de la concurrence dans les marchés numériques[2]. Face à cette évolution, les géants du numérique – qui détiennent des quantités immenses de données – croisent allègrement ces dernières obtenues via leurs différents services afin de conquérir de nouveaux marchés et de renforcer leur position sur leur marché principal. La nature de ces données n'est pas anodine. Il est souvent question de données à caractère personnel, dont le traitement est soumis au droit de la protection des données et en particulier au RGPD[3].

Ces pratiques ont, ces dernières années, attiré l'attention des autorités nationales de concurrence, nous amenant des affaires telles que celle de Meta face au Bundeskartellamt[4]. Dans cette dernière, le Bundeskartellamt, l'autorité fédérale allemande de la concurrence, condamne l'abus de position dominante de Facebook consistant à croiser les données qu'il recevait de ses services internes et externes avec le compte de chaque utilisateur, au motif qu'un tel traitement est contraire au RGPD. Ce faisant, l'autorité fait un examen incident de la conformité d'un comportement par rapport au RGPD dans le cadre de son analyse en droit de la concurrence. Pourtant, selon la jurisprudence historique de la Cour de justice de l'Union européenne (ci-après « C.J.U.E. »), un tel examen ne relève pas de sa compétence matérielle. Cette position a été vivement critiquée par la doctrine, la qualifiant d'obsolète au vu des récents développements de l'économie numérique[5].

Dans son récent arrêt du 4 juillet 2023[6], la C.J.U.E. opère toutefois un heureux revirement de jurisprudence à cet égard (I).

Les implications de l'arrêt du 4 juillet 2023 dépassent par ailleurs la seule sphère de la circulation massive et du recoupement des données à caractère personnel en interne par les géants du numérique. De fait, ces comportements vont souvent de pair avec une politique « deux poids, deux mesures ». Ainsi, bien que ces grandes entreprises se montrent très libérales dans la circulation de ces données au sein de leurs propres écosystèmes, elles tendent à invoquer le droit de la protection des données pour restreindre l'accès aux données à caractère personnel qu'elles détiennent à des tiers. L'examen incident de la conformité au droit de la protection des données à caractère personnel en droit de la concurrence ayant désormais été avalisé par la C.J.U.E., les doubles standards pratiqués – qui peuvent constituer de potentiels abus anticoncurrentiels – par ces entreprises pourront être appréhendés plus efficacement (II).

I. L'EXAMEN DE LA CONFORMITÉ AU RGPD EN DROIT DE LA CONCURRENCE

Lorsqu'il est question pour une autorité de la concurrence d'examiner la conformité d'un comportement au RGPD dans le cadre d'une analyse en droit de la concurrence, il existe deux approches (A). La première, en défaveur d'un tel examen, a récemment été désavouée par la C.J.U.E. dans un arrêt du 4 juillet 2023 (B). Il s'agit là d'un développement heureux, mais peu surprenant dans la jurisprudence de la Cour (C).

A. Deux écoles de pensée

Historiquement, les institutions européennes ont généralement adopté une approche séparatiste lorsqu'elles étaient amenées à connaître d'affaires mêlant des aspects du droit de la concurrence au droit de la protection des données. Selon cette approche, les questions

2 J. Crémer, Y.-A. de Montjoye et H. Schweitzer, « Competition Policy for the digital era – Final report », 2019, p. 19-24, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

3 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016.

4 Bundeskartellamt, décision B6-22/16, du 6 février 2019, *Facebook*, disponible sur https://www.bundeskartellamt.de.

5 O. Altmayer, « The Tipping Point – Reevaluating the ASNEF-EQUIFAX Separation of Competition of Data Privacy Law in the Wake of the 2017 Equifax Data Breach », *Northwestern Journal of International Law & Business*, vol. 39, 2018, pp. 37-58.

6 Arrêt *Meta Platforms Inc. c. Bundeskartellamt*, 4 juillet 2023, C-252/21, EU:C:2023:537, ci-après « arrêt *Meta* ». Nous n'analyserons cet arrêt que sur les aspects liés au droit de la concurrence, et non ceux liés spécifiquement au RGPD.

liées au droit de la protection des données et au droit de la concurrence sont censées être examinées séparément et, *a fortiori*, par les autorités compétentes dans ces matières. Elle est fondée sur la jurisprudence de la C.J.U.E. dans l'affaire *Asnef-Equifax*, du 23 novembre 2006. La Cour y établit que « les éventuelles questions relatives à l'aspect sensible des données à caractère personnel ne [relèvent] pas, en tant que telles, du droit de la concurrence » et ce faisant, « elles peuvent être résolues sur le fondement des dispositions pertinentes en matière de protection de telles données »[7]. Cette approche a par ailleurs été adoptée par la Commission dans ses décisions autorisant la concentration de Facebook et WhatsApp, en 2014[8], ainsi que celle de Google et de Fitbit, en 2020[9].

Cette position n'est pas exempte de critique, car elle ignore les synergies qui existent entre le droit de la protection des données et le droit de la concurrence[10]. Ces deux corpus de règles protègent la plupart du temps en effet les mêmes personnes : les consommateurs. Ces derniers pouvant également être considérés comme des personnes concernées au regard de la protection des données à caractère personnel, leur bien-être – défendu par le droit de la concurrence – peut être mis en péril dès lors que leur liberté de choix et le contrôle de leurs informations personnelles sont restreints par une entreprise dominante[11].

Dès lors, il est impératif de reconnaître le chevauchement de ces deux disciplines. Dans un monde toujours plus digital, les données à caractère personnel sont une ressource précieuse pour les géants du numérique. Grâce à leur collecte intensive, ces derniers ont acquis un pouvoir économique immense, qui menace la concurrence effective, et *a fortiori* le bien-être des consommateurs, ainsi que la vie privée des citoyens. Ces entreprises commettent des abus qu'il est parfois difficile de condamner avec le droit de la concurrence traditionnel, comme en témoigne l'adoption du *Digital Markets Act*[12] (ci-après « le DMA »). De même, elles se livrent à des pratiques de manipulation informationnelle et comportementale de leurs utilisateurs, en particulier en ce qui concerne le recueil de leurs consentements[13]. Il arrive en effet régulièrement que certains consommateurs acceptent certaines conditions d'utilisation des géants du numérique, faute de concurrence effective dans certains secteurs. De fait, le consommateur est pour ainsi dire obligé d'accepter les conditions d'utilisation des GAFAM, par exemple, chacun d'entre eux étant quasiment incontournable pour une large partie des consommateurs. Les inefficiences dans l'application de ces matières étant particulièrement liées, certains postulent qu'adopter une approche plus intégrée permettrait d'obtenir de meilleurs résultats dans ces deux disciplines[14].

Une nouvelle théorie, dite « intégrationniste », a été développée en réaction aux critiques adressées à l'approche séparatiste. Elle ouvre la porte aux arguments relatifs à la protection des données en droit de

7 C.J.U.E., arrêt *Asnef-Equifax c. Asociación de Usuarios de Servicios Bancarios*, 29 juin 2006, C-238/05, EU:C:2006:734, point 63.

8 La Commission y déclare que « toute préoccupation relative à la vie privée découlant de la concentration accrue des données sous le contrôle de Facebook à la suite de l'Opération ne relève pas des règles du droit de la concurrence de l'UE mais des règles de l'UE en matière de protection des données » (trad. libre) ; décision de la Commission du 29 août 2014, M.7217, *Facebook c. WhatsApp*, para. 164, https://ec.europa.eu/competition/.

9 Bien que plus subtilement, voy. en ce sens S. Vande Walle, « The European Commission's Approval of *Google / Fitbit* – A Case Note and Comment », *Concurrences Competition Law Review*, 2021, https://www.concurrences. com ; décision de la Commission du 17 décembre 2020, M.9660, *Google c. Fitbit*, https://ec.europa.eu/competition/.

10 Pour plus de détails voy. W. Kerber et L. Specht-Riemenschneider, « Synergies between data protection and competition law », 30 septembre 2021, pp. 29-42, https://www.vzbv.de.

11 W. Kerber et L. Specht-Riemenschneider, *ibidem*, p. 36.

12 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (Règlement sur les marchés numériques), *J.O.U.E.*, 12 octobre 2022, L 265 (ci-après « DMA »).

13 A. Gobert, « Les modalités de recueil du consentement en matière de cookies non essentiels : la chasse aux pratiques non conformes menée par la CNIL se poursuit », *R.D.T.I.*, 2022/3-4, pp. 144-158 ; P.-O. Pielaet, « La *privacy by design* à l'épreuve des "*dark patterns*" », *R.D.T.I.*, 2020/3, pp. 33-45.

14 W. Kerber et L. Specht-Riemenschneider, *op. cit.*, p. 5.

la concurrence et inversement. Le contrôleur européen de la protection des données adopte cette position en 2014, dans un avis préliminaire[15]. Il y plaide en faveur de la prise en considération de la protection des données à caractère personnel dans l'examen des activités des entreprises et de leur impact sur la compétitivité, l'efficacité du marché et le bien-être des consommateurs. De même, cette approche a été validée par la C.J.U.E. dans son récent arrêt *Meta* du 4 juillet 2023[16].

B. L'arrêt du 4 juillet 2023 dans l'affaire *Meta c. Bundeskartellamt*

Au vu de l'importance croissante que prennent les données à caractère personnel dans l'économie numérique, il était inévitable que la Cour soit amenée à se prononcer une nouvelle fois sur la question, l'approche séparatiste devenant de plus en plus intenable. L'occasion s'est présentée sous la forme de questions préjudicielles adressées à la Cour dans le cadre de l'affaire opposant Meta, anciennement Facebook, au Bundeskartellamt.

Par une décision du 6 février 2019[17], le Bundeskartellamt a condamné la société américaine Meta, pour une violation du RGPD, laquelle constituait une exploitation abusive de la position dominante de cette dernière sur le marché des réseaux sociaux en ligne. La violation consistait pour Meta à forcer les utilisateurs du réseau social Facebook à accepter que leurs données *off*[18] du réseau social soient traitées, sans consentement particulier. Meta a alors introduit un recours contre cette décision devant l'Oberlandesgericht Düsseldorf, le tribunal régional supérieur de Düsseldorf, en Allemagne. Le tribunal a adressé des questions préjudicielles à la C.J.U.E., lui demandant entre autres de se prononcer sur la compétence d'une autorité de la concurrence nationale pour constater la non-conformité d'un traitement de données à caractère personnel avec le RGPD, ainsi que sur son articulation avec les compétences des autorités nationales chargées du contrôle de la protection des données[19]. En substance, il est donc demandé à la C.J.U.E. d'apprécier si une autorité nationale de la concurrence peut constater, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise, de manière incidente, une violation du RGPD et, le cas échéant, de préciser la portée d'une telle compétence[20].

Dans un arrêt rendu en grande chambre, le 4 juillet 2023, la Cour a confirmé qu'il était parfois nécessaire pour une autorité nationale de la concurrence d'examiner la conformité d'un comportement d'une entreprise au droit de la protection des données à caractère personnel[21]. Elle cite à cet égard la Commission, qui désavoue son approche passée[22]. Selon elle, les données à caractère personnel sont devenues un paramètre significatif de la concurrence. Les exclure de l'analyse des autorités reviendrait ainsi à méconnaitre la réalité de l'économie numérique et emporterait le risque de porter atteinte à l'effectivité du droit de la concurrence[23].

Toutefois, cet arrêt n'est pas un blanc-seing permettant aux autorités de la concurrence de s'immiscer dans les compétences des autorités de contrôle. La C.J.U.E. y définit les limites de l'examen incident par les premières de la conformité d'un comportement au RGPD. Lorsqu'un tel examen est nécessaire, elle impose aux autorités de la concurrence et aux autorités de

15 European Data Protection Supervisor, « Preliminary Opinion of the European Data Protection Supervisor. Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy », 2014, p. 26, https://edps.europa.eu.

16 Arrêt *Meta*.

17 *Bundeskartellamt*, décision précitée.

18 Notons que le terme « données *off* » désigne de nombreux types de données différentes, comme les données concernant la consultation de pages Internet et d'applications tierces et les données relatives à l'utilisation d'autres services en ligne appartenant au groupe Meta, comme Instagram et WhatsApp.

19 Arrêt *Meta*, points 28-30. D'autres questions sont également posées, sur la légalité même de certaines pratiques de Meta au regard du RGPD. Ces autres questions seront analysées dans un futur article de *cette revue*.

20 Arrêt *Meta*, point 36.

21 Arrêt *Meta*, point 48.

22 Dans le même sens, nous pouvons rappeler la création de la *Digital Clearing House* (https://www.digitalclearinghouse.org/) par la Commission européenne. Cette instance composée de régulateurs nationaux en matière de concurrence, droit de la consommation et protection des données visait à permettre une meilleure interaction entre ces différents régulateurs.

23 Arrêt *Meta*, point 51.

contrôle (du RGPD), en vertu du principe de coopération loyale[24], de collaborer entre elles. Concrètement, l'autorité de la concurrence doit en premier lieu vérifier si ce comportement – ou un comportement similaire – a déjà fait l'objet d'une décision par l'autorité de contrôle compétente[25] ou par la Cour. Le cas échéant, elle ne peut s'en écarter, bien qu'elle soit libre d'en tirer ses propres conclusions en droit de la concurrence. En l'absence d'une telle décision, ou lorsqu'elle nourrit des doutes sur la portée de l'appréciation effectuée par l'autorité de contrôle compétente, l'autorité de la concurrence doit la consulter et solliciter sa coopération. Une telle demande permet entre autres de déterminer si l'autorité de la concurrence doit attendre l'adoption d'une décision par l'autorité de contrôle concernée, avant de formuler sa propre appréciation sur la question. Néanmoins, si endéans un délai raisonnable, l'autorité de la concurrence ne reçoit aucune réponse ou objection, elle peut poursuivre sa propre enquête[26].

Précisons que, selon la portée de la « décision » rendue par l'autorité de contrôle sollicitée, il est possible que cette dernière prenne une décision qui, en vertu de certains mécanismes de coordination prévus dans le RGPD[27], doive être elle-même soumise à l'avis des autres autorités de contrôle des États membres sur le territoire desquels l'entreprise concernée est active. Une consultation de cette ampleur est de nature à rallonger le temps qui s'écoulera entre la demande de l'autorité de la concurrence et la « décision » de l'autorité de contrôle. Pourtant, dans les marchés numériques, en évolution rapide, et dans lesquels le basculement d'une entreprise vers une position dominante est potentiellement irréversible, l'intervention des autorités de la concurrence se doit d'être rapide pour être efficace[28]. Les autorités de concurrence risquent ainsi de se trouver dans une position délicate, si l'autorité de contrôle consultée se manifeste mais n'est pas en mesure de rendre une « décision » rapidement. En tout état de cause, dans le cas où l'autorité de contrôle ne remet qu'un avis et ne prend pas formellement une décision (liante), il ne nous semble pas que ces règles de coordination trouvent à s'appliquer.

Sans détailler davantage les enseignements de cet arrêt en matière de protection des données, il convient de souligner que la Cour opère ici un revirement par rapport à sa jurisprudence *Asnef-Equifax*. Elle adopte une approche intégrationniste diligente. Elle reconnaît qu'il est souhaitable de rapprocher le droit de la protection des données et le droit de la concurrence, sans pour autant ignorer le risque d'interprétations divergentes qu'emporte l'examen incident par l'autorité de la concurrence d'une question relevant du droit de la protection des données à caractère personnel. Ce risque est ici mitigé, en renforçant la coopération entre leurs autorités respectives.

Notons que cette coordination entre les autorités n'est pas quelque chose de neuf en soi, et que cette coopération était déjà souvent déjà mise en place.

C. Un revirement peu surprenant de la jurisprudence *Asnef-Equifax*

Si l'approche intégrationniste de la décision du Bundeskartellamt du 6 février 2019 a désormais été confirmée par la Cour, d'autres autorités examinaient déjà la conformité au droit de la protection des données à caractère personnel dans leurs décisions. C'est le cas de l'Autorité française de la concurrence, dans l'affaire *Apple ATT*[29]. Cette dernière concerne un renforcement par Apple de sa politique de la protection de la vie privée par la mise en place d'un dispositif surnommé « *App Tracking Transparence* » (ci-après « ATT »). Ce dernier vise à requérir le consentement d'un utilisateur au suivi de son activité par des services d'entreprises tierces par un système d'*opt-in*, sans que les services d'Apple soient soumis à ce dernier. Apple

24 Consacré à l'article 4, paragraphe 3, TUE, ce dernier impose à l'Union européenne et à ses États membres, y compris leurs organes, de s'assister mutuellement dans l'accomplissement des missions découlant des traités de l'Union.

25 L'autorité compétente pourra être l'autorité de contrôle du même État que l'autorité de la concurrence à l'initiative ou, dans certains cas, celle d'un autre État membre si celle-ci est considérée comme autorité chef de file en vertu de l'article 56 du RGPD (arrêt *Meta*, points 52 et s.)

26 Arrêt *Meta*, points 52-59.

27 Art. 60 et 65 du RGPD.

28 A. De Streel, « Should digital antittrust be ordoliberal ? », *Concurrences*, n° 1, 2020, p. 3.

29 Autorité de la concurrence, décision n° 21-D-07 du 17 mars 2021, points 54-64.

y est donc accusée d'instrumentaliser l'outil ATT, sous couvert de renforcer la vie privée, pour commettre un abus de position dominante. Dans sa décision provisoire du 17 mars 2021, l'Autorité française de la concurrence ne se retranche pas derrière des considérations de compétences matérielles pour rejeter l'examen de la conformité de l'ATT au RGPD, mais l'intègre au contraire à son raisonnement. À cet égard, le *modus operandi* de l'autorité française est précurseur de la procédure fixée par la C.J.U.E. dans l'arrêt du 4 juillet 2023 pour l'examen incident de la conformité d'une pratique au RGPD. Elle fait, en effet, le choix de consulter sur ces questions la Commission Nationale de l'Informatique et des Libertés, (ci-après la « CNIL »), l'autorité de contrôle française en droit de la protection des données à caractère personnel. La CNIL rend ainsi un avis le 17 décembre 2020, sur lequel se fonde largement l'autorité[30]. Précisons que la Cour de justice indique clairement dans son arrêt que la consultation de l'autorité de contrôle nationale n'est pas suffisante si celle-ci n'est pas l'autorité chef de file et que dès lors c'est à cette dernière qu'il faut s'adresser[31].

De même, la *Competition and Markets Authority* (ci-après « la CMA »), l'autorité de la concurrence du Royaume-Uni, et *l'Information Commissioner's Office* (ci-après « l'ICO »), son homologue en droit de la protection des données, ont récemment publié une déclaration conjointe dans laquelle ils expliquent adopter une approche commune et renforcer leur coopération en particulier sur les questions liées au monde numérique[32]. Cette collaboration s'est illustrée récemment dans l'affaire *Google Privacy Sandbox*[33]. À noter que cette tendance s'exprime également hors de l'Europe[34]. En tout état de cause, la jurisprudence *Asnef-Equifax* de la C.J.U.E. était sans aucun doute devenue inadéquate dans un monde numérique où les différents corpus législatifs s'appliquent bien souvent de manière conjointe.

Si la déclaration officielle de la CMA et de l'ICO témoigne déjà d'un commencement de formalisation des relations de coopération entre ces autorités, au sein de l'Union, rien dans la décision de la C.J.U.E. n'indique cependant qu'une procédure doit être mise en place par les États membres pour les organiser. L'Italie, néanmoins, n'avait pas attendu l'arrêt du 4 juillet 2023 pour le faire. Entre les autorités en matière de protection du consommateur et les autorités de contrôle, il existait déjà une obligation de coordination. Ainsi dans une affaire concernant WhatsApp, l'AGCM, l'autorité de la concurrence et de la consommation italienne, avait considéré, après consultation de son homologue, certains agissements comme constitutifs de pratiques commerciales déloyales, notamment en vertu des règles imposées par le RPGD[35].

30 Davantage étudiée ci-après.

31 Dans l'affaire *Meta*, le Bundeskartellamt avait bien contacté tant l'autorité de contrôle compétente allemande qu'irlandaise (autorité chef de file).

32 Competition and Markets Authority et Information Commissionner's Office, « Competition and data protection in digital markets: a joint statement between the CMA and the ICO », 19 mai 2021, pp. 3-30, https://assets.publishing.service.gov.uk.

33 Le projet « *Privacy Sandbox* » qu'entend implémenter Google consiste à désactiver les cookies de tiers sur son navigateur Chrome et son moteur de navigation Chromium, afin de les remplacer par un nouvel ensemble d'outils de ciblage de la publicité et d'autres fonctionnalités, qui protégeraient davantage la vie privée des utilisateurs. En raison de plusieurs plaintes reçues à cet égard, la CMA a mené une enquête à l'issue de laquelle Google s'est proposé de prendre des engagements. En sus de ces derniers, la CMA et l'ICO ont décidé de conjointement participer à l'élaboration du projet *Privacy Sandbox* de Google afin de garantir des résultats efficaces pour les consommateurs et de protéger à la fois la concurrence et la vie privée ; X, « CMA to investigate Google's "Privacy Sandbox" browser changes », Communiqué de presse, https://www.gov.uk/government/news/ (consulté le 28 janvier 2023) ; X, « CMA to keep "close eye" on Google as it secures final Privacy Sandbox commitments », Communiqué de presse, https://www.gov.uk/government/news/ (consulté le 28 janvier 2023).

34 Voy. not. le *Consumer Data Right* conjointement mis en œuvre par l'autorité de la concurrence australienne (ACCC) et l'autorité de protection des données australienne (OAIC), qui entend implémenter une libre circulation des données à caractère personnel pour stimuler la concurrence tout en assurant le respect à la vie privée.

35 En Italie, cette coordination est même prévue dans leur Code de la consommation (art. 27.1*bis*). Pour plus d'informations sur cette affaire, voy. not. N. Zingales, « Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law », *Computer Law & Security Review*, vol. 33, 2017, pp. 553-558.

II. LA MISE EN CONFORMITÉ AU RGPD EN TANT QUE PRATIQUE ANTICONCURRENTIELLE

La portée de l'arrêt de la C.J.U.E. du 4 juillet sur les relations entre les autorités de la concurrence et les autorités de contrôle dépasse largement la situation d'une violation du RGPD en tant que pratique anticoncurrentielle. Comme l'illustrent les affaires *Apple ATT* et *Google Privacy Sandbox* (A), les géants du numérique ne se contentent pas de faire circuler massivement les données à caractère personnel en interne, comme dans l'affaire *Meta*, ils s'emploient également à restreindre l'accès à de telles données à des entreprises tierces sous couvert de respecter le droit de la protection des données à caractère personnel, en particulier le RGPD. Cette pratique d'un double standard leur permet de renforcer les effets des stratégies d'enveloppement, dans leur conquête de nouveaux marchés (B). L'avènement de l'approche intégrationniste par la C.J.U.E. permet ainsi d'appréhender ces pratiques de manière holistique (C).

A. L'instrumentalisation du RGPD dans les affaires *Apple ATT* et *Google Privacy Sandbox*

L'affaire *Apple ATT*, évoquée ci-avant, incarne pleinement la politique « deux poids, deux mesures », pratiquée par les entreprises détenant des quantités immenses de données. Si l'affaire *Meta* illustre la circulation massive en interne des données à caractère personnel, *Apple ATT* ajoute au tableau l'instrumentalisation de la mise en conformité au RGPD pour justifier l'approche restrictive au partage de ces données avec des tiers.

En juin 2020, *Apple* annonce une mise à jour de ses appareils dans le cadre de sa politique de renforcement de la protection de la vie privée de ses clients[36]. Celle-ci consiste en la mise en place du dispositif ATT, qui requiert le consentement explicite de l'utilisateur d'un iPhone avant toute utilisation de l'*Identifier for Advertisers* (ci-après, « IDFA »). L'IDFA est un identifiant unique attribué à chaque appareil Apple, qui permet le suivi de ses activités sur différents sites internet ou applications mobiles à des fins publicitaires. Sur cette base, les différentes entreprises de l'écosystème de la publicité en ligne peuvent entre autres relier l'appareil à un profil de consommation et cibler son utilisateur avec des publicités personnalisées[37]. L'ATT vient cependant chambouler ces opérations, en demandant à l'utilisateur d'autoriser le suivi de ses activités par l'application sur d'autres applications et sites web par l'intermédiaire d'une fenêtre pop-up standardisée. Si l'utilisateur refuse, l'IDFA de l'appareil ne sera pas utilisé par cette application[38]. En outre, le refus de suivi ne peut pas empêcher l'utilisateur de se servir de cette dernière, sous peine pour la société de voir son application exclue de l'App Store d'Apple[39].

Ce nouveau dispositif provoque une levée de boucliers de la part de plusieurs associations représentant différents acteurs du secteur français de la publicité en ligne, qui aboutit à une plainte en octobre 2020 devant l'Autorité de la concurrence française. Ces dernières soutiennent que l'adoption du dispositif ATT, auquel les développeurs d'application doivent recourir pour accéder à l'IDFA, constitue un abus de position dominante dans le chef *d'Apple*[40]. L'autorité française est ainsi amenée à décider si *Apple* impose des conditions de transaction non équitables en ayant recours à la sollicitation ATT pour recueillir le consentement des utilisateurs, dans l'éventuel but de dissuader les utilisateurs de donner aux développeurs d'application l'accès à leurs IDFA[41].

Parmi les arguments invoqués devant l'Autorité française de la concurrence, certains se fondent sur le droit de la protection de données à caractère personnel ou sont en lien avec ce dernier. Ainsi, il a été allégué que le dispositif serait redondant, étant donné que les développeurs d'applications étaient déjà soumis au RGPD et à la directive e-Privacy[42]. De même, les développeurs

36 Autorité de la concurrence française, décision n° 21-D-07 du 17 mars 2021, point 18.

37 Autorité de la concurrence française, décision précitée, point 5.

38 Autorité de la concurrence française, décision précitée, point 23.

39 Autorité de la concurrence française, décision précitée, points 22 et 30.

40 Autorité de la concurrence française, décision précitée, points 73-94.

41 Autorité de la concurrence française, décision précitée, point 73.

42 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement

seraient mieux à même de développer des solutions efficaces pour protéger la vie privée des utilisateurs. Ensuite, la sollicitation ATT ne serait pas conforme aux exigences imposées par le RGPD. Non seulement, elle ne fournirait pas les informations requises par les articles 13 et 14 de ce dernier, mais elle ne permettrait pas non plus aux utilisateurs de révoquer le consentement au suivi aussi facilement qu'ils l'ont accordé. Enfin, la sollicitation ATT aurait été mise en place pour d'autres motifs que la protection de la vie privée des utilisateurs. En effet, Apple n'affiche pas cette fenêtre d'information, ni aucune autre forme de recueil exprès de consentement pour son propre service publicitaire, *Apple Search Ads*. Pour ce dernier, Apple a de fait adopté un système d'*opt-out*, qui exige que les utilisateurs se rendent dans les paramètres de l'iPhone pour y décocher certaines cases pré-cochées s'ils ne souhaitent pas être soumis à ces publicités ciblées.[43]

La CNIL, consultée par l'Autorité, rejette les allégations de potentielles violations du RGPD invoquées à l'encontre du dispositif et se prononce, au contraire, en faveur de ce dernier. Selon elle, il présenterait, en effet, un véritable bénéfice tant pour les utilisateurs que pour les développeurs d'applications. Pour les utilisateurs, la sollicitation ATT offre un « meilleur contrôle sur leurs données à caractère personnel en leur permettant, d'une part, d'exprimer leurs choix de manière simple et éclairée […] et, d'autre part, en empêchant techniquement et/ou contractuellement aux éditeurs d'application de tracer l'utilisateur sans son autorisation »[44]. Pour les développeurs d'application, ce dispositif leur permet de se conformer plus facilement à la réglementation en matière de protection des données « en leur fournissant un outil simple leur permettant de recueillir un consentement valide pour leurs opérations de traçage publicitaire »[45]. Selon la CNIL, l'initiative *d'Apple* est donc non seulement légitime, mais elle est d'ailleurs fortement encouragée par le droit de la protection des données[46].

Cependant, pour l'Autorité de la concurrence, bien qu'il n'existe pas encore de décision au fond à ce stade, il n'est pas exclu que la sollicitation ATT favorise les services publicitaires *d'Apple*, tout en emportant des conséquences négatives pour les développeurs d'application[47], ce qui constituerait, le cas échéant, une forme de discrimination au profit *d'Apple*[48]. Il était en effet allégué que la mise en place de la sollicitation ATT résulterait nécessairement en une baisse de revenus publicitaires, puisque le suivi serait généralement refusé par les utilisateurs. Ce faisant, les revenus réalisés par les développeurs d'application sur iOS pourraient connaître une baisse de l'ordre de 50 %. La sollicitation ATT mettrait donc en péril le modèle de financement par la publicité ciblée de nombreuses applications. À cela s'ajoute que les développeurs retireraient des revenus en moyenne deux fois supérieurs avec la publicité personnalisée qu'avec la publicité contextuelle[49]. Néanmoins, *Apple* y trouverait son compte, car son propre service publicitaire, *Apple Search Ads*, ne serait pas soumis à la sollicitation ATT qui est un système d'*opt-in*. Puisque *Apple Search Ads* fonctionne sur un mode d'*opt-out*, il est plus difficile pour les utilisateurs de refuser le suivi publicitaire car pour ce faire, ils doivent se rendre dans les paramètres de l'iPhone pour y décocher certaines cases[50]. Ainsi, l'absence de sollicitation ATT favoriserait nécessairement *Apple*, qui bénéficie du *statu quo* puisque le système d'*opt-out* existe depuis 2016[51]. De plus, ce dispositif avantagerait le modèle d'affaires *d'Apple*, lequel est basé sur le

des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201, 31 juillet 2002.

43 Autorité de la concurrence française, décision précitée, points 75-79.

44 Autorité de la concurrence française, décision précitée, point 63.

45 Autorité de la concurrence française, décision précitée, point 64.

46 Autorité de la concurrence française, décision précitée, points 60 et 157.

47 Autorité de la concurrence française, décision précitée, point 86.

48 Autorité de la concurrence française, décision précitée, point 163.

49 Autorité de la concurrence française, décision précitée, point 88.

50 Autorité de la concurrence française, décision précitée, point 79 ; pour remédier à cette différence de traitement entre les services d'Apple et les services d'entreprises tierces, des engagements pourraient être pris par Apple, afin de soumettre Apple Search Ads à l'*opt-in*.

51 Autorité de la concurrence française, décision précitée, point 9.

paiement des utilisateurs. Le modèle de financement par la publicité ciblée – qui est le modèle dominant – étant menacé, les développeurs d'application pourraient être incités à basculer vers un modèle financé par les paiements des utilisateurs. Ainsi, cette transition jouerait dans le bénéfice d'Apple. En effet, elle applique une commission de 30 % sur les achats d'application dans l'App Store, qu'il s'agisse de versements forfaitaires ou d'abonnements payants, ainsi que sur les achats « *in-app* »[52].

L'Autorité française de la concurrence entend ces arguments, mais elle estime que seule une instruction au fond permettra de déterminer si la sollicitation ATT, pourtant *a priori* légitime au regard du droit de la protection des données, voire encouragée par ce dernier, violerait le droit de la concurrence. Il convient de noter que l'Autorité se prononce ici sur des mesures conservatoires et refuse de les ordonner au motif que l'ATT n'a pas à s'appliquer au service publicitaire d'Apple, dans la mesure où ce dernier n'utilise pas des techniques de « suivi individuel » des internautes[53]. Ce point est à peine développé dans la décision, pourtant il aurait mérité quelques lignes de plus. En effet, la notion de « suivi individuel » à laquelle se réfère l'Autorité et qui déclenche l'application du dispositif ATT, est définie par Apple comme « l'action de relier les données d'utilisateur ou d'appareil collectées à partir de [sa propre] application avec les données d'utilisateur ou d'appareil collectées à partir d'applications, de sites Web ou de propriétés hors ligne d'autres sociétés à des fins de publicité ciblée ou de mesure publicitaire »[54]. Ainsi, si le partage des données n'a lieu qu'au sein d'une seule entreprise, la demande d'autorisation de suivi n'est pas nécessaire. Dès lors qu'Apple ne fait que collecter des données propriétaires générées par l'utilisation de ses propres services, le suivi qu'elle fait ne requiert pas l'application de la sollicitation ATT[55]. Il s'agit là d'un élément essentiel. En effet, Apple semble adopter une approche très restrictive à la collecte et au partage des données avec des tiers, tout en faisant circuler (plus) librement les données de ses utilisateurs en interne. Cette pratique imposant *de facto* un double standard dans le traitement de données des internautes suscite des inquiétudes quant à une instrumentalisation du droit de la protection des données pour justifier des stratégies anticoncurrentielles (voy. *infra*).

Des préoccupations analogues ont motivé la CMA à ouvrir une investigation à l'encontre de Google pour des violations présumées du droit de la concurrence par son projet « Privacy Sandbox » en janvier 2021. Selon la CMA, le projet Privacy Sandbox était susceptible entre autres de fausser la concurrence sur le marché de la fourniture d'inventaire publicitaire au Royaume-Uni et sur le marché de la fourniture de services publicitaires en ligne au Royaume-Uni, en restreignant la fonctionnalité associée au suivi des utilisateurs pour les tiers, tout en conservant cette fonctionnalité pour Google. Plus précisément, Google n'aurait pas été aussi affecté que les tiers par la mesure en raison de son accès presque direct aux données des utilisateurs, qui ne requiert pas de *cookies* tiers, par exemple via leurs historiques de navigation. En outre, les outils alternatifs ne constituaient pas des substituts efficaces aux différentes fonctionnalités fournies par les *cookies*. Cela aurait eu pour conséquence d'empêcher les concurrents de Google de croiser les données individuelles des utilisateurs sur les différents services du web, sans impacter la capacité de Google à le faire, laquelle repose largement sur son écosystème[56]. La procédure s'étant clôturée par la prise d'engagements par Google afin de rencontrer les préoccupations de la CMA, celle-ci n'a finalement pas condamné de violation du droit de la concurrence dans le chef de Google[57]. Ces engagements impliquent notamment la participation de la CMA et de l'ICO dans l'élaboration et la mise à l'essai du projet Privacy Sandbox, ainsi qu'une suspension de la suppression des cookies tiers tant que la CMA ne sera pas convaincue que les problèmes de

52 Autorité de la concurrence française, décision précitée, point 87.

53 Autorité de la concurrence française, décision précitée, points 161-164.

54 X, « User Privacy and Data Use », https://developer.apple.com/app-store (consulté le 24 janvier 2023).

55 Autorité de la concurrence française, décision précitée, point 161.

56 Competition and Markets Authority, « Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals », 11 février 2022, Case n° 50972, pp. 35-44, https://www.gov.uk.

57 X, « CMA to keep "close eye" on Google as it secures final Privacy Sandbox commitments », communiqué de presse, https://www.gov.uk/government/news/ (consulté le 28 janvier 2023).

concurrence ont été résolus. En outre, Google s'engage à restreindre le partage des données au sein de son écosystème afin de s'assurer qu'elle ne bénéficie pas d'un avantage concurrentiel lorsque les cookies tiers seront supprimés[58].

B. Les stratégies d'enveloppement

Depuis plusieurs années, la doctrine examine les effets du RGPD sur la concurrence. De ces études, il ressort que la législation sur la protection des données à caractère personnel pourrait impacter négativement cette dernière en augmentant la concentration sur les marchés de services de données, en particulier le marché de fourniture des services publicitaires en ligne[59]. En effet, les restrictions du RGPD en matière de partage des données donnent un avantage concurrentiel aux grands acteurs de la publicité en ligne, tels que Google ou Facebook, qui sont en mesure d'acquérir de grandes quantités de données grâce à leurs propres produits. Sous couvert de la protection des données, ces grandes entreprises prennent des mesures extrêmes et refusent le partage de leurs données avec de plus petits acteurs, dont elles mettent en doute la capacité à se conformer au RGPD. Paradoxalement, les petits fournisseurs ou les nouveaux entrants ont plus à gagner à accéder aux données de services tiers que ces grandes entreprises. De fait, ces dernières disposent déjà des données dont elles ont besoin grâce à une collecte interne via leur écosystème, composé de leurs propres services[60].

Les affaires *Apple ATT* et *Google Privacy Sandbox* démontrent tout l'intérêt des entreprises dominantes à restreindre au nom de la vie privée le partage de données entre plusieurs services tiers, sans pour autant se priver de faire circuler les données qu'elles collectent au travers de leurs différents services en interne. Cette utilisation croisée des données est un élément essentiel dans leurs politiques d'expansion et leur permet de commettre des abus anticoncurrentiels. En effet, cette expansion passe par une stratégie d'enveloppement, qui consiste pour l'entreprise à « envelopper » de nouveaux marchés tout en consolidant son pouvoir de marché sur son marché principal. Plus concrètement, l'entreprise dominante sur son marché d'origine entre sur le marché cible en tirant parti du chevauchement de leurs utilisateurs. En croisant leurs données, elle capte des parts de marchés et exploite les effets de réseau qui protégeaient auparavant l'opérateur historique sur le marché cible. Elle l'empêche ainsi d'avoir accès aux utilisateurs.

Parallèlement, cette stratégie renforce sa position dans son marché d'origine, car elle empêche les concurrents du marché cible d'acquérir une supériorité en termes de données et de pénétrer sur le marché d'origine. La plateforme répète ensuite ce processus pour conquérir de nouveaux marchés et renforcer sa position sur son marché principal[61]. Sans l'utilisation croisée des données, l'enveloppement ne serait pas possible. C'est pourquoi l'engagement de Google auprès de la CMA consistant à restreindre le partage interne des données provenant de ses différents services semble particulièrement approprié.

La récente adoption du DMA offre des opportunités de remédier à la situation. À cet égard, il impose notamment aux contrôleurs d'accès[62] d'obtenir le consentement de l'utilisateur final pour combiner ou croiser ses données à caractère personnel lorsque ce dernier utilise les services d'entreprises ayant recours aux services du contrôleur d'accès ou d'autres services dudit contrôleur d'accès[63]. Ce faisant, le DMA prévient l'instrumentalisation potentielle des bases de licéité du traitement, telles que l'intérêt légitime du contrôleur d'accès ou

58 *Idem*.

59 Voy. not. M. Gal et O. Aviv, « The Competitive Effects of the GDPR », *Journal of Competition Law and Economics*, 2020, pp. 349-391 ; D. Geradin, T. Karanikioti et D. Katsifis, « GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech », *TILEC Discussion Paper DP 2020-012*, 2020, pp. 2-39, https://ssrn.com/abstract=3598130 ; T. Tombal, « Data Protection and Competition Law : Friends or Foes regarding Data Sharing ? », *TILTing Perspectives 2021 Conference : Regulating in Times of Crisis*, https://ssrn.com/abstract =3826325.

60 D. Geradin, T. Karanikioti et D. Katsifi, *op. cit.*, pp. 17-18.

61 D. Geradin, T. Karanikioti et D. Katsifi, *op. cit.*, pp. 25-26.

62 Selon l'article du DMA, un contrôleur d'accès est une entreprise avec de grandes parts de marché qui jouit d'une position durable sur le marché et qui offre un service de plateforme essentiel défini à l'article 2, 2), du DMA. Il s'agirait par exemple de Google qui fournit un moteur de recherche en ligne.

63 Art. 5.2 du DMA.

encore l'exécution du contrat[64], dont l'affaire *Meta* a fait montre[65]. Par ailleurs, l'obtention du consentement, dont l'importance comme base de licéité du traitement se voit renforcée, ne peut être rendue plus lourde pour les entreprises utilisatrices des services du contrôleur d'accès, que pour les propres services dudit contrôleur d'accès[66-67].

Ainsi, comme en témoignent les pratiques décrites ci-avant, les entreprises dominantes tendent à utiliser le RGPD – ou l'interprétation qu'elles en font – pour justifier des abus concurrentiels. Notons que la conformité au droit de la protection des données derrière laquelle ces entreprises se retranchent a été mise en question par plusieurs auteurs[68] et décisions[69].

Enfin, il est concevable que certains acteurs veuillent imposer à des entreprises tierces des conditions très, voire trop, strictes en matière de protection des données. Le droit de la concurrence s'oppose néanmoins à ce que des entreprises dominantes le fassent, tout en manquant d'appliquer cette même rigueur à leurs propres services, sous peine de commettre un abus de *self-preferencing*.

C. Les conséquences de l'arrêt du 4 juillet 2023 sur cette instrumentalisation

Les entreprises dominantes invoquent de plus en plus des arguments fondés sur le droit de la protection des données pour justifier des abus en droit de la concurrence. Une telle ligne de défense serait impossible dans un régime séparatiste, qui voit ces questions comme des considérations à part (voy. *supra*). Cette approche ayant été récemment abandonnée par la C.J.U.E., dans son arrêt du 4 juillet 2023, l'approche intégrationniste nouvellement adoptée par la Cour ouvre la porte à une certaine instrumentalisation du RGPD, bien qu'elle présente certains avantages.

Plusieurs degrés d'intégration peuvent être envisagés. Une stratégie d'intégration minimale, ou plutôt « unilatérale », consisterait pour une autorité compétente dans une matière à prendre davantage en compte les arguments tirés de l'autre matière, sans pour autant consulter l'autorité compétente dans celle-ci[70]. Cette approche a le bénéfice de rapprocher les deux matières et, plus largement, de tenir marginalement compte de leurs synergies, mais elle emporte également le risque d'interprétations divergentes. Pour cette raison, ce n'est pas la voie qu'emprunte la C.J.U.E.[71]. Elle opte pour une stratégie d'intégration coordonnée, impliquant une certaine forme de collaboration entre les différentes autorités compétentes (voy. *supra*). Cette dernière semble plus à même à résoudre efficacement les situations de chevauchement entre ces deux matières, en particulier en cas de conflit apparent. Lorsque des entreprises détenant un nombre important de données exposent et justifient leur refus de partage des données avec des tiers par des considérations issues du droit de la protection des données, il est impératif que les autorités de la concurrence collaborent avec les autorités de contrôle. Cela leur permettrait en effet de déterminer si les normes de protection des données imposées aux tiers par ces grandes entreprises sont réellement plus élevées que celles qu'elles s'appliquent à elles-mêmes[72]. Ce faisant, il leur sera plus aisé de déterminer si d'autres motifs que la protection des données se cachent derrière la pratique en question et de faire une mise en balance des intérêts en présence, en conséquence.

C'est d'ailleurs la voie que semble avoir empruntée l'Autorité française de la concurrence en consultant la CNIL dans l'affaire *Apple ATT*. Ce n'est pas la seule. Comme

64 Considérant 36 du DMA.

65 Bundeskartellamt, Décision précitée, points 676-693 et 738-783.

66 Art. 13.5 du DMA.

67 D'autres pratiques d'instrumentalisation du RGPD sont également condamnées. Voy. le considérant 40, qui estime que la pratique consistant à conditionner l'accès d'un service de plateforme essentiel à l'enregistrement ou à la création d'un compte dans le but de recevoir un deuxième service de plateforme essentiel devrait être interdite.

68 T. Tombal, *op. cit.*, pp. 1-23 ; D. Geradin, T. Karanikioti et D. Katsifi, *op. cit.*, pp. 2-39.

69 Voy. not. Commission Nationale de l'Informatique et des Libertés, *Google*, 21 janvier 2019, délibération de la formation restreinte SAN-2019-001, https://www.cnil.fr ; Commission Nationale de l'Informatique et des Libertés, *Google LLC et Google Ireland Limited*, 7 décembre 2020, Délibération de la formation restreinte SAN-2020-012, https://www.legifrance.gouv.fr/cnil/.

70 W. Kerber et L. Specht-Riemenschneider, *op. cit.*, pp. 27-28.

71 Arrêt *Meta*, point 55.

72 T. Tombal, *op. cit.*, p. 22.

exposé précédemment, la CMA et l'ICO ont également collaboré dans l'affaire *Google Privacy Sandbox* et continuent à le faire dans le contrôle des engagements de Google. Sur ce dernier point, ils ont souligné que leur coopération permettra de garantir des résultats efficaces pour les consommateurs et de protéger à la fois la concurrence et la vie privée[73]. Cet argument d'effectivité se retrouve également, au sujet du droit de la concurrence, dans la décision de la Cour[74].

CONCLUSION

L'heure est au soulagement pour les autorités de la concurrence. Depuis l'arrêt *Meta*, elles se voient confortées pour la plupart dans leur pratique déjà établie de coopérer avec leurs homologues en droit de la protection des données à caractère personnel lorsque des questions relatives à leur matière se posent en droit de la concurrence. La Cour y abandonne son approche séparatiste, datant de son arrêt *Asnef-Equifax*, et y accueille l'approche intégrationniste. Ce revirement fort attendu est une bonne nouvelle pour l'application du droit de la concurrence dans les marchés numériques. Combinée à l'approche *ex ante* du DMA, la compétence « nouvellement » reconnue aux autorités de la concurrence de procéder à un examen incident de la conformité d'un comportement au RGPD, moyennant le respect de certaines conditions, promet de préserver davantage la concurrence effective sur ces marchés. Les autorités de la concurrence pourront désormais appréhender plus facilement les abus rendus possibles par les stratégies d'enveloppement, pratiquées par les géants du numérique. Ces dernières sont de fait intimement liées à la lecture particulière du RGPD que font ces entreprises. Comme l'illustre l'affaire *Apple ATT*, il en résulte que leurs politiques en matière de vie privée sont particulièrement permissives quant au recoupement, à la réutilisation et à la circulation des données à caractère personnel au sein de leurs propres services, tout en étant fort restrictives quant aux accès des tiers à ces données. La prise en compte du droit de la protection des données à caractère personnel dans l'analyse concurrentielle, ainsi que l'appui des autorités de contrôle du RGPD, ne manquera donc pas de rendre cette analyse plus lucide sur les intérêts en présence afin de garantir le bien-être du consommateur. Espérons également que cette nécessaire coopération ne soit pas non plus instrumentalisée afin de ralentir les procédures devant les différentes autorités de contrôle. Cette crainte est d'autant plus forte dans les cas où l'autorité de contrôle serait amenée à prendre une décision devant être soumises aux mécanismes de cohérence prévus dans le RGPD.

[73] X, « CMA to keep "close eye" on Google as it secures final Privacy Sandbox commitments », communiqué de presse, https://www.gov.uk/government/news/ (consulté le 28 janvier 2023).

[74] Arrêt *Meta*, point 51.