RÉPUBLIQUE FRANÇAISE

Autorité de la concurrence

Intervention de Benoît Cœuré, président de l'Autorité de la concurrence, devant le collège de la CNIL

Droit de la concurrence et protection des données personnelles

Jeudi 2 juin 2022

9h30 - 10h30

Mme la Présidente, Mesdames et Messieurs les membres du Collège, je suis ravi d'être aujourd'hui parmi vous.

Je tiens tout d'abord à remercier la CNIL pour l'organisation de cette séance, qui nous réunit aujourd'hui pour échanger sur les relations entre le droit de la concurrence et le régime de protection des données, ainsi que sur la coopération entre nos deux institutions.

En effet, le droit de la concurrence et la protection des données personnelles constituent tous deux des outils puissants qui façonnent notre économie. Dans le contexte actuel, ces deux champs règlementaires font l'objet d'interactions toujours plus nombreuses, liées au développement de l'économie numérique fondée sur la donnée.

Une réflexion sur l'articulation, actuelle et future, entre le droit de la concurrence et le droit de la protection des données personnelles, afin de maximiser notre action au bénéfice de l'économie et des consommateurs, s'impose donc aujourd'hui. Or les interactions sont à la fois directes à travers nos pratiques décisionnelles respectives et indirectes, ou structurelles, à travers la structure des marchés et les incitations des acteurs que nous contribuons à influencer.

En méthode, il faut commencer par comprendre ces interactions – en particulier, sont-elles sources de synergies ou de tensions ? Puis décider de les intégrer ou non à notre pratique, et enfin les expliquer aux acteurs économiques, qui attendent légitimement des acteurs publics qu'ils soient prévisibles et cohérents.

Notre échange peut aussi constituer l'occasion de réfléchir ensemble à des pistes concrètes d'approfondissement de la coopération, déjà fluide et efficace, entre nos deux institutions.

1.1. A l'ère de la transformation numérique, les données personnelles constituent un enjeu majeur à l'intersection de plusieurs régimes de régulation

a) Transformation numérique et ère de la donnée

La rencontre entre le droit de la concurrence et le régime de protection des données n'est pas nouvelle. Bien avant que l'on parle des Big Tech ou des « GAFAM » (aujourd'hui les « MAMAA[1] »), l'Autorité de la concurrence s'est intéressée, dès les années 2000, en utilisant les outils usuels à sa disposition, aux pratiques des entreprises liées à l'usage de données personnelles qu'elles détiennent, par exemple pour apprécier l'avantage concurrentiel conféré par la détention de fichiers clients constitués par d'anciens monopoles historiques[2].

Un exemple marquant est celui de l'injonction prononcée par l'Autorité de la concurrence à l'égard de GDF Suez (aujourd'hui Engie) en 2014[3]. Dans cette affaire, l'Autorité a enjoint à GDF d'accorder à ses concurrents un accès à son fichier historique de clients. Elle a toutefois considéré que la communication de ces données ne pouvait se faire que dans le respect des dispositions ayant trait à la protection de la vie privée et a imposé la mise en place d'un droit d'opposition préalable des clients au démarchage des concurrents de GDF, conformément aux recommandations de la CNIL dont l'avis sur la question avait été sollicité.

Si la prise en compte par l'Autorité de la concurrence de l'utilisation des données par les entreprises n'est pas nouvelle, les récents développements technologiques ont toutefois révolutionné la collecte, le traitement et l'exploitation des données personnelles, qui sont désormais réalisables de manière massive, automatisée et presque instantanée.

La collecte et l'utilisation des données des consommateurs sont désormais au cœur des activités de nombreuses entreprises, qui s'appuient sur ces données pour offrir des nouveaux services aux utilisateurs et clients. Les entreprises de tous les secteurs de l'économie développent ainsi des stratégies pour accéder à ces données et les valoriser.

Dans ce contexte, certaines plateformes exercent un rôle particulièrement structurant au sein d'écosystèmes intégrés (par exemple en matière de publicité en ligne), ce qui aboutit à une concentration des données entre les mains de quelques grands acteurs[4].Ces derniers se retrouvent en position de force pour monétiser les données générées par leurs utilisateurs, notamment sur les marchés de la publicité en ligne.

C'est dans ces écosystèmes particuliers, caractérisés par la présence de marchés bifaces et, de plus en plus, multifaces, caractérisés par de forts effets de réseaux, que l'on peut constater

[1] Meta/Facebook, Amazon, Microsoft, Apple, Alphabet/Google

[2] Voir par exemple : Décision 03-MC-04 du 22 décembre 2003, relative à une demande de mesures conservatoires présentée par la société les Messageries Lyonnaises de Presse ; Avis 10-A-13 du 14 juin 2010, relatif à l'utilisation croisée des bases de clientèle, dans lequel l'Autorité de la concurrence a examiné l'utilisation croisée de bases de clientèle par Orange. Voir également, plus récemment, l'Avis 18-A-03 du 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet.

[3] Décision 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité.

[4] Ces sujets ont été abordés lors du séminaire Nasse « Protection de la vie privée et concurrence », en date du 14 octobre 2021.

aujourd'hui des pratiques qui posent question à la fois au regard du droit de la concurrence et de celui de la protection des données personnelles.

b) Prise en compte des paramètres de protection de la vie privée dans l'analyse concurrentielle

Les deux ensembles de règles – protection des données personnelles et droit de la concurrence - poursuivent *stricto sensu* des objectifs distincts : si la politique de la protection des données personnelles vise à protéger les utilisateurs contre toute collecte et exploitation préjudiciable de leurs données, la politique de la concurrence vise à garantir les conditions d'une concurrence libre et non faussée entre les entreprises sur les marchés dans l'intérêt des consommateurs, en favorisant l'innovation, la diversité de l'offre et des prix attractifs.

Pour remplir la mission qui lui a été assignée par le législateur, l'Autorité de la concurrence intervient de deux manières. D'une part, l'Autorité réprime les pratiques anticoncurrentielles, qui peuvent prendre la forme d'ententes ou d'abus de position dominante, et, en prononçant, si nécessaire, des mesures d'urgence, des injonctions, ou des sanctions pécuniaires. D'autre part, l'Autorité contrôle les opérations de concentration entre entreprises préalablement à leur réalisation (rachats, fusions, créations d'entreprises communes…) dépassant une certaine taille. Elle veille ainsi en amont à ce que ces opérations ne réduisent pas la concurrence et peut les autoriser, conditionner leur autorisation à la mise en place d'engagements adaptés, en cas de risque d'atteinte à la concurrence, ou interdire leur réalisation.

Malgré ces objectifs distincts, les deux cadres de régulation présentent néanmoins une certaine convergence d'objectifs, au sens large, en ce qu'ils sont, *in fine,* mis en œuvre au bénéfice des usagers.

Cette convergence – ou du moins la réflexion à mener sur cette dernière – s'illustre tout particulièrement dans le domaine du numérique, et des modèles que j'évoquais précédemment.

Ces modèles économiques, basés sur la collecte et l'exploitation massive des données, peuvent être une source d'innovations et de bénéfices pour les consommateurs, mais soulèvent néanmoins de nombreuses questions concernant les conditions dans lesquelles ces données personnelles sont collectées et utilisées.

Ces pratiques relatives à la collecte et l'utilisation des données personnelles peuvent être appréhendées par les autorités de concurrence à l'aune des objectifs qui sont les leurs :

- L'accumulation de données peut être considérée comme un élément participant à l'établissement du pouvoir de marché des entreprises considérées. La collecte et l'exploitation d'un volume important de données qui ne sont pas réplicables par des tiers peuvent en effet créer des barrières à l'entrée et être une source importante de pouvoir de marché, particulièrement lorsque les marchés en cause sont caractérisés par des forts effets de réseau.

- Le niveau de protection des données des utilisateurs peut constituer un véritable paramètre de concurrence, à l'instar du prix. En effet, si les consommateurs considèrent le niveau de protection de leurs données comme un paramètre de qualité, et donc de choix, d'un service, le degré de protection des données devient un des aspects du produit

sur lequel les entreprises se font concurrence. Toutes choses égales par ailleurs, les consommateurs choisissent le service offrant la meilleure protection de leurs données.

A ce jour, le risque d'atteinte à la concurrence du fait de la concentration de données dans les activités numériques a le plus souvent été examiné dans le cadre du contrôle des concentrations.

En effet, les opérations de concentration impliquant des entreprises utilisant les données personnelles de leurs clients peuvent porter atteinte à la concurrence, d'une part, en entrainant une baisse du niveau de protection des données personnelles des clients concernés ou, d'autre part, en renforçant les barrières à l'entrée pour les concurrents sur le marché concerné[5]. Dans le premier cas, un rachat pourrait, par exemple, éliminer un concurrent se différenciant par un niveau de protection de données personnelles plus élevé offert par ses services. La seconde hypothèse vise le cas où la concentration aboutirait à une accumulation des données par une entreprise qui serait matériellement impossible ou trop coûteuse à répliquer par ses concurrents sur le marché.

Les analyses menées par les autorités de concurrence ont progressivement évolué pour mieux prendre en compte le niveau de protection des données personnelles des utilisateurs.

Dans son examen de la fusion Google/DoubleClick[6] en 2008, la Commission européenne avait ainsi considéré que les considérations relatives à la protection de la vie privée relevaient de la législation sur la protection des données personnelles. En 2014, dans le cadre de son examen de l'opération Facebook/WhatsApp, la Commission a analysé les éventuels problèmes liés à la concentration des données des deux entités pour déterminer si celle-ci pouvait constituer une entrave au jeu de la concurrence sur le marché de la publicité en ligne (en étudiant la possibilité que Facebook utilise WhatsApp en tant que source potentielle de données d'utilisateurs afin de mieux cibler les publicités de Facebook). La Commission a conclu que l'opération ne posait pas de problèmes de concurrence, dans la mesure notamment où il demeurait un grand nombre de données d'utilisateurs d'internet utiles pour la publicité mais qui n'étaient pas sous le contrôle exclusif de Facebook. La Commission a, par ailleurs, de nouveau considéré, dans cette affaire, que les inquiétudes éventuelles liées au respect de la vie privée découlant de la concentration accrue des données sous le contrôle de Facebook n'entraient pas dans le champ d'application du droit de la concurrence de l'Union, mais relevaient « *des règles européennes de protection des données personnelles* »[7].

[5] Voir OCDE, « *Droits relatifs aux données des consommateurs et impact sur la concurrence –Note de référence du Secrétariat* », 10-12 juin 2020, par.4.1, p.25.
[6] COMP/M.4731 – Google/ DoubleClick, 11 mars 2008.
[7] COMP/M.7217 – Facebook / Whatsapp, 3 octobre 2014, par.164. La Commission européenne a par la suite infligé une amende de 110 millions d'euros à Facebook pour fourniture de renseignements inexacts au cours de l'enquête que la Commission a effectuée en 2014 au titre du règlement de l'UE sur les concentrations concernant cette acquisition : Lorsque Facebook a notifié l'acquisition de WhatsApp en 2014, la société a informé la Commission qu'elle ne serait pas en mesure d'établir d'une manière fiable la mise en correspondance automatisée entre les comptes d'utilisateurs de Facebook et ceux de WhatsApp. Cependant, en août 2016, WhatsApp a annoncé des mises à jour de ses conditions générales d'utilisation et de sa politique de confidentialité, y compris la possibilité d'associer les numéros de téléphone des utilisateurs de WhatsApp aux profils d'utilisateur de Facebook.

L'approche de la Commission a cependant progressivement évolué. Dans sa décision d'autorisation de l'opération de concentration Microsoft/LinkedIn[8], en 2016, la Commission a ainsi reconnu que la protection de la vie privée constituait un facteur important de qualité sur le marché des réseaux sociaux professionnels – et donc un paramètre de concurrence en soi (tout en indiquant que la législation européenne de protection des données personnelles limiterait la possibilité pour l'entité fusionnée des combiner les données détenues par les deux entreprises)[9].

Contrairement au contrôle des concentrations, la pratique antitrust connait peu d'exemples dans lesquels la protection de la vie privée a été abordée. Cela n'exclut pas la mobilisation des outils de répression des pratiques anticoncurrentielles, qu'il s'agisse d'abus de position dominante ou d'ententes, pour appréhender certains comportements en lien avec la collecte et le traitement des données[10].

En premier lieu, certaines entreprises pourraient tirer profit de leur position dominante pour mettre en œuvre des pratiques abusives d'éviction. En pratique, un opérateur dominant pourrait chercher à évincer des concurrents en collectant et exploitant de données impossible à obtenir par des tiers obtenues de façon non concurrentielle ou entravant la collecte ou l'accès à des données nécessaires à leur activité.

. On retrouve ici par exemple le cas que j'évoquais il y a quelques instants des fichiers clients constitués par certains opérateurs historiques en monopole, illustré récemment par notre décision sur l'exploitation abusive par EDF des données issues des fichiers de ses clients éligibles au tarif réglementé de vente[11].

En second lieu, une entreprise dominante pourrait profiter de sa position pour mettre en œuvre des pratiques abusives d'exploitation, c'est-à-dire réduire le niveau de protection des données personnelles des utilisateurs en imposant, par exemple des clauses abusives à des consommateurs qui n'auraient d'autre choix que d'accepter ces conditions dégradées en l'absence d'alternative équivalente.

C'est ce scénario novateur pour le droit de la concurrence que l'autorité allemande de la concurrence, le Bundeskartellamt, a retenu dans sa décision Facebook de 2019[12]. Dans cette affaire, l'autorité allemande était saisie des conditions générales de Facebook en Allemagne, lesquelles prévoient que les utilisateurs consentent à ce que l'entreprise collecte leurs données personnelles sur son portail, mais aussi à partir de services dont Facebook est propriétaire (WhatsApp, Instagram, etc.), voire auprès de tiers. Le Bundeskartellamt a considéré qu'imposer

[8] COMP/M.8124 – Microsoft / LinkedIn, 6 décembre 2016.
[9] Voir également la décision Apple/Shazam (2018), où la Commission européenne a examiné la capacité d'Apple à utiliser ses données utilisateurs pour renforcer la position de Shazam en matière de publicité en ligne.
[10] Voir la contribution de l'Union européenne à la note OCDE « *Droits relatifs aux données des consommateurs et impact sur la concurrence* », par.3.1.2, p.12 ; voir également Anne Witt, « Data, Privacy and Competition Law », Graz Law Working Paper N° 24-2021.
[11] Décision 22-D-06 du 22 février 2022 relative à des pratiques mises en œuvre par la société EDF dans le secteur de l'électricité. La question de l'entrave à l''accès des concurrents aux données détenues par un opérateur en position dominante n'est pas récente: voir à cet égard la décision n° 98-D-60 du Conseil de la concurrence du 29 septembre 1998, relative à des pratiques mises en œuvre par la société France Télécom dans le secteur de la commercialisation des listes d'abonnés au téléphone.
[12] Bundeskartellamt, décision n° B6-22/16 du 6 février 2019.

aux utilisateurs l'agrégation de toutes ces données, en violation des dispositions du règlement général sur la protection des données (RGPD), constituait un abus de position dominante par exploitation. En enjoignant à Facebook de ne plus imposer à l'utilisateur de consentir à cette agrégation, le Bundeskartellamt a caractérisé lui-même une violation d'un ensemble de dispositions du RGPD relatives aux conditions de recueil du consentement et au traitement des données personnelles[13].

Cette approche fait l'objet de vives discussions, concernant la pertinence d'une intervention directe des autorités de concurrence face à des pratiques en matière de protection de la vie privée.

Saisie d'une question préjudicielle par le Tribunal régional supérieur de Düsseldorf dans l'affaire précitée, la Cour de justice de l'Union européenne devra ainsi, entre autres, statuer sur la compétence d'une autorité nationale de concurrence pour se prononcer, dans le cadre du contrôle des pratiques anticoncurrentielles, sur le respect du RGPD par l'entreprise visée par sa décision. L'audience s'est déroulée le 10 mai 2022, et l'avis de l'avocat général est attendu pour le 20 septembre 2022.

Dans le cadre de l'audience devant la Cour, le Président a par ailleurs interrogé la Commission sur les risques que présenterait, pour une application harmonieuse du RGPD, un système dans lequel les autorités de concurrence pourraient adopter des décisions portant sur le respect de ce texte[14]. C'est là une autre problématique qu'il convient d'intégrer dans nos réflexions communes sur le sujet.

Relevons que les développements qui précèdent traitent de dégradation ou d'utilisation de la protection des données personnelles restrictives de la concurrence. Néanmoins, des hypothèses où un accord, ou des pratiques, mèneraient à une amélioration de cette protection, tout en restreignant la concurrence, peuvent également être envisagées.

En tout état de cause, il est certain que les analyses concurrentielles liées à l'utilisation des données personnelles se développent tant pour l'application de l'Article 102 que celle de l'Article 101 du traité sur le fonctionnement de l'Union européenne (TFUE), et les autorités de concurrence s'interrogent sur l'opportunité et la manière d'intégrer des objectifs de protection des données personnelles dans leurs différentes analyses. Nul doute que ces questions connaitront très prochainement de nouveaux développements, du fait des nombreuses affaires en cours d'examen devant différentes autorités de concurrence.

Au-delà cependant des modalités de l'intégration des dimensions « *données* » et « *vie privée* » dans le champ de l'analyse concurrentielle, la question de **l'interaction entre les deux cadres règlementaires** reste pleinement pertinente.

[13] Facebook avait interjeté appel devant l'OLG Düsseldorf (Cour d'appel) qui, dans l'attente de sa décision, a ordonné la suspension de l'exécution de l'injonction considérant qu'il existait des doutes sérieux sur la légalité de l'injonction. La Cour suprême allemande a annulé cette suspension le 23 juin 2020, le dossier est revenu devant le tribunal régional supérieur de Düsseldorf, qui a décidé de saisir la Cour de justice de l'Union européenne d'une série de questions préjudicielles le 24 mars 2021.
[14] POLITICO Pro Fair Play du 11 mai 2022, « *Meta takeaway*».

2. Interactions entre le droit à la protection des données personnelles et le droit de la concurrence : entre synergies et tensions

a) La protection des données personnelles comme paramètre de concurrence

Comme je l'évoquais précédemment, le niveau de protection des données personnelles peut être considéré dans certains cas comme un paramètre de concurrence à part entière (en tant que paramètre de qualité sur lequel s'exerce la concurrence). Dans un tel schéma, le maintien d'une concurrence effective sur le marché s'accompagne d'un fort niveau de protection des données[15]. En effet, dans ce scénario, les utilisateurs favoriseront, lorsque le choix leur est donné, une meilleure protection de leurs données personnelles, ce qui incite les entreprises concernées à améliorer leur offre dans ce domaine. La déclaration conjointe de l'Information Commissionner's Office (ICO) et la Competition and Markets Authority (CMA)[16], régulateurs des données personnelles et de la concurrence britanniques, relève à cet effet que « *Lorsque les utilisateurs peuvent exercer un véritable choix et que les fournisseurs se font concurrence sur un pied d'égalité, une concurrence efficace peut permettre une protection plus efficace de la vie privée, tandis qu'un faible niveau de concurrence peut compromettre cette protection de la vie privée.* »

Ainsi, une pression concurrentielle satisfaisante est de nature à favoriser les innovations qui promeuvent une meilleure protection des données, telles que le développement de technologies plus respectueuses de la vie privée, ou la création d'outils favorisant une plus grande mobilité des données.

Néanmoins, si ces scénarios vertueux peuvent trouver à s'appliquer dans des marchés « classiques » avec un niveau de concurrence satisfaisant, cela n'est pas nécessairement le cas dans le cadre de marchés caractérisés par de forts effets de réseaux et dominés par des acteurs au pouvoir de marché prépondérant. Dans un tel cas, l'acteur dominant peut être incité à réduire la protection des données personnelles, afin d'améliorer ses revenus grâce à la collecte toujours plus importante d'informations sur ses utilisateurs ce qui, par la même occasion, aboutira à augmenter les barrières à l'entrée pour ses concurrents (qui ne seront pas en mesure de collecter la même quantité d'informations). L'analyse concurrentielle de ces situations peut toutefois être compliquée par le fait que l'amélioration des revenus de la plateforme peut passer par la fourniture de nouveaux services aux utilisateurs ou par l'amélioration de leur qualité.

Certains auteurs considèrent par ailleurs que cette complémentarité entre protection des données et concurrence serait limitée par le phénomène parfois désigné sous le terme de paradoxe de la protection de la vie privée (« *privacy paradox* »)[17]. Sur le principe, les consommateurs déclarent valoriser un haut niveau de protection de leur vie privée, afin que

[15] Stucke, Maurice E., "*The Relationship Between Privacy and Antitrust*", 23 février 2022, Notre Dame Law Review.
[16] UK Competition Authority, ICO and CMA set out blueprint for cooperation in digital markets, Statement, 19 May 2021. Traduction libre.
[17] P. A. Norberg, D. R. Horne, et D. A. Horne, "*The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*", 6 mars 2007, Journal of Consumer Affairs 41, No. 1 (2007): 100–26; Susan Athey, Christian Catalini, Catherine E.Tucker, "*The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*", 8 avril 2018, MIT Sloan Research Paper No. 5196-17, Stanford University Graduate School of Business Research Paper No. 17-14.

leurs données personnelles ne soient pas indûment exploitées, stockées ou diffusées. Dans la pratique, les utilisateurs sous-estimeent cependant la valeur de leur vie privée, en permettant en général un accès assez libre à leurs données personnelles. Ce biais peut affecter le cycle vertueux décrit ci-avant, dans la mesure où la concurrence sur la protection de la vie privée ne peut effectivement s'exercer qu'à la condition que les utilisateurs valorisent suffisamment celui-ci pour le prendre en compte dans leurs choix de consommation. Si les consommateurs n'effectuent pas un tel choix, une concurrence vive peut conduire à une dégradation des conditions de collecte et d'exploitation des données personnelles.

b) De nouveaux équilibres à déterminer

Ainsi, si les aspects « données personnelles » et concurrence peuvent être intrinsèquement liés, leur analyse peut cependant donner lieu à certaines tensions, ou à tout le moins à des questionnements, entre champs de régulation[18].

Les règles de protection des données personnelles sont susceptibles, dans certains cas, de créer des distorsions de concurrence. Cela peut être par exemple le cas si la législation sur la protection de la vie privée rend plus difficile le partage des données personnelles entre les acteurs du marché, lorsque les données en question sont nécessaires pour que les entreprises concurrentes puissent proposer des produits compétitifs à leurs clients.

Ainsi, l'adoption du RGPD conditionne l'utilisation des traceurs (« *cookies* ») au consentement de l'internaute, ce qui peut entrer en conflit avec le modèle d'affaires de certains acteurs d'internet (ex médias ou publicitaires). Ces contraintes règlementaires peuvent être de nature à favoriser les grandes plateformes et leurs environnements dits « logués » (c'est-à-dire nécessitant une identification préalable) qui subissent moins le durcissement des conditions du recueil du consentement des internautes (en obtenant, par exemple, de l'internaute, lors de son inscription, un consentement général à la collecte de ses données en contrepartie du service rendu), au détriment des autres acteurs.

Plus généralement, les politiques de minimisation de la donnée, plus protectrices de la vie privée des utilisateurs, peuvent augmenter les coûts d'accès aux données pour des concurrents potentiels, et constituer ainsi des barrières potentielles à l'accès sur le marché. Ce type de problématiques incite à nous assurer que l'impact de ces mesures sur le fonctionnement de la concurrence soit pris en compte dès leur élaboration.

Des questions nouvelles se présentent également à nous lorsque certains acteurs de marché ont eux-mêmes décidé de modifier et renforcer leur politique de protection de la vie privée au-delà de ce que réclame la réglementation.

Cette problématique se pose ainsi avec particulièrement d'acuité dans le cas des politiques de confidentialité mises en œuvre par Apple et Google et de nombreuses voix mettent en garde contre l'utilisation d'arguments relatifs à la protection de la vie privée à des fins anticoncurrentielles[19].

---

[18] Stucke, Maurice E., "*The Relationship Between Privacy and Antitrust*", 23 février 2022, Notre Dame Law Review.

[19] Voir entre autres : Lina Khan, Statement of Chair Lina M. Khan, Regarding the Report to Congress on Privacy and Security Commission File No. P065401, 1er octobre 2021 : *« Les évènements récents mettent en évidence la*

Le cas de la *« Privacy Sandbox »* de Google est particulièrement illustratif à cet égard en ce qu'il vise à supprimer les traceurs tiers (« *third-party cookies* ») et à les remplacer par des technologies alternatives, avec pour objectif affiché de garantir plus efficacement la protection de la vie privée des utilisateurs. L'analyse de ce projet illustre la différence de prisme à travers lequel les régulateurs peuvent aborder cette annonce : les traceurs tiers suscitent depuis longtemps des inquiétudes quant au respect de la vie privée, en ce qu'ils permettent à un site web de suivre l'activité de navigation d'un internaute afin d'établir un profil d'utilisateur très précis. Néanmoins, les traceurs tiers constituent également une composante fondamentale du modèle économique des acteurs du secteur de la publicité en ligne, en permettant aux annonceurs de s'assurer que les publicités affichées correspondent aux intérêts et au profil de l'utilisateur.

La Commission européenne a ainsi ouvert une enquête sur un possible comportement anticoncurrentiel de Google dans le secteur des technologies de publicité en ligne, axée en particulier sur le projet de Google d'interdire le placement de traceurs tiers sur Chrome et de les remplacer par la panoplie d'outils « *Privacy Sandbox* »[20]. La Commission entend examiner l'incidence de ce remplacement sur les marchés de l'affichage publicitaire en ligne et de l'intermédiation en matière d'affichage publicitaire en ligne

Cette problématique a également été examinée par la CMA, qui a ouvert, en janvier 2021, une enquête afin d'examiner si les alternatives à la suppression des *cookies* proposées par Google seraient susceptibles d'entraver la concurrence sur les marchés de la publicité numérique[21]. Le 11 février 2022, la CMA a publié sa décision d'acceptation des engagements offerts par Google qui prévoient notamment (i) l'implication de la CMA et de l'ICO dans le développement et le test des projets de *Privacy Sandbox*, (ii) une transparence accrue du processus, (iii) des engagements de ne pas privilégier les services de publicité de Google, (iv) des engagements de restreindre les partages de données au sein de l'écosystème Google lorsque les traceurs tiers seront supprimés, afin de ne pas obtenir d'avantages concurrentiels sur ses concurrents.

Cette décision est met en évidence les compromis complexes entre les objectifs de protection renforcée de la vie privée et de protection de la concurrence sur les marchés numériques auxquels ont dû aboutir les régulateurs.

En France, l'affaire Apple ATT (décision 21-D-07 du 17 mars 2021) illustre la recherche d'un équilibre entre la protection des données personnelles et le développement de la publicité en ligne[22]. L'Autorité a été saisie par plusieurs associations représentant les différents acteurs de la publicité en ligne, qui contestaient les pratiques mises en œuvre par Apple à l'occasion des modifications à venir de son système d'exploitation iOS 14, et en particulier l'introduction de la

manière dont le prétexte de la protection de la vie privée peut être utilisé pour affaiblir la concurrence par les mérites » ;

[20] Voir Commission, AT.40670 Google - Adtech and Data-related practices.

[21] En entrainant une concentration encore plus grande des dépenses publicitaires au niveau de Google, et en compromettant la capacité des éditeurs en ligne tels que les journaux à générer des revenus et à continuer à produire du contenu de qualité.

[22] Décision n° 21-D-07 du 17 mars 2021 relative à une demande de mesures conservatoires présentée par les associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, et Syndicat des Régies Internet dans le secteur de la publicité sur applications mobiles sur iOS.

sollicitation App Tracking Transparency (ATT) pour les applications qui souhaiteraient faire un suivi de l'activité de l'utilisateur sur des sites tiers. L'Autorité a examiné si les mesures mises en place par Apple pour offrir à l'utilisateur un cadre renforcé de consentement pour l'utilisation de ses données personnelles pouvaient être regardées comme nécessaires et proportionnées à l'objectif de protection de la vie privée des utilisateurs Apple. En l'état de l'instruction, l'Autorité a estimé que la décision d'Apple de mettre en place un dispositif de recueil du consentement complémentaire n'apparaissait pas comme une pratique abusive justifiant des mesures conservatoires, tout en décidant de poursuivre l'instruction du dossier au fond, afin de vérifier notamment si la mise en place par Apple de la sollicitation ATT ne peut être regardée comme une forme de discrimination ou « *self preferencing* », ce qui pourrait notamment être le cas si Apple appliquait sans justification, des règles plus contraignantes aux opérateurs tiers que celles qu'elle s'applique à elle-même pour des opérations similaires. Dans sa décision, l'Autorité a reconnu, pour la première fois dans son analyse, que la protection de la vie privée des utilisateurs pouvait constituer un « objectif légitime », ce qui représente une réelle avancée dans l'évolution de l'intégration de la protection de la vie privée dans l'analyse des autorités de concurrence[23].

Cette instruction se poursuit actuellement en coopération étroite avec les services de la CNIL, également saisie par France Digitale de pratiques mises en œuvre par Apple relatives au ciblage publicitaire de ses utilisateurs.

Nous le constatons, les équilibres à trouver peuvent être complexes. Si des pratiques dégradant la protection des données personnelles peuvent être restrictives de la concurrence, il est également possible d'envisager des situations où certaines pratiques améliorant la protection de la vie privée peuvent restreindre le bon fonctionnement de la concurrence.

D'une manière plus générale, compte tenu du rôle de l'accumulation des données dans la constitution de positions qui peuvent devenir dominantes, les autorités de concurrence peuvent chercher à encourager l'interopérabilité, la portabilité voire un partage obligatoire des données, que les autorités de protection des données peuvent de leur côté, pour des raisons également légitimes, souhaiter assortir de restrictions ou de conditions.

C'est donc surtout, et avant tout, une communication et coopération efficace entre les autorités de protection des données et les autorités de concurrence qui permettra de dégager des réponses efficaces à l'ensemble de ces problématiques.

3. Nécessité d'une coopération accrue entre autorité de protection des données personnelles et autorités de concurrence

La capacité de nos autorités à agir de manière coordonnée est, j'en suis convaincu, la condition d'une réponse efficace aux défis posés par l'économie numérique. Dans ce cadre, la régulation concurrentielle et les autres types de régulation des plateformes ne doivent pas être menées en « silos », afin de permettre aux régulateurs de mieux saisir les interconnexions entre les

[23] *Ibid*, §156 : « *les règles de concurrence n'interdisent pas à Apple de mettre en place son propre recueil du consentement, en complément des plateformes de consentement utilisées par les développeurs pour répondre aux exigences du RGPD, dès lors qu'une telle décision est guidée par l'objectif légitime de protéger la vie privée des utilisateurs* ».

différentes règles applicables, et de permettre ainsi à chaque corps de règles d'atteindre ses objectifs.

Une approche coordonnée est nécessaire afin de s'assurer que les objectifs d'un des champs de régulation ne soient pas compromis par les mesures prises par l'autre régulateur.

Ce mouvement général de coopération est en cours chez certains de nos homologues. Au Royaume-Uni par exemple, l'ICO et la CMA ont publié en mai 2021 une déclaration conjointe, présentant leur point de vue commun sur la relation entre concurrence et la protection des données personnelles dans l'économie numérique, mettant l'accent sur la complémentarité des deux cadres de régulation, et affirmant leur volonté d'œuvrer conjointement afin de trouver des solutions règlementaires adaptées[24].

En France, la coopération entre la CNIL et l'Autorité est particulièrement fluide et efficace.

Elle trouve à s'appliquer dans un cadre consultatif, mais également dans un cadre contentieux[25]. Dans le cadre de sa décision Apple iOS, l'Autorité a ainsi pu bénéficier d'un avis rendu par la CNIL sur les différentes questions d'application de la législation relative à la protection de la vie privée soulevées par l'affaire. Cette coopération est intervenue dans des délais très courts, illustrant ainsi le fait que la coopération entre autorités est non seulement possible dans les affaires de fond mais également dans le cadre de procédures d'urgences. J'ai également cité notre décision de 2014 qui est un autre exemple de coopération fructueuse nous ayant permis de recueillir l'avis de la CNIL sur les modalités de recueil du consentement au démarchage par des concurrents.

N'oublions pas non plus que l'avis de la CNIL peut être sollicité par l'Autorité dans le cadre du contrôle de concentrations. Nous l'avons fait récemment dans la décision Enerest/Electricité de Strasbourg n° 12-DCC-20[26].

De la même manière, je vous invite à nous solliciter, en cas de questionnement sur les impacts potentiels de vos décisions et de vos travaux au regard du droit de la concurrence. Nous sommes à votre entière disposition pour vous éclairer et vous fournir toute notre expertise sur ces questions.

Enfin, il me semble important de rappeler que nous nous situons à un moment charnière de la régulation des marchés numériques, et que de nombreux nouveaux outils viennent - ou viendront - s'ajouter à l'écosystème législatif existant. A cet égard, les obligations imposées par la législation européenne sur les marchés numériques (« *Digital Markets Act* » ou DMA) pourront jouer un rôle clé dans la régulation des abus des plateformes structurantes en ce qui

[24] CMA et ICO « *Competition and data protection in digital markets: a joint statement between the CMA and the ICO* », 19 mai 2021.

[25] L'article R 463-9 du code de commerce dispose que : « *Le rapporteur général communique aux autorités administratives énumérées à l'annexe 4-6 du présent livre toute saisine relative à des secteurs entrant dans leur champ de compétence. Ces autorités administratives disposent pour faire part de leurs observations éventuelles d'un délai de deux mois, qui peut être réduit par le rapporteur général si l'urgence le nécessite. Ces observations sont jointes au dossier.* »

[26] Décision n° 12-DCC-20 du 7 février 2012 relative à la prise de contrôle exclusif d'Enerest par Electricité de Strasbourg, par.89. Dans le contexte de l'élaboration de l'engagement relatif à l'octroi de l'accès à tout fournisseur aux informations commerciales nécessaires à l'élaboration d'offres adaptées, les services de la CNIL ont confirmé que le dispositif envisagé était conforme aux exigences légales au regard de la loi dite « Informatique et Libertés ».

concerne la collecte et l'utilisation des données personnelles des utilisateurs. Je pense tout particulièrement à l'article 5(2) qui interdit au contrôleur d'accès de traiter les données personnelles collectées à travers ses différents services à des fins publicitaires, sauf si les utilisateurs y donnent leur consentement.

Je pense enfin au projet de loi européenne sur les données (« *Data Act* »), qui est fondamental pour promouvoir le partage de la donnée entre opérateurs dans des conditions équitables. Ce projet de texte vise ainsi à supprimer les obstacles à l'origine de la sous-utilisation des données afin de favoriser l'émergence de services innovants et de prix plus compétitifs pour le service après-vente et la réparation des objets connectés, tout en préservant les incitations des entreprises à investir dans la production de données.

Dans la perspective du Data Act, et dans le contexte plus général de l'essor des objets connectés, des données de mobilité ou encore des données de santé, comprendre le développement rapide de la production et de l'exploitation des données dans l'ensemble de l'économie mérite aujourd'hui un investissement particulier des autorités de concurrence. Notre avis en cours d'instruction sur la situation concurrentielle de l'informatique en nuage (*cloud*) pourra y contribuer.

Dans cet environnement de régulations multiples, il conviendra de continuer à échanger et à réfléchir ensemble, afin notamment de s'assurer de la bonne articulation de ces nouveaux outils avec nos actions respectives, au niveau européen et au niveau français.

Pour finir, je tiens à vous remercier, au nom de l'Autorité de la concurrence, pour cette coopération de longue date et souligner les excellentes relations de travail entre nos institutions respectives. Cette coopération s'est encore illustrée de manière très concrète par la mise en place de formations croisées des agents de nos deux institutions et je me réjouis que cette dynamique se poursuive avec l'organisation prochaine d'ateliers communs réunissant nos services.

Dans un contexte où les problématiques de protection des données et de droit de la concurrence sont toujours plus liées, il nous revient à présent de renforcer nos liens pour l'avenir, en explicitant la position de l'Autorité de la concurrence et de la CNIL sur ces sujets, aux croisements de nos actions de régulation.