

**DIRECTION DES AFFAIRES FINANCIÈRES ET DES ENTREPRISES
COMITÉ DE LA CONCURRENCE**

Compte rendu de la table ronde sur la relation entre concurrence et confidentialité des données

Annexe au compte rendu succinct de la 143e réunion du Comité de la concurrence

12-14 juin 2024

Ce document établi par le Secrétariat de l'OCDE présente un compte rendu détaillé des discussions de la table ronde sur la relation entre concurrence et confidentialité des données, organisée par le Comité de la concurrence le 13 juin 2024.

Pour toute question relative à ce document, veuillez prendre contact avec M. Antonio Capobianco.
[Courriel : Antonio.CAPOBIANCO@oecd.org]

JT03569793

Compte rendu de la table ronde sur la relation entre concurrence et confidentialité des données

1. Introduction du Président

Le 13 juin 2024, le Comité de la concurrence a organisé une table ronde sur la relation entre concurrence et confidentialité des données présidée par M. Frédéric Jenny.

Le **Président** présente la discussion et annonce qu'elle comportera trois parties. La première portera sur les liens entre politique de la concurrence et confidentialité des données, la deuxième sur l'expérience des pays dans le cadre de leurs activités d'application du droit de la concurrence et la troisième sur la question de la coopération entre les autorités de la concurrence et celles chargées de la protection des données.

Avant d'entrer dans le détail des contributions, le Président rappelle l'importance croissante des données, en particulier dans l'économie numérique, où elles sont indispensables au fonctionnement des plateformes en ligne et modèles économiques numériques. La question se pose donc de savoir si la confidentialité et le recueil de données sur les consommateurs constituent des enjeux relevant des règles de concurrence et si des critères se rapportant à la concurrence devraient être intégrés aux processus décisionnels des autorités de protection des données. Il faut aussi se demander si des facteurs jusqu'alors étrangers à un domaine d'action devraient être pris en compte dans les évaluations. Par exemple, faut-il considérer la confidentialité des données comme un critère de qualité dans les évaluations d'impact sur la concurrence, ou les conséquences sur la concurrence doivent-elles entrer en ligne de compte lors de l'application des règles relatives à la confidentialité des données ? Ces questions sont particulièrement pertinentes s'agissant des secteurs innovants, où l'on rencontre beaucoup de marchés numériques bifaces complexes et de modèles de monétisation des données, comme l'extraction de données ou l'apprentissage automatique. De surcroît, beaucoup d'autorités de la concurrence et d'autorités de protection des données commencent à coopérer sous diverses formes (ex.: plateformes ou forums).

Le Président annonce ensuite que trois orateurs invités vont faire profiter la table ronde de leurs connaissances : **Tim Capel**, qui dirige le service juridique de l'Information Commissioner's Office (ICO) du Royaume-Uni, **Katherine Kemp**, professeure associée de droit à la Faculté de droit et de justice, Université de Sydney, et **Giuseppe Colangelo**, professeur associé à l'Université de la Basilicate. Il donne ensuite la parole au **Secrétariat**, invitant **Carolina Abate** à ouvrir la discussion.

Carolina Abate se concentre sur l'interaction entre concurrence et confidentialité des données. Elle explique que même si l'application du droit de la concurrence et la confidentialité des données ont toujours constitué des domaines distincts, les choses semblent évoluer depuis peu, certaines juridictions reconnaissant que le recueil, l'accumulation et l'échange de données sur les consommateurs peuvent poser des problèmes du point de vue de la concurrence. Lorsque les consommateurs sont aussi des personnes concernées par les données, la confidentialité peut être une dimension hors prix de la concurrence. Le Secrétariat ajoute que dans le cadre d'une approche « intégrationniste » récente, la confidentialité est de plus en plus vue comme un critère à prendre en compte dans les évaluations d'impact sur la concurrence, et ce de deux manières. Premièrement, lorsque des entreprises sont en concurrence sur le degré de protection des données, les évaluations devraient en tenir compte. Deuxièmement, même lorsque la

confidentialité n'est pas directement un argument concurrentiel, il peut arriver que le pouvoir de marché des entreprises repose sur l'accumulation, l'assemblage et le traitement de données, si bien que ce traitement devient un facteur concurrentiel déterminant.

Giuseppe Bianco aborde la question complémentaire du caractère problématique ou non de la concurrence sur la confidentialité des données. Il évoque le déséquilibre entre les personnes concernées par les données et les responsables du traitement, ajoutant que les entreprises de relativement grande taille pourraient avoir plus de comptes à rendre parce qu'elles représentent un niveau de risque plus élevé dans le cadre du traitement de données à caractère personnel. Il insiste également sur la gravité des préjudices subis par les personnes. Dans ses considérants, le Règlement général sur la protection des données (RGPD) précise que le consentement peut ne pas être valable en cas de déséquilibre manifeste entre la personne concernée et le responsable du traitement. Le Secrétariat ajoute que la confidentialité des données peut fonctionner comme un atout concurrentiel parce qu'elle peut être considérée comme une dimension de la qualité et que les entreprises peuvent se faire concurrence en offrant une meilleure protection. Il insiste également sur l'importance de la notion de retrait du consentement, en particulier dans les marchés relativement peu concurrentiels où ce retrait avoir un impact négatif sur les personnes concernées par les données. Giuseppe Bianco fait observer que les autorités de protection des données cherchent de plus en plus à comprendre la dynamique des marchés et estime qu'une coopération efficace entre les différents domaines de la réglementation est essentielle.

2. Liens entre politique de la concurrence et confidentialité des données

Après avoir remercié le Secrétariat, le **Président** invite **Tim Capel** à apporter un éclairage sur le travail des autorités de protection des données et à donner son avis sur le point de savoir si des considérations liées à la concurrence devraient être prises en compte dans l'évaluation de l'autorité de protection des données ou devraient rester l'affaire de la seule autorité de la concurrence.

Tim Capel commence par expliquer que les autorités de protection des données abordent les données à caractère personnel sous l'angle des droits. Il précise que pour comprendre cette approche, il faut se rappeler de la genèse des lois sur la confidentialité des données, qui ont notamment été inspirées par l'article publié en 1890 par Samuel Warren et Louis Brandeis sous le titre « *The Right to Privacy* ». L'idée était qu'il fallait protéger les personnes du pouvoir excessif des entreprises et de l'État, une idée qui n'a rien perdu de sa pertinence à l'ère du numérique. La reconnaissance du droit au respect de la vie privée en tant que droit fondamental intervenue après la Seconde Guerre mondiale, en particulier en Europe, explique que les autorités de protection des données aient pour mission de protéger les données à caractère personnel au nom de la dignité et de l'autonomie de l'être humain.

Ces autorités reconnaissent aussi la valeur sociale de la confidentialité des données, puisqu'elles tiennent compte des préjudices résultant d'un traitement des données illicite pour la société en général. Le RGPD en est le reflet, en ce qu'il conjugue les principes d'équité, de droits pour les individus, de droit à l'effacement, etc. Si les droits individuels sont au cœur de l'interprétation des lois sur la protection des données, des cadres internationaux tels que le RGPD ont aussi pour but de faciliter la libre circulation des données à caractère personnel, ménageant un juste équilibre entre respect de la vie privée et considérations économiques. Tim Capel ajoute que les autorités de protection des données vont désormais au-delà des préoccupations habituelles relatives à la confidentialité des données pour s'intéresser aux risques liés aux données massives et la prise de décision algorithmique. Elles font aujourd'hui appel à l'analyse économique pour comprendre quels

intérêts motivent les entreprises, compte tenu de la dynamique des modèles économiques qui reposent sur des données. Les données à caractère personnel, qui sont par nature un bien non rival, peuvent être partagées sans perdre de leur valeur. Toutefois, leur accumulation par les entreprises engendre des risques pour le respect de la vie privée et réduit la transparence. L'intervenant estime que les autorités de protection des données sont de plus en plus attachées à favoriser une innovation responsable et une croissance économique durable respectueuse des droits à la protection de la vie privée. Elles souhaitent trouver un moyen terme entre la protection des informations des personnes et l'incitation à l'innovation. Elles sont cependant confrontées à des difficultés pour assurer le suivi de responsables du traitement ou de sous-traitants très divers. Tim Capel aborde également la question du lien entre confidentialité des données et concurrence. Une intervention précoce visant à empêcher tout recueil illicite de données est susceptible de limiter la concentration du marché, alors que l'inaction peut être défavorable aux entreprises respectueuses des règles. L'intervention des autorités de protection des données peut permettre de découvrir des pratiques cachées en matière de données, ce qui est un moyen d'accroître le choix des consommateurs sur la base du respect de la confidentialité des données et, sur les marchés dominés par des acteurs historiques, d'offrir des perspectives aux entreprises concurrentes. Enfin, Tim Capel cite trois domaines dans lesquels les autorités de protection des données peuvent appliquer des concepts relevant du droit de la concurrence : lorsqu'elles prennent en compte le pouvoir de marché pour évaluer la relation entre le responsable du traitement et la personne concernée par les données, lorsqu'elles plaident pour la portabilité des données et lorsqu'elles s'attaquent à l'architecture de choix en ligne et à des pratiques préjudiciables telles que la conception d'interfaces truquées visant à manipuler les utilisateurs pour qu'ils fournissent plus de données que ce qu'ils seraient prêts à communiquer volontairement. En conclusion, Tim Capel insiste sur l'importance de la coopération entre autorités de protection des données et autorités de la concurrence pour l'encadrement des marchés numériques.

Le **Président** remercie **Tim Capel** pour son avis sur le fait que les autorités de la concurrence et les autorités de protection des données peuvent coopérer. Il invite ensuite la professeure **Katherine Kemp** à s'exprimer sur la manière dont les considérations liées à la protection des données doivent être prises en compte dans l'évaluation des autorités de la concurrence et à apporter un éclairage sur les pratiques cachées en matière de données.

Katherine Kemp commence par citer les principaux obstacles qui empêchent de bien appréhender et de bien aborder les préoccupations liées à la confidentialité des données dans le cadre du droit de la concurrence, remettant en cause plusieurs mythes bien ancrés, en allant au-delà des États-Unis et de l'Union européenne (UE). Le premier mythe est l'hypothèse voulant que la protection des données ne soit qu'une question de préférence subjective des consommateurs. Selon elle, la dégradation de la protection des données est à l'origine de préjudices objectifs, augmentant le risque d'usurpation d'identité, de fraude, de manipulation et de discrimination. Le deuxième mythe est celui du « paradoxe du respect de la vie privée », selon lequel les consommateurs prétendraient être attachés à ce respect tout en continuant d'utiliser des services aux pratiques contestables en la matière. Katherine Kemp explique que souvent, les consommateurs ne connaissent pas tous les risques auxquels ils sont exposés, d'où l'impossibilité de prendre des décisions éclairées au sujet de leurs données. Le troisième mythe est celui qui fait de la démocratisation des données la solution aux problèmes. Les données à caractère personnel sont la propriété des individus et ne doivent donc pas être transformées en marchandises à des fins de concurrence. Souvent, les données anonymisées peuvent être ré-identifiées. Dès lors, le concept de démocratisation n'est pas pertinent.

Katherine Kemp explique ensuite qu'on parle de « pratiques cachées en matière de données » lorsque les entreprises ont des politiques opaques en matière de protection des

données, utilisent des interfaces truquées et se livrent à une surveillance cachée. Il est fréquent que les autorités de la concurrence ne s’y intéressent pas, considérant que ces pratiques relèvent de la réglementation relative à la protection des données. Or, cette séparation des domaines peut engendrer des lacunes importantes, comme en témoigne la fusion Google/DoubleClick. Elle rappelle que Google avait initialement promis de ne pas regrouper ses données sur les recherches des internautes avec celles de DoubleClick, mais est ensuite revenue sur cet engagement sans en subir de réelles conséquences. Cette affaire montre bien que l’absence de coordination entre les autorités chargées de la concurrence et celles compétentes en matière de protection des données peut entraîner des préjudices à la vie privée qui peuvent aussi fausser la concurrence.

Évoquant l’évolution de l’intelligence artificielle (IA), l’intervenante décrit les problèmes que pose l’utilisation par les entreprises d’énormes volumes de données pour entraîner les modèles au mépris des règles relatives à la protection des données. La concurrence que se livrent les entreprises technologiques dans le domaine de l’IA, par exemple les tentatives de Meta d’imiter la stratégie de Google, est la preuve de la nécessité d’appliquer avec rigueur les règles relatives à la protection des données afin d’éviter un nivellement par le bas des normes relatives à la protection des données. Katherine Kemp cite également les exemples de l’approche adoptée par le Bundeskartellamt, en Allemagne, dans l’affaire Meta et l’importance récemment donnée par la Federal Trade Commission, aux États-Unis, au respect de la vie privée des consommateurs. Toutefois, ces approches sont peut-être difficilement transposables à des juridictions appliquant d’autres cadres réglementaires, en particulier lorsque le droit de la concurrence est davantage axé sur les pratiques d’éviction que sur la dégradation de la protection des données. En conclusion, Katherine Kemp rappelle qu’il est important que les autorités de la concurrence et les autorités de protection des données collaborent pour harmoniser leurs interventions.

3. Expérience des pays en matière d’application des règles relatives à la confidentialité des données

Le **Président** remercie Katherine Kemp et passe aux contributions individuelles des pays. Il invite l’**Italie** à s’exprimer sur l’articulation entre protection des données à caractère personnel et soutien à la concurrence.

L’**Italie** évoque l’importante expérience accumulée par le pays en matière de données massives, notamment une enquête sectorielle multidisciplinaire lancée en 2018. Chaque autorité poursuivait des objectifs distincts, ce qui a mis en lumière les synergies et éventuelles contradictions existant entre des objectifs de cadres réglementaires différents. Le délégué souligne qu’il est important de comprendre les modèles économiques qui sous-tendent les activités dans le secteur numérique au lieu de se concentrer exclusivement sur un comportement précis. Les entreprises numériques recueillent des données en proposant des services initialement gratuits afin d’accumuler des utilisateurs et des données, exploitant les effets de réseaux et les marchés bifaces. Une fois qu’elles ont acquis un pouvoir de marché, elles commencent à monétiser un côté du marché tout en continuant d’accumuler des données. L’Italie cite l’exemple de la fusion Facebook/WhatsApp et fait observer que l’autorité de protection des données et celle de la concurrence ont joué un rôle central dans la surveillance des premières phases de l’acquisition de données, se penchant sur des questions telles que les informations trompeuses, les invites en ligne et les choix par défaut qui exploitent les biais comportementaux pour obtenir le consentement des utilisateurs. À cela s’ajoutent des préoccupations au sujet d’entreprises qui refusent l’interopérabilité, comme dans les affaires Google/Android et Google/Hoda. Ces affaires, de même que l’affaire Apple/ATTF, qui est en cours, montrent que les pratiques en matière

de protection de la vie privée et de données peuvent être des stratégies utilisées pour conserver un pouvoir de marché. L'Italie souligne qu'il est important de comprendre les facteurs qui motivent l'adoption de ces modèles économiques.

Après avoir remercié l'Italie, le **Président** invite la **FTC (États-Unis)** à s'exprimer sur l'interaction entre confidentialité des données et concurrence.

La **FTC** répond que même si la protection de la confidentialité des données a été considérée comme une dimension hors prix de la concurrence dans quelques interventions visant à faire respecter le droit de la concurrence, il n'en a pas découlé d'améliorations de cette protection à l'échelle sectorielle. En réalité, dans divers secteurs, les entreprises continuent de collecter d'énormes volumes de données et d'effectuer un traçage des consommateurs, souvent en utilisant la publicité numérique. La plupart du temps, les consommateurs n'ont pas conscience des grandes quantités de données recueillies et des préjudices qui peuvent en résulter. Parmi les affaires notables figure celle impliquant Rite Aid, une importante chaîne pharmaceutique aux États-Unis, qui utilisait la reconnaissance faciale depuis huit ans pour surveiller ses clients. La FTC a estimé que Rite Aid n'avait rien fait pour empêcher le préjudice aux consommateurs, et l'entreprise a accepté une mesure lui interdisant pendant cinq ans de faire appel à la reconnaissance faciale à des fins de surveillance et lui imposant des règles strictes pour l'utilisation future de technologies biométriques. La FTC estime en outre que le modèle « *notice-and-consent* » (informer et obtenir le consentement) ne protège pas correctement le consommateur, les politiques relatives à la confidentialité des données étant souvent difficiles à comprendre et les entreprises faisant appel à des « interfaces truquées » pour orienter les consommateurs vers des choix dans lesquels la protection des données est minimale. Pour y remédier, la FTC cherche à imposer des protections de la confidentialité exigeantes, par exemple en restreignant la possibilité d'échanger des informations sensibles comme les données de géolocalisation. Elle indique en outre envisager des règles qui pourraient agir sur l'intérêt que les entreprises ont à s'engager dans une surveillance numérique massive et qui pourraient stimuler la concurrence en favorisant l'adoption de modèles économiques qui ne reposent pas sur ce type de pratiques, ce qui permettrait peut-être à de nouveaux entrants ne possédant pas de gros volumes de données de livrer une concurrence plus effective. Enfin, la FTC avance qu'il est possible de favoriser à la fois la protection des données et la concurrence en créant un régime permettant de tenir compte des préoccupations relatives à cette protection dans le cadre des interventions, du processus normatif ou de la législation.

Le représentant de la FTC donne ensuite la parole à celui du **ministère de la Justice des États-Unis (DOJ)**, qui ajoute que les lignes directrices relatives au contrôle des fusions publiées en 2023 reconnaissent qu'il existe de nombreuses dimensions de la concurrence, dont des dimensions liées à la qualité telles que les dispositions relatives à la protection des données (ex.: le contentieux impliquant Google Search).

Après avoir remercié les délégués, le **Président** demande à l'**Autriche** de s'exprimer sur la synergie entre droit de la concurrence et confidentialité des données.

L'**Autriche** souligne qu'il est de plus en plus important de conjuguer ces deux aspects en adoptant la théorie qui fait de la protection de la confidentialité des données une composante de la qualité. Lorsque des entreprises se font concurrence sur la base de normes de respect de la vie privée, la protection des données devient un aspect important de la concurrence. La modification des conditions d'utilisation de WhatsApp, en 2021, qui a temporairement entraîné une vague de départs d'utilisateurs au profit de services de messagerie protégeant mieux la confidentialité des données est un exemple qui illustre bien le rôle de la protection des données en droit de la concurrence. Le projet de fusion entre Facebook et GIPHY, bloqué parce qu'il risquait de renforcer encore les capacités de collecte de données de Facebook et d'accroître les barrières à l'entrée, fournit un autre

exemple. En conclusion, l'Autriche souligne que la protection des données est cruciale pour le droit de la concurrence, les préférences des consommateurs évoluant en faveur de produits et services qui garantissent une meilleure protection des données.

Le **Président** remercie l'Autriche et donne la parole au **Costa Rica**.

Le Costa Rica commence par expliquer que la législation sur la protection des données actuellement en vigueur, qui date de 2011, n'est pas adaptée à l'environnement numérique. Deux projets de loi sont donc actuellement examinés. Ils visent à moderniser le cadre réglementaire, en particulier pour que les individus aient des droits sur leurs données – droits d'accès, d'opposition, de portabilité des données, entre autres. Les deux autorités de la concurrence existant au Costa Rica (Copromcom et Sutel) ont défini six aspects essentiels à prendre en compte pour définir ce nouveau cadre juridique. Le premier est la nécessité d'encourager la collaboration entre différents organismes publics pour éviter un cloisonnement rigide entre les autorités chargées de la concurrence, des consommateurs et de la protection des données. Deuxièmement, les nouvelles règles ne doivent pas être trop coûteuses à respecter. Le troisième aspect est la nécessité de ne pas oublier que l'obligation d'obtenir le consentement exprès pourrait surtout pénaliser les entreprises de petite taille ou de création récente, ce qui pourrait avoir un impact sur la concurrence. Quatrièmement, il faut avoir conscience que des lois plus exigeantes en matière de protection des données limitent la capacité des nouvelles entreprises à acquérir des données sur les consommateurs, ce qui revient à conférer un avantage concurrentiel aux entreprises en place. Cinquièmement, il faut veiller à concevoir avec soin les mécanismes de portabilité des données pour lever les risques liés au transfert de données. Enfin, il serait bon que l'autorité de protection des données ait le pouvoir de conclure des accords de coopération avec d'autres organismes pour garantir une coordination.

Après avoir remercié le Costa Rica, le **Président** demande à **Israël** de présenter son cadre en matière de portabilité des données.

Israël présente l'initiative relative à la portabilité des données prise conjointement par l'autorité israélienne de la concurrence, l'autorité chargée de la protection des données et celle chargée de la protection des consommateurs. L'objectif était de permettre au consommateur d'avoir le choix et d'augmenter la mobilité entre prestataires de services. L'équipe tripartite a publié un rapport recommandant l'introduction d'un droit général à la portabilité des données dans le droit israélien. Bien que ce droit n'ait pour l'heure pas encore été inscrit dans la législation, les principes défendus par le rapport ont été appliqués dans des réformes pilotées par l'autorité de la concurrence. Ce fut notamment le cas lors de la mise en œuvre de la portabilité des données dans le secteur financier, en particulier concernant le transfert de données financières issues des comptes joints. L'autorité de protection des données estimait qu'il fallait obtenir le consentement de tous les titulaires du compte alors que l'autorité de la concurrence souhaitait simplifier les démarches pour les consommateurs. Un compromis a finalement été trouvé : il a été décidé que le consentement d'un seul titulaire serait nécessaire à condition que les autres titulaires soient informés sans délai et aient le droit de révoquer le consentement. En conclusion, Israël indique que le fait d'avoir soulevé les désaccords entre les autorités et d'en avoir discuté pendant la rédaction du rapport a facilité la coopération ultérieure.

Le **Président** remercie Israël et invite **Giuseppe Colangelo** à présenter la partie suivante des débats.

4. Coopération entre autorités de la concurrence et autorités de protection des données

Giuseppe Colangelo présente une analyse de l'intégration entre droit de la concurrence et de la protection des données en s'appuyant sur un article récent cité dans la note de référence du Secrétariat de l'OCDE. Deux grandes visions peuvent être distinguées : la vision dite « intégrationniste », qui considère que le droit relatif à la protection des données et celui de la concurrence peuvent se compléter, et l'approche dite « séparatiste », qui traduit une méfiance vis-à-vis de l'intégration des questions relatives à la confidentialité des données dans les interventions visant à faire respecter le droit de la concurrence. Selon la première approche, les autorités de la concurrence devraient examiner si les stratégies d'accumulation de données nuisent à la protection de la vie privée et augmentent le pouvoir de marché. En revanche, les tenants de l'approche séparatiste, dont l'intervenant fait partie, estiment que les deux corpus juridiques poursuivent des objectifs différents et que les regrouper pourraient avoir des conséquences secondaires négatives. Par exemple, les entreprises pourraient exploiter les règles relatives à la protection des données pour justifier un comportement anticoncurrentiel. Selon lui, l'affaire allemande « Facebook » illustre cette approche, les pratiques de Facebook en matière d'accumulation de données ayant été traitées comme une exploitation abusive, par l'entreprise, de son pouvoir de marché. Il oppose à cette approche le règlement de l'UE sur les marchés numériques, lequel introduit une exception au titre de la protection des données qui souligne le rôle du RGPD lorsqu'il s'agit de déterminer la légalité du traitement des données et qui peut donc conduire à faire primer la protection des données sur les problèmes de concurrence. Giuseppe Colangelo fait en outre observer que le contrôle des concentrations est un domaine dans lequel une approche intégrée serait mieux à même de limiter l'accumulation de données, mais que la Commission européenne a rarement bloqué un projet de fusion sur la seule base de problèmes de protection des données.

Il présente plusieurs affaires illustrant l'utilisation que les entreprises peuvent faire de la question de la protection des données pour se mettre à l'abri d'interventions pour infraction au droit de la concurrence, par exemple l'affaire Apple/ATTF et l'affaire impliquant le « bac à sable vie privée » de Google, dans lesquelles des mesures visant à garantir la confidentialité des données ont été invoquées pour justifier des actions potentiellement anticoncurrentielles. Il présente quatre grandes théories du préjudice concernant l'approche intégrée. La première repose sur l'idée qu'il existe un lien entre le manque de concurrence, les marchés numériques et la confidentialité des données, la deuxième concerne le contrôle des fusions, à savoir que l'accumulation de données lors de fusions comme celle impliquant DoubleClick exige un contrôle rigoureux compte tenu du risque de violation des règles relatives à la protection des données. La troisième considère la confidentialité des données comme une composante de la qualité des produits et services. La dernière concerne les situations dans lesquelles les individus sont obligés d'accepter des conditions non respectueuses de la vie privée dans le cadre de modèles fondés sur le principe « à prendre ou à laisser ». L'affaire Meta marque une étape importante pour ce qui est de la clarification du lien juridique entre protection des données et droit de la concurrence, la Cour de justice européenne ayant estimé que les autorités de la concurrence pouvaient tenir compte d'aspects liés à la protection des données même lorsque les pratiques en cause étaient conformes au RGPD. Giuseppe Colangelo relève toutefois que l'arrêt de la Cour ne résout pas totalement les difficultés liées au rapprochement des deux domaines, en particulier en l'absence de violation claire du RGPD. L'affaire Telepass, en Italie, dans laquelle l'autorité de protection des données est intervenue, illustre ces difficultés. L'intervenant termine son propos en mettant en garde contre un trop grand recours à l'approche intégrée, faisant observer que la coopération entre les autorités de la concurrence et celles chargées de la protection des données est certes utile s'agissant de l'application du RGPD, mais ne permet

pas d'éliminer les contradictions entre préoccupations concernant la protection des données et comportement anticoncurrentiel. Le risque est que la confidentialité des données soit considérée comme un « bien de valeur supérieure » et l'emporte sur les objectifs du droit de la concurrence.

Le **Président** remercie Giuseppe Colangelo et donne la parole à **Katherine Kemp**, puis à **Tim Capel**.

Katherine Kemp souligne qu'il est de plus en plus fréquent que les entreprises justifient un comportement potentiellement anticoncurrentiel en invoquant la nécessité de protéger la vie privée des consommateurs. L'affaire qui a impliqué le Toronto Real Estate Board (TREB) au Canada il y a une dizaine d'années en est une illustration remarquable : la cour d'appel fédérale a écarté l'argument tiré du respect de la confidentialité des données invoqué dans une affaire d'abus de position dominante en considérant qu'il ne s'agissait que d'un prétexte, quand bien même ce type d'argument était considéré comme recevable en principe. Récemment, de grandes plateformes numériques ont commencé à définir leurs propres règles en matière de confidentialité des données au sein de leurs propres écosystèmes. Certains de ces arguments tirés de la confidentialité des données sont en réalité des prétextes qui visent à obtenir un avantage concurrentiel sur les concurrents. Alors que ces plateformes excluent des concurrents au nom du respect de la vie privée des consommateurs, elles partagent souvent librement les données à caractère personnel au sein de leurs diverses entités, sans se préoccuper du principe de limitation de la finalité contenu dans les règles sur la confidentialité des données. L'une des questions importantes qui se pose pour les autorités concerne le point de savoir s'il faudrait que les entreprises concurrentes aient aussi accès à ces données pour des raisons d'équité ou s'il faut plutôt empêcher le regroupement de données entre différentes entités d'une même entreprise. L'intervenante est favorable à la deuxième approche et met en garde contre un excès de scepticisme à l'égard des moyens de défense tirés de la protection des données. Par ailleurs, il peut arriver que des améliorations de la protection des données pour les consommateurs se produisent dans un marché alors que les préjudices à la concurrence ont lieu dans un autre, ce qui empêche les entreprises d'utiliser l'argument de la confidentialité des données pour justifier leur comportement. Katherine Kemp estime qu'il faut harmoniser le droit relatif à la protection de la vie privée et le droit de la concurrence pour obtenir des réponses cohérentes et claires des autorités.

Tim Capel estime que les autorités de protection des données doivent jouer un rôle plus offensif dans les affaires qui concernent aussi le droit de la concurrence. Selon lui, les interventions dans le champ de la protection des données pourraient être favorables à la concurrence parce qu'elles luttent contre les pratiques qui contribuent à la concentration du marché, comme l'accumulation de données et l'extraction de données à partir de pages web. Des débats sont en cours parmi les acteurs de la protection des données concernant la meilleure manière d'aborder ces questions, notamment à travers la clarification des cadres juridiques et l'amélioration de la coopération avec les autorités de la concurrence. L'intervenant insiste sur l'importance de la collaboration entre autorités de la concurrence et autorités de protection des données, en particulier en Europe. Par ailleurs, dans l'affaire relative au « bac à sable vie privée » de Google, par exemple, l'Information Commissioner's Office (ICO) du Royaume-Uni a joué un rôle fondamental, apportant ses compétences à la Competition and Markets Authority (CMA) et examinant les arguments tirés de la protection des données avancés par Google. Enfin, il pense que même s'il subsiste des écueils, le renforcement du dialogue entre autorités est positif et devrait faciliter la résolution de ces questions complexes.

Le **Président** remercie les experts et invite l'**Italie** à faire part de ses commentaires.

L'**Italie** insiste sur l'importance de la coopération entre autorités, en particulier concernant de nouveaux règlements tels que ceux sur les services numériques, sur les marchés numériques et sur les données. L'objectif devrait être de garantir que le traitement des affaires ne se heurte pas à des lacunes réglementaires. Tout en reconnaissant que les contradictions évoquées pourraient conduire à l'annulation de certaines décisions, le délégué se veut optimiste, citant des affaires impliquant de grandes entreprises comme WhatsApp, Apple, Google, Meta et TikTok, dont beaucoup sont en cours ou ont abouti à une confirmation des décisions. Il invite les autorités à continuer de repousser les frontières dans le traitement des affaires.

Après avoir remercié l'Italie, le **Président** demande à **Tim Capel** comment il voit la protection de la vie privée comparativement à d'autres droits tels que la liberté d'entreprendre et s'il considère que les règles qui la protègent se situent à égalité avec le droit de la concurrence ou si elles sont différentes.

Tim Capel commence par rappeler que le respect de la vie privée est un droit fondamental, qui puise ses racines dans des inquiétudes anciennes au sujet de l'accumulation de données et de la perte d'autonomie individuelle. Il reconnaît que concilier ce droit avec d'autres, comme la liberté d'entreprendre, n'est pas tâche aisée et insiste sur la nécessité que des autorités distinctes soient chargées de la protection des données et de la concurrence, tout en reconnaissant un risque de conflit. La coopération entre ces autorités est indispensable, parce que la désignation de l'autorité compétente pour diriger certaines enquêtes est parfois une décision difficile. Enfin, Tim Capel rappelle l'importance du principe de proportionnalité dans les décisions et plaide pour que les autorités dialoguent avec les pouvoirs publics afin de trouver des réponses à ces questions complexes.

Le **Président** remercie Tim Capel avant d'inviter l'**Espagne** à intervenir.

L'**Espagne** explique que l'article 3 de la loi espagnole sur la concurrence permet l'examen de pratiques de concurrence déloyales dès lors qu'elles ont un impact sur la concurrence au sens des articles 101 et 102 du Traité sur le fonctionnement de l'UE (TFUE). Il faut rapporter la preuve des violations de la loi, par exemple des manquements aux règles sur la confidentialité des données, et de leur impact sur la concurrence. Les juges peuvent appliquer la législation sur la concurrence déloyale sans avoir à prouver l'impact sur le marché, mais les autorités de la concurrence sont seules compétentes en cas d'incidence sur la structure du marché ou le bien-être du consommateur. L'article 3 permet d'appliquer le droit sans avoir à prouver l'existence d'une position dominante, ce qui offre une certaine souplesse pour de futures affaires.

Le **Président** remercie l'Espagne et propose à l'**UE** d'évoquer les manières concrètes dont le droit de la concurrence et la protection des données se sont chevauchées dans différentes juridictions.

L'**UE** commence par noter que la protection des données joue un rôle dans les affaires de fusion et d'infractions au droit de la concurrence, que ce soit dans les théories du préjudice ou dans la conception des mesures correctives. Dans le domaine du contrôle des fusions, les règles relatives à la protection des données peuvent avoir une incidence en limitant les effets liés aux données, comme dans les affaires Meta et Google/Fitbit par exemple. Qui plus est, l'UE évalue si une fusion réduit la concurrence sur la protection des données, comme dans l'affaire Microsoft/LinkedIn. Dans les affaires d'infractions au droit de la concurrence, en particulier de position dominante, les considérations liées à la protection des données proviennent du comportement de l'entreprise ou en font partie intégrante. Du point de vue des procédures, la Commission européenne coopère avec les autorités de protection des données pour garantir une cohérence des décisions. Enfin, les préoccupations liées à la protection des données influent également sur la conception des

mesures correctives, en particulier concernant l'accès aux données ou leur portabilité, comme en témoigne l'affaire Google/Fitbit. Toutefois, la pertinence de ce type de mesures correctives dépend de chaque affaire.

Le **Président** remercie l'UE et invite le **Brésil** à parler de l'affaire « Magalu Pagamentos et Hub ».

Le **Brésil** explique que la confidentialité des données relève de la compétence de l'Autorité brésilienne de protection des données, et que les problèmes liés à cette question sont analysés au cas par cas. Le CADE l'a démontré en 2021, lors du contrôle d'une fusion entre Magalu Pagamentos et Hub Prepaid. Malgré l'existence de problèmes, il a autorisé l'opération sans restriction, faisant valoir que la conformité à la loi sur la protection des données suffisait à empêcher toute utilisation abusive des données. Par ailleurs, le CADE soutient des politiques favorables à la concurrence et collabore avec d'autres organismes. Cette collaboration apparaît de manière évidente dans une affaire dans laquelle la modification de la politique de WhatsApp en matière de confidentialité des données obligeait les utilisateurs à partager leurs données avec Facebook sous peine de ne plus avoir accès à l'application. Le CADE a publié une recommandation commune pour empêcher WhatsApp d'appliquer ses nouvelles règles. En résumé, la politique de la concurrence peut indirectement protéger la confidentialité des données en la considérant comme une dimension de la qualité, mais la protection de la vie privée ne constitue pas son objectif premier au Brésil.

Le **Président** remercie le Brésil et propose à la **Grèce** de présenter sa théorie du préjudice en matière de confidentialité des données dans le contexte du contrôle des fusions.

La **Grèce** précise d'abord qu'en 2022, l'autorité grecque de la concurrence (HCC) a évalué une fusion numérique impliquant Delivery Hero, une entreprise ayant son siège à Berlin et exploitant une plateforme de livraison de repas, et E-Table, la principale plateforme de réservation de restaurants en Grèce. La HCC craignait d'abord que l'opération n'ait des effets de conglomerat et ne permette le déploiement de stratégies de promotion personnalisées sur la base des données fusionnées, ce qui aurait encore renforcé la position de marché de l'entité. Elle a examiné ce risque en faisant appel à des théories du préjudice, en particulier à l'agrégation des données et au couplage fondé sur la politique de protection des données, et a conclu que l'opération risquait d'avoir des effets d'exploitation parce qu'elle limiterait la protection de la vie privée des consommateurs. La HCC a également estimé qu'il y avait des risques associés à l'intégration verticale, à savoir que l'entité issue de la fusion pourrait avoir accès à des informations sensibles sur des concurrents. La fusion a finalement été autorisée sous réserve de mesures correctives, par exemple une interdiction stricte de fusionner les données sur les consommateurs détenues par les deux plateformes sauf consentement exprès des utilisateurs conformément au RGPD, en particulier à l'article 51.

Le **Président** remercie la Grèce et invite l'**Allemagne** (le **Bundeskartellamt**) à présenter la décision majeure prise dans l'affaire Meta et les principaux éléments matériels de cette affaire.

L'**Allemagne** explique qu'en 2019, le Bundeskartellamt a ouvert une enquête sur le comportement abusif de Meta en matière de collecte de données sur les utilisateurs. L'enquête a été axée sur la position dominante de l'entreprise sur le marché et sur ses pratiques consistant à collecter des données de façon illimitée. Le Bundeskartellamt a utilisé le RGPD comme référence sans pour autant appliquer directement la législation relative à la protection des données. Meta a contesté la décision, ce qui s'est soldé par de multiples procédures juridiques, dont un renvoi préjudiciel devant la Cour de justice européenne. La Cour a finalement confirmé qu'il était loisible aux autorités de la

concurrence de prendre en compte les règles sur la protection des données et a insisté sur la nécessité d'une coopération entre les autorités de la concurrence et de protection des données. Trois conclusions essentielles peuvent en être tirées : premièrement, les pratiques de Meta en matière de données ont été jugées abusives vis-à-vis des consommateurs, contraints d'accepter la collecte d'un gros volume de données ; deuxièmement, il y a eu une pratique d'éviction des concurrents de Meta, qui n'avaient pas le même accès aux données des utilisateurs ; enfin, il faut offrir aux utilisateurs une version du service qui ne traite que les données à caractère personnel nécessaires à la fourniture du service, éventuellement moyennant paiement d'un prix approprié. L'Allemagne ajoute que cette affaire n'est pas un cas isolé et a eu un impact sur la législation, notamment sur l'article 19a de la loi allemande sur la concurrence et sur l'article 5, paragraphe 2, du règlement européen sur les marchés numériques. Des affaires similaires sont apparues depuis, par exemple l'affaire Google Data et l'enquête en cours dans l'affaire Apple/ATTF. Cette enquête concerne des risques d'autofavoritisme et d'entrave à des tiers plutôt que des risques d'abus. Le système de traçage d'Apple exige un consentement supplémentaire pour pouvoir suivre les utilisateurs sur des applications et sites Internet tiers. Toutefois ce système de traçage (ATTF) ne semblait pas s'appliquer à ses propres services, ce qui signifie que l'affaire concernait la sélection de l'entreprise pouvant acquérir des données. Apple soutient qu'elle privilégie la protection des données, mais cette approche ne concerne apparemment que les entreprises externes et non ses propres services, ce qui pose une question fondamentale, à savoir celle de savoir si l'accès aux données doit être gouverné par la loi ou par les acteurs en position dominante.

L'Allemagne évoque également l'affaire Facebook, qui a commencé en 2019, et qui n'a toujours pas été résolue malgré les multiples phases judiciaires par lesquelles elle est passée. Le délégué signale les retards non négligeables causés par l'utilisation, par les entreprises, de toutes les voies juridiques possibles pour différer les décisions et s'interroge sur la capacité du cadre juridique actuel à permettre un traitement efficace de ce type d'affaires alors que les technologies évoluent rapidement. Il déplore cette lenteur, soulignant que les entreprises utilisent souvent des tactiques dilatoires. Les activités se transformant à vive allure sous l'effet de l'IA, il se demande si le cadre juridique actuel est de nature à permettre un traitement adapté d'affaires anciennes dans un monde qui évolue rapidement.

Le **Président** reconnaît l'importance du dernier commentaire du délégué allemand avant de donner la parole à la **France**.

La **France** insiste sur l'importance de la collaboration entre les autorités de la concurrence et les autorités de protection des données, y compris en cas de désaccords. Cette collaboration est essentielle pour se repérer dans le paysage réglementaire et garantir que les entreprises savent ce qu'elles ont à faire pour respecter le droit relatif à la confidentialité des données et celui de la concurrence, *a fortiori* dans un environnement juridique et technologique qui change vite. Le délégué se dit surpris d'entendre le professeur Giuseppe Colangelo affirmer que la coopération est un problème en soi. En effet, même si elle peut conduire à des conclusions différentes, la coopération n'en demeure pas moins une obligation légale et les entreprises devraient être informées de la façon dont les deux autorités interagissent. Il cite l'exemple de la collaboration accrue entre l'Autorité de la concurrence et la CNIL (l'autorité de protection des données française). Cette collaboration prend la forme de séminaires et ateliers communs et a été renforcée par la signature d'un protocole de coopération. L'une des premières affaires examinées est l'affaire Meta, qui concerne un domaine où le paysage juridique relatif à la confidentialité des données et à la concurrence a beaucoup évolué. La coopération transparaît aussi dans les nouveaux textes législatifs adoptés au niveau européen, par exemple les règlements sur les marchés numériques, sur les données, sur la gouvernance des données et sur l'IA. Le délégué

souligne que les autorités doivent clarifier la façon dont ces règlements seront appliqués et interprétés.

Il cite l'exemple de l'enquête ouverte par l'Autorité de la concurrence contre Google, qui a abouti à l'imposition de 250 millions EUR d'amende en lien avec des droits voisins se rapportant à des contenus de presse. Cette affaire n'impliquait certes pas de données à caractère personnel, mais elle était centrée sur des droits de propriété intellectuelle et sur le fait que Google n'avait pas informé les éditeurs ou ne leur avait pas permis de refuser l'utilisation des données. Elle illustre la complexité du traitement des données et les intérêts qui sont communs au droit relatif à la protection de la vie privée et au droit de la concurrence, même lorsque l'objet de l'affaire outrepassé les préoccupations habituelles en matière de confidentialité des données. L'affaire ATTF est un autre exemple de cette interaction. En l'espèce, il s'agissait de déterminer si les pratiques d'Apple étaient discriminatoires à l'égard de ses concurrents et favorisaient ses propres services. La CNIL a fourni des recommandations d'après les exigences en matière de consentement prévues par la loi sur la protection des données, mais l'Autorité de la concurrence a surtout cherché à déterminer si les actions d'Apple étaient constitutives d'un comportement discriminatoire. Cette affaire illustre la complémentarité des deux corpus juridiques, l'autorité de la concurrence reconnaissant que la protection de la vie privée des consommateurs peut être un objectif légitime en droit de la concurrence.

Le délégué français évoque aussi les problèmes liés à la longueur des procédures judiciaires, en particulier lorsque de grandes entreprises technologiques sont impliquées. Ces entreprises ont les moyens de retarder l'aboutissement des procédures, ce qui constitue une difficulté pour des autorités de réglementation qui cherchent à suivre le rythme rapide des changements technologiques. Il existe en outre un déséquilibre entre concurrence et protection de la vie privée dans les décisions européennes. Alors que la vie privée est un droit fondamental protégé par l'article 8 de la Convention européenne des droits de l'homme, le droit de la concurrence n'a pas toujours le même poids, même quand les deux enjeux sont importants. En conclusion, le délégué souligne que même si les contradictions entre les règles sur la protection des données et la concurrence sont appelées à perdurer, une coopération étroite entre les autorités compétentes est indispensable.

Le **Président** remercie la France pour sa contribution et introduit la dernière partie de la discussion, en l'occurrence les modèles de coopération et l'expérience en matière de coopération entre autorités de protection des données et autorités de la concurrence. Il passe ensuite la parole au **Royaume-Uni**.

5. Modèles de coopération entre les autorités de protection des données et les autorités de la concurrence

Le **Royaume-Uni** est représenté par **Andrew Thompson**, de l'ICO, et par **Noel Tarleton**, de la CMA, qui commence par se présenter. **Andrew Thompson** (ICO) évoque ensuite l'interaction croissante entre la protection des données et la concurrence dans les marchés numériques, précisant que ces aspects ayant déjà été décrits, il n'y reviendrait pas. Il préfère se concentrer sur des considérations pratiques et sur la coopération entre les autorités, grandement facilitée par le Digital Regulation Cooperation Forum (DRCF) au Royaume-Uni. Le DRCF a été créé pour examiner les perspectives et défis nés des marchés numériques, qui transcendent souvent les frontières traditionnelles entre domaines de la réglementation. Son cadre de fonctionnement est souple et il coordonne les efforts déployés dans des domaines où la coopération aura le plus fort impact public. Une équipe centrale dotée en personnel, dirigée par Kate Jones, définit l'orientation stratégique et assure la

coordination. Le DRCF veille également à l'implication de responsables des quatre autorités à travers l'organisation de réunions trimestrielles et l'établissement de plans de travail annuels. Depuis 2020, l'ICO et la CMA se sont concentrés sur plusieurs priorités d'intérêt mutuel, notamment la publication de communiqués communs sur l'affaire du « bac à sable vie privée » de Google et sur les écosystèmes mobiles, en particulier le dispositif ATTF d'Apple et le partage d'information. La note de position commune sur les interfaces en ligne dommageables, publiée en 2023, est un autre exemple de coopération. Ce document portait sur la manière de permettre au consommateur d'avoir un choix et un contrôle réels et abordait la transparence et l'autonomie du consommateur. Il décrivait également des comportements tels que le fait d'inciter les utilisateurs à accepter des pratiques contre leur gré en matière de données et contenait des recommandations à suivre par les entreprises pour concevoir des architectures de choix favorables aux consommateurs du point de vue de la protection des données et de la concurrence.

Andrew Thompson laisse ensuite **Noel Tarleton** continuer la présentation.

Noel Tarleton souligne que les modèles de fondation et l'IA générative évoluent rapidement, d'où la nécessité pour les autorités de réglementation de faire preuve d'anticipation. La CMA a lancé son enquête sur les modèles de fondation en mai 2023 et a publié des rapports en septembre et avril. Parallèlement, l'ICO a ouvert une consultation sur l'IA générative et la protection des données, ce qui témoigne du besoin de plus en plus grand d'influer sur le marché au lieu de réagir à des problèmes qui apparaissent. Le rapport publié en avril par la CMA propose des principes essentiels pour orienter l'évolution du marché. Le communiqué commun de la CMA et de l'ICO visait à explorer d'éventuels sujets d'intérêt commun et à garantir une approche cohérente des réglementations. Noel Tarleton cite l'exemple de la transparence de l'utilisation des données, essentielle pour la protection des consommateurs comme pour la protection des données. Par ailleurs, la CMA et l'ICO revoient actuellement leur communiqué commun de 2021, qui concernaient les synergies et les conflits entre protection des données et concurrence. La nécessité de veiller à ce que les entreprises n'utilisent pas la réglementation sur la protection des données comme un prétexte pour justifier un comportement anticoncurrentiel est un enjeu important. À titre d'exemple, toute intervention des autorités de la concurrence doit tenir compte des conséquences de la protection des données – l'affaire relative au « bac à sable vie privée » de Google en est une illustration. Dans sa version actualisée en 2025, le communiqué portera sans doute sur des thèmes tels que l'accès aux données, le partage des données, l'interopérabilité et le choix des utilisateurs.

Dans la dernière partie de la présentation, **Andrew Thompson** souligne que la coopération entre l'ICO et la CMA ne se limite pas à des priorités bilatérales. Elle associe également l'Ofcom et la Financial Conduct Authority (FCA), dans le cadre de projets plus vastes menés sous l'égide du DRCF. Les travaux sur l'IA constituent une initiative majeure, qui vise à analyser les avantages et dangers de l'IA, à garantir la cohérence de concepts essentiels tels que l'équité et la responsabilité et à approfondir la compréhension de l'audit de l'IA. Par ailleurs, le DRCF réalise des analyses prospectives pour assurer une veille des technologies émergentes telles que l'informatique quantique, le web 3.0, les technologies immersives et l'identité numérique. Un projet visant à renforcer les compétences du personnel des autorités de réglementation est également en cours, l'objectif étant surtout de constituer et d'entretenir un vivier de talents en s'appuyant sur la formation. À cela s'ajoute un projet pilote financé par des fonds publics et ayant pour but de fournir des conseils aux porteurs d'innovation concernés par plusieurs domaines de la réglementation. L'intervenant encourage les parties prenantes à explorer le site internet du DRCF pour de plus amples informations sur ces projets.

Le **Président** remercie le Royaume-Uni et pose deux questions : (a) la coopération est-elle nécessaire ? et (b) le communiqué commun reflète-t-il un consensus absolu ou rend-il compte de différences sur certains points ?

Andrew Thompson reconnaît qu'il est difficile d'éliminer les conflits entre accès aux données et protection de la vie privée. Il prend l'exemple de l'accès aux données, qui peut éliminer les barrières à l'entrée et promouvoir la concurrence, mais aussi nuire au respect de la vie privée et engendrer de nouveaux risques. La solution consiste à concevoir des mesures correctives qui privilégient la protection des données et l'équité dès la conception. Cette approche exige parfois des compromis mais doit permettre de parvenir à une solution pragmatique et équilibrée tenant compte à la fois des inquiétudes pour la protection de la vie privée et des préoccupations relatives à la concurrence.

Noel Tarleton confirme que toutes les contradictions entre protection des données et concurrence ne peuvent pas être éliminées. Même s'il subsiste des difficultés, le principal objectif est la clarté, en particulier s'agissant des situations dans lesquelles les entreprises utilisent les arguments relatifs à la protection des données comme prétexte.

Le **Président** remercie les délégués du Royaume-Uni pour leur présentation et invite le **Canada** à faire part de son expérience en matière de coopération.

En juin 2023, le **Canada** a créé un forum des organismes de réglementation qui a pour but de favoriser la collaboration et la mise en commun d'informations entre organismes fédéraux. Ce forum regroupe le Bureau de la concurrence, le Conseil de la radiodiffusion et des télécommunications canadiennes et le Commissariat à la protection de la vie privée. Il a principalement vocation à examiner des questions complexes liées au marché numérique et à renforcer la coopération entre les domaines de compétence. Durant sa première année de fonctionnement, il s'est attaché à permettre aux organismes d'établir des liens et de comprendre les compétences des autres. Il s'est également concentré sur l'IA, retenue en raison de son évolution rapide, et a organisé une série de conférences données par des experts pour former le personnel aux fondamentaux de l'IA. La deuxième année est consacrée à la poursuite des travaux sur l'IA et à la portabilité des données. Globalement, la première année de fonctionnement a été productive et est annonciatrice d'un renforcement de la collaboration entre autorités de réglementation.

Le **Président** remercie le Canada et demande au **Mexique** de présenter le contenu du protocole d'accord conclu entre l'Institut fédéral des télécommunications (IFT) et l'autorité de protection des données.

Le **Mexique** explique que la coordination entre l'autorité chargée de la concurrence et celle chargée de la protection des données s'intensifie parce que les données sont un enjeu de plus en plus important dans les marchés numériques. La protection des données relève de la compétence de l'Institut national de la transparence concernant l'accès aux informations et la protection des données à caractère personnel (INAI), tandis que la surveillance de la concurrence dans le secteur des télécommunications et de la diffusion est assurée par l'IFT. En 2021, ces deux organismes ont signé un protocole d'accord pour renforcer la collaboration visant à favoriser la transparence, la protection des données et la concurrence. Ce protocole d'accord porte sur le partage de données statistiques, la réalisation de travaux de recherche communs et l'organisation d'activités collaboratives. Le délégué décrit deux actions de sensibilisation importantes : en 2023, l'IFT et l'INAI ont publié à l'intention des seniors un guide sur la protection des données à caractère personnel afin de renforcer la maîtrise du numérique et de prévenir les violations de données. En 2024, l'IFT a créé un outil interactif qui permet de comparer les mentions sur la confidentialité des données des principales plateformes numériques. Par ailleurs, l'IFT a conduit des études de marché sur la concurrence dans les marchés numériques, dont une analyse du rôle potentiel de la

collecte massive de données. Enfin, le Mexique juge crucial que les autorités de réglementation des télécommunications et celles chargées de la protection des données tiennent compte de la dynamique concurrentielle pour que de meilleures réponses puissent être apportées aux défis que constituent la concurrence et la protection des données dans les marchés numériques.

Après avoir remercié le **Mexique**, le Président invite le **BIAC** à fournir des recommandations concernant le traitement des problèmes complexes engendrés par l'interaction entre données et concurrence.

Le **BIAC** souligne que si les données sont indispensables au fonctionnement de l'économie numérique, elles sont à l'origine de problèmes épineux pour les consommateurs et les marchés. Le délégué soulève des questions importantes sur la manière de concilier les droits au respect de la vie privée et l'action en faveur de l'innovation et de la concurrence et sur les politiques adaptables qu'il faudrait concevoir face à la complexité du monde reposant sur les données. Il explique que la confidentialité des données et la concurrence sont interconnectées, d'où la nécessité d'adopter une approche globale tenant compte des intérêts divers des parties prenantes, dont les plateformes, les annonceurs et les utilisateurs. Il préconise aussi d'encourager la collaboration entre autorités de la concurrence et autorités de protection des données, de même que d'associer d'autres acteurs – universitaires, entreprises, etc. – et les organisations internationales pour recueillir leur point de vue et de bonnes pratiques. Il s'attarde ensuite sur trois points clés : les autorités devraient en permanence évaluer les résultats de leurs actions ; elles devraient tenir compte de la diversité du secteur numérique ; les autorités chargées de la concurrence et celles chargées de la protection des données devraient coopérer pour établir un cadre juridique cohérent de nature à améliorer la concurrence et la protection de la vie privée. En conclusion, le BIAC insiste sur l'importance de la collaboration entre tous les acteurs afin que l'économie numérique ait des retombées positives pour les consommateurs et pour les marchés.

Le **Président** remercie le BIAC et donne la parole à la **Direction de la science, de la technologie et de l'innovation (DSTI)**.

Le représentant de la **DSTI** remercie d'abord les participants, précisant qu'encourager la coopération entre autorités de réglementation est une de ses principales priorités stratégiques. Il insiste sur deux aspects importants. Premièrement, l'IA, les données et la concurrence ont été abordées comme des thèmes distincts tout au long des débats, alors qu'il conviendrait de les envisager davantage comme formant un tout. Deuxièmement, il annonce la tenue prochaine d'un événement avec Kate Jones, la Présidente du DCRF, au Royaume-Uni, et le Réseau international de coopération en matière de réglementation numérique. Des membres du réseau et des pays intéressés par la coopération entre autorités de réglementation dans le domaine numérique devraient participer à cet événement, programmé pour le 8 novembre 2024.

Le **Président** remercie la DSTI, puis invite les experts à réagir aux contributions précédentes, en commençant par **Katherine Kemp**, suivie de **Giuseppe Colangelo**.

Katherine Kemp insiste sur deux aspects importants. Premièrement, elle reconnaît que dans l'affaire Meta, abordée sous l'angle de l'exploitation abusive, il a également été dit qu'il pouvait y avoir éviction. Toutefois, cette affaire est compliquée à transposer aux juridictions qui ne reconnaissent que les pratiques d'éviction parce que les tribunaux risquent alors de demander pourquoi d'autres sources de données n'ont pas été recherchées. Deuxièmement, elle fait observer que les tensions entre autorités de la concurrence et autorités de protection des données apparaissent souvent dans les cas où de grandes entreprises technologiques n'appliquent pas les règles relatives à la protection des données

de façon systématique dans leurs diverses unités, d'où la nécessité d'une harmonisation des interventions visant à faire respecter ces règles.

Giuseppe Colangelo indique souscrire à certains propos tenus et souligne que malgré une prise de conscience des conflits possibles entre protection des données et concurrence, il n'adhère pas à l'argument de la valeur ajoutée et invite à la prudence concernant le périmètre de l'intervention.

Tim Capel se dit reconnaissant d'avoir eu l'occasion de participer aux débats, soulignant la qualité des exemples cités. Il se dit optimiste tout en reconnaissant la nécessité d'être réaliste. Il souligne en outre que les autorités de protection des données pourraient avoir intérêt à mieux connaître les pratiques des autorités de la concurrence, souvent mieux dotées en ressources. Il s'appuie sur son expérience pour insister sur la valeur du resserrement des liens entre autorités de réglementation, souligne le problème posé par la durée des procédures judiciaires et exprime son enthousiasme à la perspective de l'événement programmé le 8 novembre.

Le **Président** remercie tous les participants et indique souscrire à l'argument de **Tim Capel** sur l'intérêt de la coopération. Il insiste sur l'importance d'un dialogue continu entre autorités de réglementation, comme au Royaume-Uni et au Canada, et annonce qu'après la pause, la discussion portera sur le choix des sujets des futures tables rondes.