Organisation de Coopération et de Développement Économiques

DAF/COMP/M(2020)1/ANN5/FINAL

Non classifié | Français - Or. Anglais

13 décembre 2021

DIRECTION DES AFFAIRES FINANCIÈRES ET DES ENTREPRISES
COMITÉ DE LA CONCURRENCE

Compte rendu de la table ronde sur les droits relatifs aux données des consommateurs et leur impact sur la concurrence

Annexe au compte rendu succinct de la 133e réunion du Comité de la concurrence tenue à distance du 10 au 16 juin 2020

12 June 2020

Ce document est un compte rendu des débats de la table ronde sur les droits relatifs aux données des consommateurs et leur impact sur la concurrence qui s'est tenue pendant la 133e réunion du Comité de la concurrence.

D'autres documents liés à ce sujet sont disponibles à l'adresse suivante : www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm.

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

JT03487311

Compte rendu de la table ronde sur les droits relatifs aux données des consommateurs et leur impact sur la concurrence

Ce document établi par le Secrétariat est un compte rendu des débats qui ont eu lieu dans le cadre de la table ronde du Comité de la concurrence sur les droits relatifs aux données des consommateurs et leur impact sur la concurrence qui s'est tenue à distance le 12 juin 2020.

Remarque liminaires

Le **Président** souhaite la bienvenue aux participants et présente le thème de la table ronde : les droits relatifs aux données des consommateurs et leur impact sur la concurrence. Il indique ensuite que différents pays dans le monde ont récemment créé de nouveaux droits liés aux données des consommateurs, et souligne que les interactions entre les législations et politiques en matière de concurrence, de protection des consommateurs, et de protection des données et de la vie privée suscitent de plus en plus de débats. Dans certains marchés, la façon dont sont développés et mis en œuvre les droits relatifs aux données des consommateurs peut en effet avoir des répercussions sur la bonne marche de la concurrence, notamment par une augmentation des obstacles à l'entrée ou par une modification des dispositifs d'incitation. Certaines mesures correctrices pourtant souhaitables et relevant du droit de la concurrence peuvent en outre entraîner une baisse du niveau de protection des données des consommateurs. Il est donc essentiel d'encourager la coopération entre les autorités de la concurrence et les organismes de protection des données.

Le Président fait remarquer que des questions se posent également, lorsque les autorités de la concurrence ont à évaluer des problèmes de concurrence, concernant le degré de prise en compte des droits relatifs aux données des consommateurs et des problèmes existants en matière de protection des données et de la vie privée. À cet égard, mais aussi au vu de l'évolution de ces difficultés dans le temps, le Président cite Zanfir-Fortuna et Ianc (2019[1]) :

> *À l'origine, les autorités de la concurrence considéraient la législation sur la protection des données comme une question séparée, sans pertinence dans le cadre des procédures de contrôle des fusions, et mettaient par conséquent ces deux domaines du droit sur deux plans différents. Dans un second temps, le fait que les règles de protection des données peuvent en réalité avoir une incidence (favorable comme préjudiciable) sur la concurrence s'est de plus en plus imposé dans l'élaboration des politiques et dans le règlement des différends. Les autorités chargées de la protection des données ont quant à elles également commencé à s'investir dans ces questions.*
>
> *Nous sommes aujourd'hui à l'aube d'une troisième phase [articulée autour des] considérations juridiques sur la protection des données […].*

Le Président souligne que Zanfir-Fortuna et Ianc (2019[1]) ont surnommé cette évolution la phrase de l'« hyperprotection », définie comme la protection des droits des personnes et de leur bien-être en tant que les personnes concernées ou que participants au marché, et ce, grâce à l'élaboration de politiques cohérentes et à une application convergente du droit par

les autorités de la concurrence et les organismes de protection des données et des consommateurs.

Le Président ajoute que cette évolution potentielle fait apparaître de nouvelles questions : les autorités de la concurrence devraient-elles prendre en compte le niveau de protection des données des consommateurs en tant que composante de la performance économique ? Dans ce cas, une baisse du niveau de protection pourrait être vue comme une augmentation implicite des prix. Une baisse de la protection n'aurait-elle donc pas d'incidence négative sur la concurrence ? Une infraction à la législation sur la protection des données pourrait-elle constituer une atteinte au droit de la concurrence ? Les autorités de la concurrence devraient-elles s'intéresser aux effets d'une fusion sur la protection des données ? Les autorités de la concurrence devraient-elles chercher à compléter les réglementations ou capacités d'exécution insuffisantes ou défaillantes en matière de protection des données des consommateurs ? Ces questions ont été jugées pertinentes dans le cadre des débats de la table ronde.

Le Président indique que le Comité de la concurrence a déjà examiné certaines de ces questions lors de tables rondes antérieures, dont la réunion de concertation de 2016 sur les données massives et les tables rondes de 2018 sur la problématique de la qualité sur les marchés sans contrepartie monétaire et sur les effets hors-prix des fusions. Lors de la réunion de concertation sur les données massives, il fut notamment question de déterminer si l'accès aux données pouvait conférer un certain pouvoir de marché (autrement dit si les données pouvaient constituer un obstacle à l'entrée). Les tables rondes de 2018 permirent quant à elles d'aborder le niveau de protection de la vie privée proposé par les entreprises afin de déterminer s'il pouvait être un aspect de la qualité sur lequel les entreprises sont en concurrence.

Le Président souligne que ce thème a suscité un grand nombre de contributions, soit 19 au total, dont 12 de pays membres de l'OCDE, 4 de pays participants de l'OCDE, et trois respectivement du BIAC (*Business at OECD*), du BEUC (Bureau européen des unions de consommateurs) et du TUAC (*Trade Union Advisory Committee*, ou Commission syndicale consultative auprès de l'OCDE). Il présente ensuite les experts du panel et les remercie pour les enregistrements vidéo de leurs interventions, lesquels ont été préalablement chargés sur le site internet de la table ronde :

- M[me] Elizabeth Denham, commissaire à l'information du Royaume-Uni (présidente de l'*Information Commissioner's Office*) et présidente de l'Assemblée mondiale pour la protection de la vie privée. Dans son intervention vidéo, M[me] Denham souligne l'importance de la coopération entre les autorités de la concurrence et les organismes de protection des données, que ce soit pour renforcer la confiance des consommateurs, évaluer les incidences potentielles des fusions ou encore mettre en œuvre les mécanismes de portabilité des données ;

- M. Wolfgang Kerber, professeur d'économie à l'université de Marbourg, spécialiste de la concurrence et des données, notamment en lien avec l'internet des objets. Dans sa contribution vidéo, M. Wolfgang Kerber aborde des sujets comme la gouvernance des données et la concurrence, en s'appuyant sur ses recherches consacrées aux véhicules connectés. Il défend également la thèse selon laquelle les questions relatives au droit de la concurrence et au respect de la vie privée devraient être traitées de façon simultanée ;

- M. Alessandro Acquisti, professeur de technologies de l'information et de politiques publiques à l'université de Carnegie Mellon, spécialiste de l'économie de la vie privée. Dans sa contribution vidéo, M. Acquisti s'intéresse aux travaux de

recherche consacrés au comportement des consommateurs vis-à-vis de leur vie privée et à la valeur qu'ils y accordent.

Les discussions de la table ronde sont articulées autour des trois axes suivants :

1. **Évaluations d'impact sur la concurrence** : comment prendre en compte les politiques de protection des données et de la vie privée dans l'évaluation des problèmes de concurrence ?
2. **Mesures correctrices relevant du droit de la concurrence** : comment élaborer des mesures correctrices dans les affaires de concurrence tout en garantissant qu'elles ne portent pas atteinte à la protection des données et de la vie privée ?
3. **Élaboration des politiques** : comment promouvoir la concurrence dans la conception et l'application des droits relatifs aux données des consommateurs, et comment développer des politiques contribuant à encourager la concurrence et la protection des données et de la vie privée, mais aussi la protection des consommateurs, dans le contexte de l'exploitation de leurs données.

Pour lancer les discussions de la table ronde, le Président propose aux experts d'indiquer quel message ils souhaitent faire passer en priorité.

- **M^me^ Denham** souligne que le respect de la vie privée n'avait jamais été pris en compte dans l'analyse de la concurrence, y compris dans le cadre de fusions or, dans un monde qui repose chaque jour davantage sur les données, la concurrence et la protection des données doivent toutes deux contribuer à protéger les intérêts des personnes, notamment en termes d'autonomie et de liberté de choix.
- **M. Kerber** précise que dans l'économie numérique la relation entre le droit de la concurrence et la législation sur la protection des données est particulièrement complexe compte tenu des interactions qui existent entre les défaillances du marché, les pratiques d'application du droit et les mesures correctrices mises en place. Cela suppose une analyse approfondie des affaires et une bien plus grande coordination entre les différents domaines de l'action publique.
- **M. Acquisti** explique qu'il existe une abondance de preuves empiriques montrant que les consommateurs ont à cœur de protéger leur vie privée en ligne et prennent même des mesures concrètes en ce sens. Il est également largement démontré que divers obstacles et barrières peuvent nuire aux comportements en faveur de la protection de la vie privée, de l'asymétrie de l'information à la rationalité limitée. Il souligne ainsi que l'évolution des marchés vis-à-vis de la protection de la vie privée ne rend pas nécessairement compte des préférences réelles des consommateurs.

Partie I : Évaluations d'impact sur la concurrence

La première partie de la table ronde est consacrée à la manière dont les autorités de la concurrence prennent en compte la protection des données et de la vie privée dans le cadre de leurs activités d'application du droit. Le **Président** rappelle la proposition de M. Kerber selon laquelle, plutôt que de laisser les questions de vie privée aux autorités chargées de la protection des données, il conviendrait que les autorités de la concurrence prennent en considération les défaillances du marché liées aux problèmes comportementaux et d'information susceptibles de limiter l'efficacité des politiques de protection des données et l'évaluation des problèmes potentiels de concurrence. Le Président indique alors que la

première partie de la table ronde sera l'occasion d'entendre les différents avis des délégués sur cette question.

Les débats s'ouvrent avec l'intervention des **États-Unis**, qui dans leur contribution (OCDE, 2020[2]) précisent que :

> *Les droits relatifs aux données des consommateurs et le droit de la concurrence ont des objectifs différents en termes d'action publique, et ils sont souvent protégés par des règles et des dispositifs d'application spécifiques. Dans la mesure où, parallèlement aux autorités de la concurrence, les responsables publics peuvent chercher à faire progresser des objectifs différents grâce aux politiques en matière de données, nous recommandons aux responsables publics envisageant l'adoption de nouveaux droits relatifs aux données des consommateurs ou la modification des droits existants de prendre également en considération les incidences possibles sur la concurrence, ainsi que sur d'autres objectifs en faveur de la concurrence, et notamment l'innovation. Les autorités de la concurrence doivent avoir conscience des effets de la législation relative à la protection de la vie privée sur les marchés sur lesquels elles cherchent à déterminer l'existence d'atteintes à la concurrence, mais aussi lorsqu'elles évaluent l'efficacité probable des mesures correctrices adoptées en réponse à des comportements ou opérations préjudiciables pour la concurrence.*

Les **États-Unis** soulignent que la Commission fédérale du commerce américaine (*Federal Trade Commission*, FTC) est chargée à la fois de l'application du droit de la concurrence et de la législation sur la vie privée, et jouit donc d'une certaine expérience en la matière. L'économie américaine s'appuie fortement sur les données et celles des consommateurs constituent une ressource et un produit importants pour de nombreux biens et services. Il n'est donc pas étonnant que les droits relatifs aux données puissent avoir une incidence sur la concurrence dans certains marchés. À titre d'exemple, dans l'affaire instruite par la FTC contre Core Logic, l'autorité considérait que l'accumulation de données historiques constituait un obstacle à l'entrée. La procédure de règlement prévoyait donc une obligation pour Core Logic de céder ses données sous licence aux nouveaux entrants.

Dans certains marchés, la protection de la vie privée peut avoir un réel intérêt pour l'analyse de la concurrence en tant qu'élément constitutif de la qualité. Il s'agit en effet d'une dimension hors prix sur laquelle les entreprises se font concurrence et qui peut être affectée négativement par une fusion ou d'autres types d'événements. Déterminer objectivement la valeur réelle accordée par les consommateurs à la protection de leur vie privée ainsi que la dynamique de marché sous-jacente n'est pas une tâche facile.

Les États-Unis considèrent que l'existence d'interactions entre la concurrence et la protection de la vie privée n'impliquent pas nécessairement que les législations correspondantes devraient être fusionnées. Chacune répond à des objectifs particuliers et exigent l'application de mesures correctrices spécifiques, et leurs interactions sont à la fois complexes et différentes selon le contexte. Le renforcement des droits relatifs aux données des consommateurs peut avoir pour effet de stimuler la concurrence, notamment en réduisant l'asymétrie de l'information ou en limitant les pratiques d'éviction. La protection de la vie privée et la concurrence peuvent toutefois également être antagonistes, au point que certains arbitrages soient inévitables. Exiger par exemple d'une entreprise qu'elle partage ses données ou permettent à ses concurrents d'y accéder sur sa plateforme peut contribuer à la bonne marche de la concurrence, mais réduire d'autant le niveau de protection de la vie privée. De la même manière, les législations en faveur du respect de la vie privée peuvent porter atteinte à la concurrence en renforçant la position des entreprises en place et en augmentant les coûts pour les petites et moyennes entreprises. Par conséquent, bien que la protection de la vie privée puisse présenter un intérêt au regard du

droit de la concurrence, elle ne doit pas en devenir un objectif distinct. Dans le cas contraire, précisent les États-Unis, certaines incohérences se feraient jour et aussi bien la concurrence que la protection de la vie privée pourraient en pâtir. Les États-Unis indiquent enfin que le contrôle des fusions, pourtant susceptible de servir de nombreuses fins de manière pratique, n'est pas plus un moyen d'assurer l'application de la législation sur la vie privée qu'il ne l'est pour la législation environnementale, le droit du travail ou tout autre objectif éventuellement recherché par les pouvoirs publics.

Le ministère de la Justice des États-Unis (*Department of Justice*, DOJ) propose à son tour un aperçu de son expérience. À l'instar de la FTC, le DOJ s'intéresse à la manière dont les consommateurs peuvent subir un préjudice anticoncurrentiel lorsque les plateformes numériques recueillent davantage de données personnelles sans pour autant leur offrir de contrepartie par le biais de services à valeur ajoutée. L'un des principaux marchés où cette dynamique peut être observée est celui de la publicité numérique. Le DOJ enquête depuis longtemps sur les infractions au droit de la concurrence dans les marchés de biens et services financés par la publicité et porte régulièrement ces affaires en justice, mais jamais auparavant les données recueillies à l'échelle des individus n'avaient représenté une ressource aussi importante pour les modèles économiques basés sur les annonces publicitaires. Pour mieux comprendre la dynamique concurrentielle dans ces marchés, le DOJ a organisé un atelier public au début de l'année 2019. À cette occasion, différents experts et acteurs du secteur se sont entretenus de la manière dont les entreprises recueillent et monétisent les données, puis mis en évidence que même si la collecte et le partage de données par des tiers sont souvent critiqués pour leurs implications au regard de la protection de la vie privée, ils peuvent être des outils essentiels pour instaurer une certaine discipline parmi les opérateurs en place et renforcer les contrôles sur les comportements anticoncurrentiels dans les écosystèmes financés par la publicité. Les *cookies* tiers utilisés sur les sites internet, par exemple, peuvent garantir que les données relatives aux consommateurs et issues de leurs interactions avec les sites internet proviennent de sources différentes (ce qui peut s'avérer utile dans le cadre de publicité ciblée). Ils peuvent en outre être utilisés par les sociétés d'analyse pour contrôler l'efficacité des annonces en ligne. Cette capacité à mesurer directement le retour sur investissement de la publicité peut grandement contribuer à stimuler la concurrence entre différentes sources d'espace publicitaire.

Les autorités de la concurrence se sont déjà appuyées sur des acteurs tiers lors de l'élaboration de mesures correctrices visant à restaurer la concurrence. Le DOJ a récemment exigé le partage des données dans le cadre des mesures correctrices imposées lors de la fusion CVS/Aetna. La cession sous licence de logiciels fondés sur les données fait également partie des mesures correctrices adoptées dans certaines affaires (Google ITA, par exemple). Dans leur recherche du niveau de protection juridique optimal en matière de données et de protection par défaut de la vie privée, les autorités doivent prendre en compte l'expression possible des préférences des consommateurs en matière de protection de la vie privée, ou la possibilité de déterminer ou mesurer le degré d'intention des consommateurs à partager leurs données avec une partie mais pas une autre, ou à partager leurs données à des fins spécifiques mais pas à d'autres fins. Restreindre l'accès aux données à des acteurs tiers risque d'entraver la bonne marche de la concurrence et avoir une incidence négative sur le bien-être des consommateurs, sans pour autant améliorer de manière significative la protection de leur vie privée.

Le **BIAC** prend ensuite la parole et se déclare fermement convaincu que même si le droit de la concurrence et la législation relative à la protection des données et de la vie privée servent des objectifs stratégiques différents, ces deux domaines d'action doivent faire l'objet d'une coordination étroite. Il est impératif que les autorités de tutelle se coordonnent entre elles, notamment dans la mesure où les objectifs des deux systèmes, malgré une

ambition commune d'amélioration de la protection des consommateurs, peuvent mener vers des orientations différentes. Le droit de la concurrence protège les consommateurs en encourageant une concurrence intense, ancrée dans l'idée que des marchés concurrentiels sont un terrain idéal pour l'investissement, l'efficacité, l'innovation et la croissance. Le droit de la concurrence vise ainsi à offrir aux consommateurs une plus grande autonomie et à les doter d'un réel pouvoir de décision, alors que les législations relatives à la protection de la vie privée et à la protection des consommateurs visent plutôt à protéger les personnes de tout préjudice découlant de pratiques déloyales ou abusives. Ces approches distinctes du bien-être des consommateurs ne mettent pas nécessairement ces deux systèmes en opposition, mais elles peuvent susciter des considérations différentes en matière d'action publique. Le BIAC estime que pour être réellement efficace, il est important de respecter les différences de ces deux systèmes et non les ignorer.

Le BIAC s'inquiète également du risque qu'un système hybride ne freine toute innovation dans l'exploitation des données par les entreprises. La collecte et l'utilisation des données par les entreprises offrent de nombreux avantages, lesquels ne sont pas limités à des considérations d'efficacité ou d'innovation. Ces pratiques offrent également de nombreux avantages aux consommateurs sous la forme de produits et de services plus pertinents, et ce, pour un coût plus fiable (voire nul). Un chevauchement des réglementations pourrait avoir un effet dissuasif pour les entreprises désireuses d'investir et de se développer dans une juridiction particulière. Le BIAC estime par conséquent qu'il est essentiel de lutter contre toute redondance et d'encourager la clarté des réglementations (dans la mesure où un manque de clarté pourrait entraîner une paralysie des investissements). Les décisions rendues en matière de concurrence peuvent être difficiles à appliquer pour d'autres entreprises en raison de leur caractéristiques particulières, notamment dans les secteurs innovants comme le commerce électronique, les réseaux sociaux et les entreprises de technologie financière (Fintechs), dont la taille et l'importance ne font qu'augmenter dans l'économie mondiale. Le BIAC conclut qu'une coordination efficace dans la mise en application des textes est essentielle pour garantir que l'innovation et l'investissement continuent de s'intensifier sans porter atteinte à la concurrence ou à la protection des données.

Rappelant la procédure actuellement engagée contre Facebook par le Bundeskartellamt, le **Président** donne la parole à Allemagne.

À l'instar des États-Unis, l'**Allemagne** considère que le droit de la concurrence et la législation sur la vie privée ne doivent pas être confondus, et souligne que le Bundeskartellamt n'est pas une autorité chargée de la protection de la vie privée. L'Allemagne précise que, s'agissant des modèles économiques axés sur les données, le droit de la concurrence et la législation sur la vie privée s'entrecroisent de telle façon qu'il est particulièrement difficile de faire la part des choses dans les affaires où les données sont le principal moteur des entreprises en position dominante et dans lesquelles les données peuvent faire l'objet de mesures correctrices. Dans le cas de l'affaire Facebook, l'accès aux données personnelles est (en parallèle aux effets de réseau) un facteur essentiel pour l'évaluation de la position dominante de l'entreprise. Cela est d'ailleurs reflété dans le droit de la concurrence allemand, qui précise que *« dans l'appréciation d'une position dominante, l'accès aux données constitue un facteur essentiel »*. L'Allemagne poursuit en indiquant que si une entreprise en situation de « surdomination » porte systématiquement atteinte aux principes de protection de la vie privée dans le cadre même de son modèle économique, la manière dont elle recueille et traite ces données est une dimension que les autorités de la concurrence doivent prendre en considération. Cette question est au cœur de la procédure engagée contre Facebook par le Bundeskartellamt depuis 2019. Le problème n'est pas que Facebook recueille des données depuis sa propre plateforme (une pratique dont ont conscience la plupart des utilisateurs), mais que Facebook recueille également des

données sur ses consommateurs à partir de plateformes tierces pour les conserver dans les comptes des utilisateurs de Facebook. Les utilisateurs n'ont aucun moyen de contrôler les données collectées, car l'utilisation des services de Facebook est conditionnée à leur consentement au recueil de données personnelles sur d'autres plateformes. La collecte de données et le droit de la concurrence sont dans ce cas précis étroitement liés. D'après l'Allemagne, les autorités de la concurrence doivent pouvoir s'appuyer sur un paramètre précis afin d'évaluer si une entreprise en position dominante gère ou non les données des consommateurs de manière appropriée. Dans cette optique, et dans le contexte allemand, il convient de noter que la question de l'utilisation appropriée des données des consommateurs a été tranchée par les responsables européens à travers le Règlement général sur la protection des données (RGPD). Le RGPD est donc un élément important à prendre en considération pour déterminer si une entreprise dominante abuse de sa position. S'agissant des mesures correctrices adoptées, elles portaient également sur les données et visaient à limiter la capacité de Facebook à les recueillir. Le Bundeskartellamt n'obtint pas gain de cause devant le Tribunal de grande instance lors d'une audience préliminaire, mais fit appel de cette décision. La Cour suprême fédérale doit organiser une audience contradictoire le 23 juin 2020. Bien que le législateur et les autorités de la concurrence abordent cette affaire selon une perspective spécifique, la décision finale revient au tribunal.

Le **Japon** présente ensuite ses récents travaux relatifs aux plateformes numériques et fait part de l'examen par la Commission de la concurrence japonaise (*Japan Fair Trade Commission*, JFTC) de la mesure dans laquelle la qualification d'abus de dépendance ou d'abus d'un pouvoir de négociation supérieur, plutôt que d'abus de position dominante, pourrait constituer un outil efficace pour simplifier certaines des interactions entre le droit de la concurrence et la législation sur la protection des données.

Le Japon souligne d'abord les inquiétudes grandissantes concernant l'utilisation des données des consommateurs par les plateformes numériques. Face à cette évolution, la JFTC a constitué un groupe d'étude et mené des entretiens afin de déterminer si, et le cas échéant de quelle manière, la Loi antimonopole japonaise pouvait être appliquée aux comportements abusifs des plateformes numériques dans leur utilisation des informations personnelles. Sur cette base, la JFTC a publié de nouvelles lignes directrices en 2019 destinées à préciser dans quels cas l'acquisition, la détention et l'utilisation d'informations à caractère personnel par les plateformes numériques pourraient relever d'un abus de pouvoir de négociation supérieur en vertu de la Loi antimonopole. Ces lignes directrices stipulent que si une plateforme numérique désavantage les consommateurs ou leur porte préjudice en abusant d'un pouvoir de négociation supérieur, on peut estimer qu'un tel comportement ne pèsera pas seulement sur la liberté de choix et l'indépendance des consommateurs, mais il conférera aussi à cette plateforme un avantage concurrentiel. Les lignes directrices proposent par ailleurs plusieurs exemples d'acquisition ou d'utilisation injustifiée d'informations à caractère personnel sur les consommateurs, susceptibles de constituer des pratiques d'abus de pouvoir de négociation supérieur. C'est notamment le cas lorsqu'une plateforme numérique acquiert des informations au-delà du cadre nécessaire pour atteindre l'objectif déclaré initial, sans avoir obtenu le consentement des consommateurs ou après avoir contraint les consommateurs à donner leur consentement.

Le Japon explique ensuite le lien entre les dispositions relatives aux abus de pouvoir de négociation supérieur et la Loi sur la protection des informations à caractère personnel (PICP). Ces deux régimes divergent aussi bien dans leurs objectifs que dans leurs champs d'application. Si une entreprise recueille ou exploite des données personnelles sans l'accord des intéressés (ce qui constitue de fait une infraction à la Loi sur la PICP), c'est le comité de protection des informations à caractère personnel qui prendra en charge l'affaire afin d'assurer la protection des droits et intérêts des consommateurs. Toutefois, si le

comportement d'une entreprise risque d'avoir un effet préjudiciable sur la concurrence (pas seulement en cas d'absence de consentement des utilisateurs, mais aussi lorsqu'une entreprise oblige les consommateurs à accepter que leurs informations personnelles soient utilisées), la JFTC enquêtera sur ces pratiques en vertu de la Loi antimonopole. Lorsque cela s'avère nécessaire, la JFTC travaille en collaboration avec le comité de la PICP pour examiner les affaires opposant les plateformes numériques et les consommateurs.

Le **Président** invite les experts à réagir, en commençant par **Wolfgang Kerber**. M. Kerber précise que la protection de la vie privée couvre des notions très différentes aux États-Unis et en Union européenne. La protection de la vie privée fait partie des droits fondamentaux dans les pays de l'Union européenne. À l'inverse, la contribution écrite des États-Unis indique qu'il existe sans doute un équilibre à trouver avec les avantages de l'économie des données, l'innovation, mais aussi la recherche d'efficacité. Autrement dit, une certaine tension s'exerce entre la protection de la vie privée d'un côté, et l'innovation et l'efficience économique de l'autre. Cela peut également donner lieu à une relation différente aux États-Unis et en Union européenne entre, d'une part, le droit et la politique de la concurrence et, d'autre part, la législation et la politique de protection des données et de la vie privée.

M. Kerber précise qu'il existe également une autre divergence notable (en matière d'exploitation abusive) dans le fait de considérer que la protection des consommateurs contre les effets redistributifs négatifs du pouvoir de marché sur le bien-être des consommateurs relève ou non de la politique de la concurrence. Sur cette question, il tient à souligner la différence majeure d'appréciation entre les États-Unis et l'Union européenne. Les interventions de l'Allemagne et du Japon laissent apparaître que dans ces pays, et plus généralement dans l'Union européenne, ces pratiques abusives entrent dans le champ d'application du droit de la concurrence. Le Japon considère qu'il s'agit d'une question de pouvoir de négociation supérieur, et c'est d'ailleurs l'un des points clés dans l'affaire Facebook instruite par le Bundeskartellamt, que l'on peut résumer à une simple affaire d'abus, où il est question de déterminer si la capacité du pouvoir de marché à entraîner des effets négatifs sur la protection de la vie privée relève directement du droit de la concurrence. La difficulté consiste toutefois à définir les références à utiliser pour qualifier un abus de position dominante au regard des données des consommateurs. M. Kerber estime que considérer une violation du RGPD comme constitutif d'une infraction au droit de la concurrence semble contraire à l'esprit même du droit de la concurrence. Le RGPD ne définit en effet qu'une norme minimale en matière de protection de la vie privée, et ce niveau de protection peut être différent du niveau offert dans le cadre d'une concurrence efficace.

M. Kerber recommande également que les autorités de la concurrence tiennent compte de l'incidence des défaillances du marché sur la protection des données et de la vie privée, et prennent ces défaillances en considération dans l'élaboration des mesures correctrices. Il préconise en outre une collaboration renforcée entre les autorités chargées de la protection des données et les autorités de la concurrence. Concernant l'affaire instruite par le Bundeskartellamt à l'encontre de Facebook, il aurait souhaité qu'une action soit menée en parallèle par les autorités chargées de la protection des données, débouchant sur une décision coordonnée permettant d'apporter une réponse commune à cette double défaillance du marché. L'objectif n'aurait pas été de mener une enquête ou une procédure conjointe, mais d'arriver à une combinaison idéale de mesures correctrices.

Elizabeth Denham revient ensuite sur la collaboration et la coopération entre les autorités de la concurrence et les organismes de protection des données. Elle rappelle que ces autorités ont un rôle différent, et qu'une part importante de son travail consiste à protéger des libertés et droits fondamentaux qui n'affectent pas la bonne marche de la concurrence. À titre d'exemple, le recours aux technologies de reconnaissance faciale par les forces de

police n'a aucune incidence sur le secteur privé et la concurrence. Un diagramme de Venn permet de mettre à jour une certaine convergence des intérêts et des travaux des autorités de la concurrence et des organismes de protection des données, notamment au regard de la protection des consommateurs, mais aussi de notions comme l'équité, la transparence et la protection des données dès la conception, afin de permettre aux consommateurs de prendre des décisions éclairées en toute autonomie.

M^me^ Denham souligne que cette collaboration et cette coopération renforcées demeurent relativement récentes, et précise qu'il y a encore un an et demi à deux ans elle ne suivait pas de près les travaux de l'autorité britannique de la concurrence et des marchés (*Competition and Markets Authority*, CMA) Face au nombre croissant de points de convergence, une structure de gouvernance formelle réunit désormais quatre fois par an autour d'un programme de travail commun les directeurs de la CMA, de l'organisme de réglementation du secteur des médias et des communications (*Office of Communications*, Ofcom) et de l'*Information Commissioner's Office* (ICO). Ces instances ont notamment collaboré sur la question de la publicité numérique. L'ICO a lancé une enquête sur l'utilisation des données à caractère personnel dans le cadre d'enchères en temps réel dans la publicité en ligne. Après avoir organisé une table ronde, l'ICO publia un rapport sur les risques d'atteinte à la protection des données dans l'écosystème actuel et le contexte des enchères en temps réel. La CMA ayant ouvert une enquête sur le marché de la publicité numérique, l'ICO choisit de suspendre temporairement ses travaux. L'ICO coopère désormais à l'enquête de la CMA en participant aux travaux de recherche. S'agissant de la publicité numérique, M^me^ Denham indique également qu'en tenant compte des incidences des enchères en temps réel au regard du RGPD, il est possible que sa décision dans cette affaire ait eu comme conséquence non intentionnelle de renforcer la position des principaux acteurs du marché. En tant que commissaire à l'information, M^me^ Denham est légalement tenue de veiller à la promotion de l'innovation et de l'économie numérique. Il est donc de sa responsabilité de prendre en compte les répercussions des mesures correctrices, sanctions et décisions qu'elle adopte sur ces deux domaines d'action.

L'**Allemagne** mentionne ensuite deux points. D'une part, elle précise que le Bundeskartellamt travaille en étroite collaboration avec les autorités allemandes de protection de la vie privée. Il existe plusieurs de ces autorités en Allemagne à la fois au niveau fédéral et au niveau régional. Bien que la décision du Bundeskartellamt d'entamer une procédure à l'encontre de Facebook n'eût pas officiellement reçu l'aval des différentes autorités de protection de la vie privée, ces dernières appuyaient néanmoins cette décision de manière officieuse. D'autre part, l'Allemagne indique que si une entreprise en situation de « surdomination » oblige les consommateurs à confier chaque jour davantage de données, enfreignant ainsi systématiquement les dispositions du RGPD et renforçant chaque jour sa position, enfreignant à un second titre les dispositions du RGPD, il serait logique que les autorités de la concurrence puissent s'intéresser à la manière dont cette entreprise recueille toutes ces données. Si la loi oblige les autorités de la concurrence à traiter cette question, il doit exister un paramètre sur lequel s'appuyer, et dans le cas de l'Allemagne il a été convenu que ce paramètre ne pouvait être que le RGPD.

M. Alessandro Acquisti aborde alors la question de l'attitude des consommateurs, de leur comportement et de la valeur qu'ils accordent au respect de la vie privée. M. Acquisti commence par examiner la notion de « vie privée ». Il existe d'un côté une définition dominante de la vie privée datant d'Alan Westin, qui correspond au contrôle de ses propres informations personnelles et donc à la protection de ces informations. Dans ses travaux, le psychologue social américain Irwin Altman définit la vie privée comme un processus de gestion des limites, plutôt que d'être uniquement et immuablement une affaire de protection. Altman envisageait la vie privée comme le processus dynamique et dialectique de s'ouvrir ou de se fermer aux autres. Cette distinction a des implications pratiques

considérables, notamment car il existe de nombreuses données factuelles témoignant de comportements en ligne en faveur de la protection de la vie privée de la part des consommateurs. Ces données proviennent à la fois d'études comportementales, d'études de terrain et d'expériences en laboratoire, parmi lesquelles l'étude Pew de 2013, qui a révélé que 86 % des participants américains avaient pris au moins quelques dispositions pour protéger leur vie privée en ligne, que ce soit en supprimant les *cookies*, en chiffrant leurs messages électroniques, en évitant d'utiliser leur véritable identité sur certains forums ou en utilisant un réseau privé virtuel (VPN pour *virtual private network*). Une enquête réalisée en 2017 a également montré que près de la moitié des participants utilisaient le mode privé de leur navigateur internet. Enfin, une étude réalisée par des universitaires a montré en 2017 que 93 % des utilisateurs de Facebook avaient modifié les paramètres par défaut de leurs profils afin que leurs publications soient moins visibles ou qu'elles ne soient plus accessibles de manière publique. L'abondance d'éléments témoignant de comportements en faveur de la protection de la vie privée fait qu'ils passent désormais quasiment inaperçus. À titre d'exemple, les utilisateurs font preuve d'initiative :

- en choisissant, selon leurs besoins, de répondre à tous les destinataires ou seulement à certains dans leurs communications en ligne ;
- en utilisant des comptes de messagerie différents pour séparer leur vie professionnelle de leur vie privée ;
- en activant ou non leur caméra lors d'appels vidéo ou de conférences.

Les utilisateurs négocient en permanence les limites de leur vie privée. On constate toutefois aussi clairement l'existence de comportements en faveur du partage et de la divulgation d'informations personnelles. D'après Irwin Altman, l'une des raisons de l'existence de données que l'on pourrait considérer comme contradictoires tient au fait que les utilisateurs veulent gérer eux-mêmes les limites entre leur vie publique et leur vie privée. Ils souhaitent donc dévoiler publiquement des données dans certains cas, mais protéger leurs données dans d'autres circonstances. On pourrait en conclure qu'aucun problème ne se pose réellement dans la mesure où les consommateurs semblent capables de choisir quand imposer des limites pour protéger leur vie privée en ligne. D'autres problèmes se posent néanmoins, expliquant l'existence de données contradictoires attestant à la fois de comportements en faveur de la protection de la vie privée et relevant de la divulgation volontaire d'informations personnelles. Les consommateurs sont néanmoins confrontés à des problèmes, obstacles ou barrières du côté de la demande qui ne leur permettent pas de contrôler facilement les contours de leur vie privée en ligne. S'ils pouvaient contrôler efficacement le vie privée, les consommateurs auraient la capacité d'atteindre l'équilibre souhaité entre partage et protection de leurs informations personnelles. Les difficultés du côté de la demande incluent notamment l'asymétrie de l'information, l'absence de connaissances suffisantes du moment où des données sont recueillies, par qui et à quelles fins, les problèmes de bidirectionnalité et tout autre problème relatif aux heuristiques et aux biais comportementaux cognitifs (comme l'actualisation hyperbolique). Il existe en outre des problèmes du côté de l'offre qui ne font qu'exacerber les difficultés du côté de la demande, comme l'effet de captivité, les externalités de réseau, les coûts de conversion ou encore le recours à une forme d'incitation psychologique visant à pousser les consommateurs à partager davantage de données. M. Acquisti conclut ainsi que les autorités de la concurrence et les autorités chargées de la protection de la vie privée ne doivent pas considérer que les résultats du marché sont nécessairement révélateurs des préférences sous-jacentes réelles des consommateurs en matière de respect de la vie privée.

Partie II : Mesures correctrices relevant du droit de la concurrence

La deuxième partie de la table ronde est consacrée aux mesures correctrices adoptées dans les affaires de concurrence en lien avec les données des consommateurs. Il s'agit d'un sujet important étant donné que certaines mesures correctrices en faveur de la concurrence peuvent directement nuire à la réalisation des objectifs de protection des données et de la vie privée.

Cette deuxième partie commence par l'intervention du **Royaume-Uni**, dont la contribution écrite aborde différentes mesures correctrices potentielles applicables aux problèmes identifiés par la CMA comme étant liés à la publicité numérique et aux plateformes en ligne. Le Royaume-Uni explique considérer les mesures relatives à l'accès aux données et à l'interopérabilité des données comme complémentaires et faisant donc partie de l'éventail d'options disponibles. Il appuie également l'observation de M. Acquisti selon laquelle les consommateurs ne disposent pas nécessairement du degré de contrôle souhaité sur leurs données à caractère personnel, notamment en raison des techniques d'incitation utilisées par les entreprises.

S'agissant des mesures correctrices, le Royaume-Uni indique avoir tendance à considérer les mesures relatives à l'accès aux données comme spécifiques à la lutte contre les silos (p. ex. : les données de clic et de requêtes de Google). S'agissant des obligations d'interopérabilité, le Royaume-Uni estime qu'elles constituent un moyen efficace de contrebalancer les effets de réseau. Ces deux approches permettent d'appréhender les problèmes de protection des données de manière différente. Des tensions peuvent s'exercer à de nombreux égards entre les régimes de concurrence et de protection des données mais c'est loin d'être la règle. Par exemple, la protection des données peut améliorer l'autonomisation des consommateurs et ainsi stimuler la concurrence. Il existe donc une forte synergie entre ces régimes du côté de la demande.

Il est en outre possible de remédier aux éventuelles tensions qui apparaissent par la mise en place de mesures spécifiques. Ainsi, en cas de problème d'accès aux données, il doit être possible de permettre aux entreprises concurrentes de récupérer les données utiles, quitte à supprimer les éléments personnels d'identification qu'elles contiennent par un processus d'agrégation, d'anonymisation ou tout autre mécanisme pertinent. Sur la question de l'interopérabilité, l'un des principaux enjeux est de déterminer si ces mesures sont réellement adoptées dans l'intérêt des consommateurs, auquel cas il est bien plus facile de respecter les principes de consentement relatifs à la protection des données comme base juridique pour le traitement des données. Il reste alors généralement à déterminer comment garantir que les consommateurs pourront exercer leur droit de contrôle et de consentement. Par ailleurs, lorsque ces mesures sont mises en œuvre, elles doivent l'être de manière à n'avoir aucune incidence sur la concurrence. Concernant la « pile des technologies publicitaires », le principe de consentement pourrait constituer une base de traitement particulièrement efficace, mais il ne devrait pas pouvoir octroyer un quelconque avantage aux entreprises en place par rapport aux autres acteurs, d'autant moins lorsque leurs activités sont en substance relativement similaires. La neutralité concurrentielle est par conséquent un principe important à prendre en considération. Il convient toutefois d'approfondir les discussions sur la façon d'atteindre cette neutralité et d'établir un point d'équilibre entre les différents avantages et inconvénients. Ces discussions sont l'occasion de mettre à profit les compétences des autorités chargées de la protection des données, comme l'ICO au Royaume-Uni.

Le **Canada** aborde ensuite les arbitrages réalisés lors de l'élaboration des mesures correctrices relevant du droit de la concurrence afin que celles-ci ne portent pas préjudice au respect de la vie privée. Le principal élément de jurisprudence applicable dans le droit

de la concurrence canadien découle de l'affaire d'abus de position dominante engagée contre le *Toronto Real Estate Board* (TREB). Dans cette affaire, l'association d'agents immobiliers avait adopté des règles interdisant à ses membres d'utiliser ou de divulguer en ligne, par le biais des sites internet de leurs bureaux virtuels, certaines informations contrôlées par l'association, y compris des données relatives aux ventes antérieures (prix de vente d'habitations, notamment). Le commissaire canadien de la concurrence a donc saisi le Tribunal de la concurrence estimant que ces restrictions avaient des répercussions négatives sur la concurrence et constituaient un abus de position dominante. Le TREB justifiait notamment ces pratiques par sa volonté de respecter la vie privée de ses clients conformément à la législation canadienne en la matière. Le Tribunal ne put retenir cette défense, notamment car le TREB avait déjà autorisé ses 40 000 membres à partager ces mêmes informations (données sur les ventes antérieures, par exemple) avec leurs clients par d'autres moyens que via leurs bureaux virtuels (par fax, par messagerie, etc.). Confirmant l'avis du commissaire de la concurrence, le Tribunal considéra que les règles imposées par le TREB étaient constitutives d'un abus de position dominante, et ordonna au TREB de les retirer. La décision du Tribunal dans cette affaire ne vient pas nécessairement en appui d'un principe général selon lequel le respect de la vie privée des consommateurs ne serait pas un aspect pertinent dans le cadre des décisions rendues en vertu du droit canadien de la concurrence. Dans cette affaire, le Tribunal a plutôt considéré que l'argument de la protection de la vie privée n'avait été envisagé que dans un second temps, servant ainsi de « prétexte » à l'application de restrictions anticoncurrentielles.

La Cour d'appel fédérale estima que toute pratique d'entreprise ayant une incidence négative sur la concurrence mais dont l'adoption est nécessaire à des fins de conformité avec d'autres lois ou réglementations, comme la législation relative à la protection des consommateurs, ne constitue pas nécessairement une infraction au droit de la concurrence. Dans l'élaboration de mesures correctrices notamment, le Bureau de la concurrence Canada peut être tenu de prendre en compte les effets qu'une conduite donnée peut avoir sur des aspects comme la vie privée des consommateurs et autres droits relatifs aux données de manière générale.

Le **Brésil** aborde à son tour certaines des affaires notables dont il a eu à connaître. Dans sa contribution écrite, le Brésil fait valoir que *« stimuler la concurrence en suscitant une augmentation du partage de données ne se fait pas nécessairement au détriment de la vie privée des consommateurs »* (OCDE, 2020[3]). Pour illustrer cette thèse, il choisit de présenter l'affaire Bradesco. Cette grande banque brésilienne a renforcé la procédure de connexion aux comptes bancaires de ses clients en mettant en place une authentification à deux facteurs (généralement utilisée uniquement pour confirmer les opérations). La banque Bradesco fut soupçonnée d'avoir adopté cette pratique dans le but d'empêcher Guiabolso, une entreprise de technologie financière (Fintech) offrant des services de gestion des finances personnelles, d'accéder aux données de ses clients (données auxquelles elle aurait normalement accès par l'analyse des données des comptes de dépôt des clients après obtention de leur consentement éclairé). Ayant reconnu le caractère anticoncurrentiel de cette pratique, le conseil administratif de défense économique brésilien (*Conselho Administrativo de Defesa Econômica*, CADE) s'est retrouvé dans la situation délicate de devoir élaborer une mesure correctrice potentielle. Au cours de son enquête, le CADE a déterminé que Bradesco avait invariablement refusé de négocier le développement d'une interface de programmation (*application programming interface*, API) qui aurait permis le partage de données avec Guiabolso (alors que Bradesco avait autorisé ce développement avec une autre entreprise active dans un marché sans lien avec les services financiers). Le CADE imposa donc à l'entreprise l'obligation de partager ses données, si nécessaire par le biais d'une API destinée à connecter ses bases de données avec celles de la Fintech sous réserve du consentement de leurs clients communs. Une coopération avec la banque

centrale brésilienne pourrait en outre s'avérer particulièrement utile pour définir plus en détail les aspects techniques de l'API. Celle-ci pourrait également être développée de sorte à être conforme à la nouvelle réglementation en matière de systèmes bancaires ouverts (*open banking*), publiée récemment au Brésil avec une entrée en vigueur prévue pour la fin de l'année 2021.

L'**Égypte** évoque ensuite le recours à la portabilité des données comme mesure correctrice dans le cas d'une fusion entre deux plateformes de covoiturage. En l'espèce, la portabilité des données faisait partie des mesures correctrices liées aux données exigées par les autorités égyptiennes de la concurrence (*Egyptian Competition Authority*, ECA) dans leur décision sur l'acquisition de Careem par Uber, soit les deux plus importantes plateformes de covoiturage de la région. L'ECA estima que la concentration des bases de données de l'entreprise issue de la fusion était l'un des principaux enjeux de cette opération, notamment au vu de la rareté de ce type de données en Égypte. Ces données sont en effet essentielles au modèle économique d'Uber et des plateformes de covoiturage concurrentes. Constatant que la possession de données devient à la fois un avantage concurrentiel et un obstacle à l'entrée, l'ECA a convenu qu'autoriser la concentration de données par une seule et même entité causerait un préjudice important à la concurrence sur le marché concerné. Si aucune mesure correctrice n'avait été mise en place, cette concentration de données aurait rendu quasiment impossible toute nouvelle entrée et par là même limité le choix des consommateurs. L'ECA considéra la portabilité des données comme un moyen d'éviter tout effet de captivité pour les consommateurs et de permettre l'entrée sur le marché de nouveaux acteurs.

La société Uber fut donc contrainte d'autoriser ses utilisateurs à accéder à leurs données personnelles en leur offrant la possibilité de les télécharger directement. Uber s'engagea également à mettre tout en œuvre pour faciliter l'interopérabilité de ces données avec d'autres plateformes et permettre ainsi aux consommateurs de transmettre leurs données à d'autres prestataires de services de covoiturage. L'une des principales difficultés auxquelles fut confrontée l'ECA consistait à mettre en place l'interopérabilité entre les plateformes, notamment en raison des problèmes techniques sous-jacents. En l'absence d'interopérabilité, l'ECA exigea qu'Uber s'engage à permettre aux utilisateurs de télécharger leurs données dans un format courant et à coopérer au mieux de leurs capacités avec les autres fournisseurs de services de covoiturage. L'ECA souligna l'importance de la coopération entre les autorités de la concurrence et les organismes de protection des données dans l'élaboration des mesures correctrices, mais aussi la nécessité de renforcer la sensibilisation aux technologies numériques afin de favoriser une intensification de la concurrence.

Le **Président** invite les experts à partager leurs points de vue sur les mesures correctrices, à commencer par **M^me^ Elizabeth Denham**, qu'il interroge sur l'expérience du Royaume-Uni en matière de coopération entre organismes dans l'élaboration de mesures correctrices. M^me^ Denham indique qu'au-delà des cadres formels de coopération mentionnés précédemment, les programmes de détachement sont un moyen efficace de faciliter la coopération entre différents organismes. L'ICO sollicite d'ailleurs actuellement le détachement d'économistes afin lui permettre de mieux comprendre les répercussions des décisions et mesures correctrices qu'il adopte. Le Parlement britannique vient par exemple d'approuver un code de conception adapté à l'âge, visant à prévoir une protection de la vie privée dès la conception de services destinés aux enfants, et dont les 15 spécifications de conception doivent faire l'objet d'une analyse économique d'impact par l'ICO. Le niveau de maturité de la coopération entre les autorités chargées de la protection des données et les autorités de la concurrence varie grandement à travers le monde. Dans certains pays, ce dialogue n'a pas encore commencé, alors qu'il a atteint une maturité satisfaisante au Royaume-Uni.

M^me^ Denham considère les fusions et les acquisitions comme deux domaines où la coopération s'avère particulièrement importante, et souligne que la participation des autorités de la concurrence à l'examen des acquisitions a pu être lente, notamment dans les cas où les corpus de données sont l'enjeu principal d'une fusion. Elle précise que ce fut d'ailleurs le cas en 2016 dans l'affaire Facebook/WhatsApp, puisque l'ICO est intervenu en tant qu'autorité chargée de la protection des données, considérant qu'il n'existait aucune base légale obligeant WhatsApp à partager ses données avec sa nouvelle société mère, en l'occurrence Facebook. L'ICO exigea finalement que WhatsApp s'engage à ne pas partager son corpus de données tant que l'entreprise n'aurait pas apporté la preuve qu'elle en avait légalement le pouvoir. M^me^ Denham ajoute qu'envisager les données comme une ressource dans le cadre de fusions et d'acquisitions constitue un nouvel axe majeur de recherche et de coopération. Dans le cas des acquisitions, il est toutefois difficile d'attribuer une valeur précise à des données, dans la mesure où la nature des données et les mécanismes de protection sous-jacents dépendent fortement du contexte. Des travaux complémentaires et une coopération renforcée sont donc nécessaires. En tant qu'autorité chargée de la protection des données, l'ICO doit se fier à son propre jugement pour déterminer ce qui est juste et raisonnable selon les circonstances. De la même manière, les autorités de la concurrence pourront être plus efficaces dans l'analyse et l'évaluation de la valeur quantitative des données si elles travaillent en collaboration avec les autorités chargées de la protection des données et appliquent les enseignements tirés de l'évaluation d'autres actifs incorporels, comme la « bonne volonté ». M^me^ Denham souligne également qu'il pourrait être utile de donner aux autorités de la concurrence le pouvoir d'intervenir dans les affaires traitées par les autorités chargées de la protection des données, et inversement, lorsque cela va dans le sens de l'intérêt général.

M^me^ Denham insiste enfin sur la nécessité de s'atteler à la question du traitement dissimulé des données. L'ICO a cherché à regarder « sous le capot » afin de permettre aux consommateurs de mieux comprendre dans quels écosystèmes complexes leurs données sont traitées. Les autorités doivent ainsi non seulement prendre en compte les attitudes et comportements en ligne des consommateurs, mais aussi les sensibiliser au fonctionnement de ces écosystèmes particulièrement complexes. L'ICO a notamment mis en œuvre cette approche dans l'affaire Cambridge Analytica, en s'intéressant au partage en ligne des données des électeurs, ainsi qu'aux mécanismes d'incitation et aux changements de comportement dans ce contexte. M^me^ Denham souligne qu'il est absolument indispensable que les autorités chargées de la protection des données continuent de permettre aux consommateurs et à toute personne concernée de voir de quelle manière sont traitées leurs données en ligne. Ce travail est déjà mis en œuvre dans le domaine de la publicité numérique.

Le **Président** pose ensuite à M. Wolfgang Kerber la question suivante pour le compte de la Suède : au vu du volume de données collectées, existe-t-il un risque que le partage de données permette aux entreprises de déduire des informations sur les stratégies commerciales de leurs concurrents, ou peut-on raisonnablement estimer que le partage des données des consommateurs ne facilitera pas les ententes ?

M. Kerber précise que tout dépend du type de données. Il est par exemple peu probable qu'ouvrir l'accès à certaines informations comme les données de consommation énergétique ou les données techniques de véhicules connectés, dont les composants sont contrôlés à des fins de diagnostic et de maintenance à distance, puisse faciliter les ententes. Ce type de données ne permet de tirer aucune conclusion sur les stratégies commerciales des concurrents. La situation serait néanmoins tout à fait différente si, par exemple, les données partagées concernaient les achats réalisés par les consommateurs, dans la mesure où elles sont susceptibles d'inclure des informations relatives aux transactions elles-mêmes. Si ces données comprenaient des éléments liés aux prix, aux quantités ou aux

remises et que les données de transaction étaient partagées entre tous les acteurs d'un même secteur, cela pourrait s'apparenter à un système traditionnel d'informations sur les marchés et permettrait aux entreprises de se surveiller entre elles et de pérenniser une entente sur les prix. Tout dépend donc de la nature des données partagées sur les consommateurs, ce qui montre l'importance d'une analyse efficace des informations partagées, de la manière dont elles sont partagées et avec qui.

M. Alessandro Acquisti précise ensuite que toute approche stratégique fondée sur la prise en charge par les consommateurs de la protection de leurs propres données est vraisemblablement vouée à l'échec. De très nombreuses données factuelles permettent aujourd'hui d'affirmer que les approches basées sur l'avertissement et le consentement des consommateurs ne sont pas suffisantes, et qu'une transparence et un contrôle renforcés sont des conditions minimales nécessaires pour que les consommateurs puissent gérer efficacement leur vie privée en ligne. Selon l'étude mentionnée précédemment qui révèle que la moitié des participants utilisent le mode privé de leur navigateur internet, il ressort également que deux tiers des utilisateurs ont une vision erronée de ce qu'est réellement la navigation privée, estimant que cette fonction leur assure une protection bien supérieure à ce qu'elle ne permet réellement. D'après cette étude, 93 % des utilisateurs de Facebook modifient désormais leurs paramètres par défaut de sorte à rendre leurs publications moins visibles. Pendant que les utilisateurs cherchaient à protéger davantage leur vie privée, Facebook partageait leurs données avec un nombre toujours plus grand d'acteurs tiers. Face aux difficultés grandissantes et en constante évolution, le consommateur moderne doit en permanence trouver de nouveaux moyens de gérer et de protéger sa vie privée. M. Acquisti considère cette situation injuste et ingérable pour les consommateurs, et ajoute que si l'objectif des responsables publics est de protéger la vie privée des consommateurs, s'appuyer sur un mécanisme qui donne trop d'importance aux principes d'avertissement et de consentement ne peut que se solder par un échec.

En réponse à l'intervention de M. Acquisti, les **États-Unis** soulignent que bien que les consommateurs adoptent des comportements témoignant d'une compréhension limitée du traitement de leurs données, et même s'il existe des éléments soutenant la thèse selon laquelle le marché ne reflète pas complètement ce que souhaitent les consommateurs, cela ne signifie pas nécessairement que les responsables publics comprennent mieux leurs préférences. Les États-Unis mettent également en garde contre le fait de laisser croire qu'il pourrait exister des préférences non révélées sur le marché et par conséquent qu'un certain pouvoir de marché serait à l'œuvre. Les États-Unis considèrent à l'inverse que les autorités de la concurrence doivent continuer de se fier aux éléments factuels dont elles disposent et qu'en l'absence de tels éléments probants, elles doivent se montrer particulièrement prudentes avant de permettre que d'autres valeurs, aussi importantes soient-elles, deviennent des questions relevant de la politique de la concurrence et de son application. La question du respect de la vie privée peut s'avérer pertinente, soulignent les États-Unis, mais les autorités de la concurrence doivent déterminer cette pertinence au cas par cas.

M. Alessandro Acquisti indique partager les préoccupations exprimées par les États-Unis et confirme qu'il est essentiel de faire preuve de prudence dans l'interprétation des données. Il mentionne alors les travaux d'Irwin Altman, dans lesquels il existe une distinction entre la protection de la vie privée souhaitée et la protection de la vie privée effective, autrement dit : entre le niveau de protection auquel les consommateurs aspirent et le niveau de protection qu'ils parviennent à mettre en œuvre. Sur les marchés, la protection de la vie privée peut être assurée de façon plus ou moins performante. Les consommateurs peuvent ainsi bénéficier d'une protection plus faible ou plus robuste qu'ils ne le souhaitent réellement. L'existence, au moins en théorie, d'asymétries (asymétrie de l'information, rationalités, biais, etc.) n'offre en soi aucune indication sur le fait que la vie privée serait trop ou pas assez protégée. M. Acquisti avance toutefois que si l'on prend en considération

les données d'enquêtes et les pratiques du côté de l'offre qui poussent les consommateurs à divulguer toujours plus d'informations, on se rend compte que le marché n'offre qu'une protection trop limitée de la vie privée. M. Acquisti estime ainsi que la protection de la vie privée effective sur le maché est probablement inférieure au niveau de protection souhaité.

Partie III : Élaboration des politiques

La troisième partie des débats est consacrée à la coopération dans l'élaboration des politiques portant sur les droits relatifs aux données des consommateurs et leur impact sur la concurrence.

La discussion commence par une intervention de l'**Italie**, qui a adopté une approche pluridisciplinaire dans la réalisation d'une étude récente sur les données massives, en impliquant la fois l'autorité de la concurrence, l'organisme de réglementation du secteur des communications et les organismes de protection des données. D'après l'Italie, lorsqu'il est question des droits relatifs aux données des consommateurs, la complexité des enjeux fait que la définition d'un cadre réglementaire approprié doit non seulement s'appuyer sur l'application du droit de la concurrence, mais aussi sur une sensibilisation adaptée. Partant de trois perspectives différentes, l'étude de marché a conclu qu'il n'était pas possible d'affronter efficacement les défis posés par l'économie numérique sans adopter une approche commune, et décrit comment des synergies entre ces trois institutions, dotées des outils complémentaires appropriés, peuvent être mises en œuvre efficacement tout en respectant leurs difficultés respectives. Parmi ses principales conclusions, l'étude mettait en avant que les consommateurs n'ont qu'une conscience limitée de la valeur économique des données qu'ils divulguent, notamment dans le cadre de services proposés gratuitement, soit lorsque les données à caractère personnel constituent la seule valeur d'échange du service concerné. L'étude menée auprès des consommateurs par les autorités italiennes de la concurrence semble par ailleurs confirmer l'existence d'un « paradoxe du respect de la vie privée », désignant le décalage observé entre les inquiétudes exprimées des consommateurs et leur comportement réel en ligne. Près de 93 % des utilisateurs interrogés déclarent accorder de l'importance au respect de leur vie privée, mais seulement un tiers d'entre eux s'opposent au recueil et à l'exploitation de leurs données. S'agissant des droits relatifs aux données des consommateurs, l'autorité de la concurrence, l'organisme de réglementation du secteur des communications et les organismes de protection des données ont formulé des recommandations importantes à l'intention des responsables publics, comme la mise en place de mesures visant à réduire l'asymétrie de l'information dès la phase de collecte de données ou à faciliter la portabilité des données par le développement de systèmes interopérables. Fortes de cette expérience commune, les trois institutions se sont engagées à signer un protocole d'accord en vue d'une coopération permanente dans le domaine des données massives.

L'**Espagne** prend ensuite la parole. Dans sa contribution écrite, elle préconise une coopération renforcée entre les autorités et les institutions impliquées dans la réglementation relative aux données des consommateurs, et s'inquiète de la possibilité que les règlementations horizontales ne soient pas suffisantes pour résoudre certains types de problèmes de concurrence. L'Espagne souligne toutefois que les responsables publics devraient réfléchir à la nécessité de mettre en place des réglementations sectorielles lorsque cela s'avère judicieux. À titre d'exemple, la portabilité des données semble avoir des effets favorables à la concurrence dans l'économie du partage. Dans le cas des Fintechs, les principes de neutralité technologique, de systèmes bancaires ouverts et d'interopérabilité sont particulièrement pertinents. L'Espagne examine actuellement ce qui doit s'appliquer dans le cas de la publicité en ligne et précise que des débats se sont engagés à ce sujet dans l'ensemble des pays européens. L'expérience de l'Espagne a permis de mettre en lumière

deux points essentiels. Le premier est la nécessité d'associer différents instruments : les règlementations horizontales, les règlementations sectorielles et la promotion de la concurrence dans l'élaboration de règlementations efficaces, ainsi que l'application du droit de la concurrence suivant les cas. Le second est que le niveau de complexité technique est particulièrement élevé. Il convient par conséquent d'adopter une approche multidimensionnelle et pluridisciplinaire, associant les compétences de différents organismes. Dans la mesure où l'autorité espagnole de la concurrence est également le principal organe de réglementation sectoriel des secteurs réglementés, elle peut tirer parti d'un grand nombre des points de vue et de compétences utiles.

S'agissant des éventuelles lacunes des règlementations horizontales, l'Espagne indique qu'assurer le respect de la vie privée et la protection des données des consommateurs et exiger de recueillir le contentement des consommateurs peut fausser la concurrence et profiter aux principaux acteurs du marché, dans la mesure où ils sont plus à même d'obtenir le consentement des consommateurs et d'accéder à leurs données. L'Espagne souligne ainsi sa préférence pour les approches sectorielles associant tous les instruments nécessaires en fonction de la situation. Par exemple, la portabilité des données peut s'avérer utile dans le secteur des paiements, mais être moins adaptée à d'autres secteurs. L'Espagne préconise une coopération administrative entre les différents organismes et considère nécessaire de s'équiper des outils appropriés pour résoudre ces défis complexes. Avoir l'autorité de réglementation des télécommunications et l'autorité de la concurrence dans une même enceinte permet un échange intéressant de points de vue sur les mesures correctrices adaptées dans les affaires complexes liées à la définition du pouvoir de marché, aux obligations d'accès ou à l'interopérabilité, et sur les mesures correctrices appropriées pour assurer un équilibre entre la concurrence, l'innovation et les investissements.

Le **Président** demande ensuite à la Commission européenne si elle considère le Règlement général sur la protection des données (RGPD) adopté en Europe comme un instrument limité et s'il ne conviendrait pas de mettre en place des outils plus efficaces.

La **Commission européenne** précise que le RGPD est un dispositif législatif destiné à garantir la protection d'un droit fondamental. Cela vaut même lorsque l'ensemble des droits spécifiques aux personnes concernées doivent, pour être efficaces, être également assortis d'obligations pour les entreprises. La Commission européenne souligne que le besoin d'une législation horizontale rigoureuse est par conséquent évident et que le RGPD impose un niveau minimum de protection pour les droits des personnes concernées. La Commission européenne examine en outre certains domaines pour lesquels l'adoption d'une législation plus ciblée pourrait être justifiée, par exemple pour résoudre des problèmes d'accès ou de portabilité des données. La pertinence d'une telle législation devrait être déterminée non seulement en fonction de la structure du marché, comme d'autres l'ont souligné, mais aussi selon les types de données et leurs modalités d'utilisation. Ces instruments devraient s'inscrire dans une interaction avec les règles de base et non chercher à les remplacer. À titre d'exemple, la Directive européenne sur les services de paiement (DDP) prévoit une obligation d'ouvrir l'accès aux données aux fournisseurs de certains services définis, et ce, afin de développer la concurrence et l'innovation dans les services. Cette obligation dépend en outre de l'intention spécifique des consommateurs, cette fois encore conformément aux règles de base en matière de protection des données.

Comme la Commission européenne l'a décrit dans sa contribution écrite, l'article 20 du RGPD garantit un ensemble de droits fondamentaux stricts. Il convient néanmoins d'aller plus loin non seulement sous la forme de solutions technologiques innovantes qui seront mises en œuvre en partie dans le secteur privé et en partie avec le soutien des pouvoirs publics, mais aussi dans certains domaines particuliers soumis à des règles sectorielles spécifiques. La stratégie de la Commission européenne en matière de données, dont les

contours et détails restent encore à définir, met en avant la possibilité de concevoir des règles spécifiques, par exemple afin de régir l'accès aux données des consommateurs générées automatiquement grâce aux applications de l'internet des objets (IdO), comme les appareils domestiques et le prêt-à-porter connectés. Autre exemple, cette stratégie en matière de données préconise également la création d'« espaces de données » européens pour les secteurs essentiels, lesquels espaces peuvent inclure des règles spécifiques sur l'accès et la portabilité des données. Comme le décrit le document de stratégie, les données de santé des consommateurs sont l'un des types de données qui pourraient être concernés. Dans ce domaine comme dans d'autres, les responsables publics doivent élaborer les règles applicables de sorte à limiter les effets de captivité et encourager la portabilité des données, y compris entre les États membres.

S'appuyant sur les commentaires de M^me^ Denham dans sa présentation vidéo, la Commission européenne souligne également que la portabilité des données sera plus efficace contre les effets de captivité si la structure du marché concerné permet à des acteurs autres que l'entreprise en place d'exister. Pour renforcer notre capacité à résoudre les problèmes structurels, et bien évidemment pour permettre un contrôle actif continu au cas par cas, la Commission européenne a lancé au début du mois de juin des consultations publiques sur deux propositions majeures. La première est l'adoption d'une législation sur les services numériques, incluant des règles *ex ante* potentielles pour les très grandes plateformes en ligne qui agissent en tant que « contrôleuses d'accès » et définissent actuellement les règles du jeu pour leurs utilisateurs et leurs concurrents. La seconde consiste en la création d'un nouvel outil en matière de concurrence visant à remédier aux problèmes structurels en imposant la mise en place de mesures correctrices (structurelles ou comportementales) sans qu'il soit nécessaire d'identifier préalablement de violation des règles de la concurrence. Ces deux propositions impliquent des considérations stratégiques différentes. Il convient notamment de se demander si ce nouvel outil doit être limité aux marchés numériques ou avoir une application plus horizontale, s'il devrait concerner uniquement les entreprises en position dominante ou s'étendre également aux entreprises non dominantes mais qui détiennent un pouvoir de marché, et enfin de quelle manière cet outil doit s'appliquer précisément.

La Commission européenne a conscience de la possibilité que les grandes plateformes se servent du respect de la vie privée pour justifier une modification des politiques et restrictions en matière de partage des données. Ces considérations sont complexes et n'en sont qu'à un stade préliminaire, et un certain nombre d'autorités chargées de la protection des données (dont l'autorité irlandaise) continuent de mener des enquêtes sur les principales plateformes, lesquelles enquêtes pourraient avoir une incidence sur certaines de ces pratiques. La législation sur la protection des données en tant que telle pourrait donc évoluer à court ou moyen terme. Par ailleurs, une autorité de la concurrence pourrait se voir confier la tâche, d'une part, d'examiner les effets sur la concurrence des comportements donnant lieu à une restriction de l'accès aux données des consommateurs et, d'autre part, de chercher un moyen d'encourager la concurrence tout en assurant la protection de la vie privée.

La **Colombie** partage ensuite son expérience de la mise en œuvre d'actions de promotion de la concurrence dans le but d'influencer l'élaboration des politiques dans différents domaines. L'autorité colombienne de la concurrence (*Superintendencia de Industria y Comercio*, SIC) dispose de compétences particulières en matière de concurrence, de protection des données et de protection des consommateurs. La SIC est engagée dans la promotion de la concurrence, ce qui passe notamment par i) la reconnaissance de la pertinence de la conformité aux politiques de protection des données et des consommateurs ; ii) l'évaluation des effets possibles sur la concurrence des mesures proposées impliquant la réglementation des activités économiques fondées sur les

données ; et iii) l'élaboration de recommandations visant à atténuer ces effets. Pour illustrer ses propos, la Colombie présente deux exemples :

- En 2013, la SIC a fait part de ses commentaires au ministère des Technologies de l'information et des communications relativement à un projet de réglementation établissant des obligations et conditions générales auxquelles devraient se soumettre les opérateurs de services postaux de paiement afin d'obtenir les qualifications nécessaires (systèmes et exigences en matière d'atténuation des risques et de gestion des actifs, par exemple) pour atténuer, entre autres, les risques de blanchiment de capitaux et de financement du terrorisme. La SIC mit en évidence que l'une des principales conséquences du projet était que les opérateurs de services postaux de paiement pourraient identifier les clients à partir d'informations à caractère personnel, comme leurs coordonnées, leur profession, leur signature ou leurs empreintes digitales. La SIC préconisa par conséquent l'application des dispositions du régime colombien de protection des données. En 2016, la SIC a infligé une amende à un opérateur de services postaux de paiement pour ne pas avoir informé convenablement les consommateurs que leurs données à caractère personnel seraient utilisées pour des propositions de commercialisation et de publicité sortant du périmètre de leur relation commerciale particulière. L'autorité considéra que les modalités de consentement de l'entreprise n'étaient pas suffisamment claires et précises concernant les moyens de collecte des données à caractère personnel, les droits des consommateurs en tant que personnes concernées et les coordonnées de la personne responsable du traitement des informations transmises dans le cadre d'une transaction commerciale.
- En 2017, la SIC a fait part de ses commentaires au ministère des Transports concernant les conditions d'interopérabilité des postes de péage assurant la perception électronique des droits applicables aux véhicules. L'objectif était d'établir les conditions juridiques, techniques et financières entre les intermédiaires et les opérateurs, afin de permettre aux utilisateurs signataires de contrats avec un intermédiaire de passer librement d'un système de péage à l'autre, assurant ainsi une interopérabilité à l'échelle nationale. L'opérateur serait ainsi responsable d'assurer le bon fonctionnement des routes et des péages électroniques, et de l'application des droits de péage. Le rôle de l'intermédiaire serait alors d'établir un contrat avec les utilisateurs et, entre autres, de percevoir les paiements des clients et verser une redevance aux opérateurs de péages pour l'exploitation de l'infrastructure routière. La projet proposait d'imposer plusieurs conditions et obligations aux opérateurs et aux intermédiaires en vue de l'obtention des certifications appropriées. Ce contexte suscitait toutefois des inquiétudes en matière de concurrence. D'après la SIC, définir certaines obligations pour permettre aux différents acteurs de communiquer semblait être une approche proportionnée et raisonnable.

L'**Australie** aborde ensuite la mise en œuvre du droit applicable aux données des consommateurs (DDC) adopté en août 2019. Le DDC a été volontairement élaboré de sorte à couvrir l'ensemble des données des consommateurs, mais son déploiement est échelonné par secteur, à commencer par le secteur bancaire, puis le secteur de l'énergie. La commission australienne de la concurrence et des consommateurs (*Australian Competition and Consumer Commission*, ACCC) est chargée d'élaborer les dispositions du DDC. L'ACCC est également l'organisme responsable de fournir les moyens technologiques à l'appui du partage de données et de l'application des règles de la concurrence. Le commissariat à l'information (*Office of the Australian Information Commissioner,* OAIC) joue également un rôle dans la mise en œuvre du DDC et ces deux organismes ont convenu

d'une politique commune de conformité et d'application du droit. L'ACCC et l'OAIC travaillent également en étroite collaboration avec le *Data Standards Board* chargé du développement des normes et structures pour le partage de données.

L'Australie indique également avoir tiré des enseignements de l'expérience du Royaume-Uni en matière de systèmes bancaires ouverts, et notamment le fait que la portabilité des données est un principe complexe et difficile à appliquer, ce qui explique le choix d'un déploiement progressif du DDC. Dans le cadre de cette approche échelonnée, à partir du 1er juillet 2020 les quatre principales banques australiennes seront en mesure de partager des informations de base sur les comptes d'épargne et d'opérations et sur les cartes de crédit des clients individuels. À partir du 1er novembre, le partage sera élargi aux données relatives aux prêts (dont les prêts immobiliers, les prêts d'investissement et les comptes d'ordre immobiliers), mais aussi aux comptes joints, aux comptes clôturés et, par le biais d'une série d'API complémentaires particulièrement utiles pour le partage de comptes, à des opérations comme les prélèvements automatiques et les paiements à échéance. À partir du 1er février 2021, les banques seront tenues de partager les données d'un grand nombre de comptes différents, comme les comptes fiduciaires et les mécanismes des financement d'actifs. L'un des principaux enjeux reste toutefois la sécurité. Dans la mesure où l'ACCC tiendra un registre des clés de sécurité afin de faciliter le partage de données, une discussion s'est engagée pour déterminer à qui incombe la responsabilité de garantir la sécurité de l'écosystème dans son ensemble. D'un point de vue international, une augmentation de la concurrence et un développement des échanges commerciaux transfrontières ne sont pas sans avantages. Certains obstacles restent toutefois à surmonter, comme les habilitations, l'identification des clients ou la mise en place de protections de la vie privée adaptées.

L'**Allemagne** intervient brièvement pour indiquer que le droit de la concurrence allemand est actuellement en cours de révision. Les modifications proposées incluent des dispositions relatives aux données et à l'accès à ces données. Il est notamment prévu d'élargir la théorie des installation essentielles, dont l'application était jusqu'à maintenant relativement limitée, afin de l'étendre à l'accès aux données Une autre modification porte sur l'accès aux données lorsqu'il existe un pouvoir de marché relatif, en particulier si une entreprise est impliquée dans la production de ces données. L'Allemagne souligne que ces modifications pourraient soulever des questions quant au rôle possible du RGPD si une autorité de la concurrence doit ouvrir l'accès aux données à caractère personnel à des acteurs tiers qui ont besoin de ces données pour être en mesure de soutenir la concurrence des principaux acteurs en place. Du moins s'agissant de l'Allemagne, de nouvelles avancées sont à prévoir concernant les données et l'accès aux données du point de vue du droit de la concurrence, de la politique de la concurrence et de leur application.

Le **Président** invite ensuite les experts à faire part de leurs derniers commentaires avant la conclusion de la table ronde, à commencer par M. Wolfgang Kerber.

M. Kerber revient sur les commentaires de M. Acquisti concernant l'approche stratégique et convient que les responsables de l'action publique doivent faire preuve de prudence par rapport aux politiques de protection des données et des consommateurs qui s'appuient sur le comportement de ces consommateurs. Autrement dit, dans quelle mesure informer les consommateurs et leur donner conscience de certains types de dangers est-il suffisant, que ce soit relativement au partage de données ou de manière plus générale ? M. Kerber partage le scepticisme de M Acquisti sur la pertinence de s'appuyer sur le comportement des consommateurs individuels pour assurer une protection efficace de la vie privée et souligne également que les consommateurs ne pourraient en réalité avoir qu'un choix limité en matière de respect de leur vie privée. Il préconise ainsi que les responsables de l'action publique se demandent si l'information des consommateurs peut réellement être suffisante

pour résoudre les défaillances du marché liées aux problèmes comportementaux et d'information, et par conséquent si une réglementation spécifique est nécessaire.

Le **Président** invite M^me^ Elizabeth Denham à prendre une dernière fois la parole.

M^me^ Denham estime qu'au cours des cinq prochaines années la concurrence, la protection des consommateurs et la protection des données seront encore plus étroitement liées, et qu'elles évolueront en parallèle. Cette évolution est inhérente au fonctionnement de l'économie numérique et au rôle même de ces données (pour la plupart à caractère personnel). Elle reprend également à son compte les propos de M. Kerber et indique que même si les responsables publics et les autorités de la concurrence tentent de sensibiliser les consommateurs au traitement de leurs données dans un écosystème spécifique, ceux-ci s'attendent à ce que quelqu'un d'autre assure leurs arrières (soit les pouvoirs publics). Les consommateurs imaginent qu'il existe une ou plusieurs autorités qui « veillent au grain » (surtout dans le cas des grandes plateformes), qui ont établi des normes à respecter et qui interviennent lorsqu'un consommateur, une personne concernée ou un marché subit un préjudice. Il n'est donc pas raisonnable de penser que les consommateurs comprennent toutes les implications de ce à quoi ils consentent. Pour conclure, M^me^ Denham précise que le consentement va de plus en plus souvent être remis en cause dans le monde numérique et qu'au lieu de s'en remettre au simple consentement des consommateurs, les normes de gouvernance des données, la promotion de pratiques éthiques et l'adoption d'une approche normative plus systémique vont jouer un rôle grandissant.

Le **Président** remercie enfin les experts, ainsi que les pays ayant participé à la table ronde que ce soit par lors des débats ou à travers leurs contributions écrites. Il souligne que d'importants points d'accord se sont dégagés. Le premier a trait aux interactions qui existent la concurrence et la protection des données, et au fait que ces deux domaines d'action, dont les objectifs sont différents, peuvent selon les circonstances se renforcer mutuellement ou entrer en conflit l'un avec l'autre. Le second concerne l'existence d'une tendance, au niveau de l'élaboration des politiques, vers davantage de coopération, un facteur particulièrement important pour éviter les conflits. S'agissant des mesures correctrices, il apparaît en outre clairement que dans la plupart des cas des échanges plus suivis entre les organismes de protection des données et les autorités de la concurrence pourraient s'avérer bénéfiques. Un aspect sur lequel des différences sont ressorties et sur lequel les experts ont particulièrement insisté est le fait qu'en la matière les consommateurs ne sont pas toujours en mesure de faire les choix auxquels ils aspirent en réalité. Les efforts engagés dans la promotion de la concurrence, ou même dans la promotion de la protection des données, peuvent ainsi ne pas être suffisants pour permettre aux consommateurs d'exprimer leurs véritables préférences.

Deux questions se posent alors. D'une part, ce problème devrait-il être pris en considération dans l'analyse des autorités de la concurrence ? Le sentiment général qui se dégage de la table ronde est qu'il encore trop tôt pour cela et nous manquons d'informations pertinentes. La tendance n'est pas à l'abandon des analyses classiques, sauf sans certaines juridictions, et l'Allemagne a clairement choisi une approche différente. D'autre part, si l'on considère, à l'instar des spécialistes de l'économie comportementale, que les choix des consommateurs sont particulièrement contraints en matière de données, quelle incidence cela peut-il avoir sur la valeur de la concurrence en termes de promotion du bien-être des consommateurs ? Autrement dit, nous partons du postulat qu'une augmentation de la concurrence permet une amélioration du bien-être des consommateurs. Cela vaut-il encore dans un domaine où les consommateurs peuvent ne pas avoir conscience des choix qui s'offrent à eux, des choix qu'ils devraient faire ou même de ce que sont réellement leurs préférences ? Face à ces interrogations, il pourrait être intéressant d'aborder de nouveau

ces thèmes avec les experts présents lorsque nous aurons renforcé la coopération entre nos autorités de la concurrence et nos différents organismes de protection des données.

Références

González Fuster, G., R. van Brakel et P. De Hert (dir. pub.) (2019), *Data Protection and Competition Law: The Dawn of 'Uberprotection'*, Edward Elgar Publishing, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290824. [1]

OCDE (2020), *Consumer data rights and competition – Note by Brazil*, https://one.oecd.org/document/DAF/COMP/WD(2020)41/en/pdf. [3]

OCDE (2020), *Consumer data rights and competition – Note by the United States*, https://one.oecd.org/document/DAF/COMP/WD(2020)39/en/pdf. [2]