Organisation de Coopération et de Développement Économiques

DAF/COMP(2020)1

Non classifié **Français - Or. Anglais**

2 juin 2020

DIRECTION DES AFFAIRES FINANCIÈRES ET DES ENTREPRISES
COMITÉ DE LA CONCURRENCE

Droits relatifs aux données des consommateurs et impact sur la concurrence – Note de référence du Secrétariat

10 au 12 juin 2020

Ce document a été préparé par le Secrétariat de l'OCDE pour servir de document de travail à l'appui de la réunion du Comité de la concurrence qui se tiendra le 12 juin 2020.

Les opinions exprimées et les arguments employés ici ne reflètent pas nécessairement le point de vue officiel de l'Organisation ou des gouvernements de ses pays membres.

D'autres documents consacrés à ce sujet sont disponibles à l'adresse suivante : http://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]

JT03462409

Droits relatifs aux données des consommateurs et impact sur la concurrence

Par le Secrétariat[*]

À mesure qu'augmente le nombre de consommateurs de l'économie numérique qui s'appuient sur des services fondés sur les données, les droits relatifs aux données des consommateurs suscitent un intérêt croissant à travers le monde. Ces droits peuvent notamment inclure des droits fondamentaux à la protection de la vie privée, ainsi que tout un éventail de mesures comme la portabilité des données, laquelle vise à donner aux consommateurs un meilleur contrôle de leurs données.

Ce document examine comment la politique de la concurrence et son application peuvent encourager une concurrence plus efficace dans les marchés impliquant les données des consommateurs. Un niveau de concurrence effectif permet théoriquement d'améliorer les résultats pour les consommateurs en assurant une protection renforcée de leur vie privée et un contrôle accru de leurs données à caractère personnel. Cela ne semble toutefois pas être une règle absolue, notamment lorsque les consommateurs n'exercent pas les droits qu'ils ont sur leurs données, potentiellement en raison de biais comportementaux ou de l'absence apparente de choix. Il existe donc un débat sur la nécessité, et le cas échéant sur la manière, d'incorporer dans le cadre de l'application du droit de la concurrence une évaluation de l'incidence des pratiques visées sur l'efficacité de la protection des données et de la vie privée. Certaines questions se posent également sur la possession de données des consommateurs et notamment si celle-ci dresse des obstacles à l'entrée ou si la théorie des installations essentielles peut permettre de résoudre ces problèmes. Certains aspects des droits relatifs aux données des consommateurs, comme la portabilité des données, ont néanmoins justement pour objectif de promouvoir la concurrence en facilitant la comparaison et le changement de prestataires. On ignore toutefois précisément comment mettre ces mesures en œuvre pour encourager au mieux la concurrence.

Ce document a également pour objectif d'analyser ces problématiques et finit par démontrer que la politique de la concurrence et son application jouent bel et bien un rôle dans l'amélioration des résultats pour les consommateurs dans les marchés exploitant leurs données. Dans l'idéal, ces mesures doivent être déployées en collaboration avec les organismes publics chargés de la protection des données, ainsi que de la politique de protection des consommateurs et de son application.

[*] Ce document a été préparé par Anna Barker de la Division de la concurrence de l'OCDE. Il a par ailleurs été enrichi des commentaires d'Antonio Capobianco, Pedro Caro de Sousa, Pedro Gonzaga, Chris Pike et Ania Thiemann (tous membres de la Division de la concurrence de l'OCDE).

Table des matières

1. Introduction

1. La transformation numérique modifie en profondeur nos économies et nos sociétés, et s'appuie pour cela en partie sur la collecte et l'utilisation d'un volume de données des consommateurs en constante augmentation. Les données sont ainsi devenues un enjeu majeur et l'on estime que la quantité de données produites dans le monde passera de 33 zettaoctets en 2018 à 175 zettaoctets en 2025 (Commission européenne, 2020[1]). Pour donner un ordre de grandeur, un zettaoctet correspond à environ 250 milliards de DVD (Arthur, 2011[2]). Nous assistons par ailleurs à *« l'émergence d'un écosystème de données mondial dans lequel les services d'analyse et de données sont commercialisés et utilisés dans tous les secteurs et au-delà des frontières nationales »* (OCDE, 2015, p. 24[3]).

2. De nombreuses entreprises s'appuient aujourd'hui sur les données qu'elles recueillent auprès de leurs consommateurs lorsque ces derniers utilisent l'internet, des applications numériques ou encore des appareils de l'internet des objets (IdO). Dans ce contexte, l'utilisation des données des consommateurs a favorisé et continuera d'encourager la création d'un large éventail de biens, de services et de modèles économiques innovants, et ce, souvent pour un prix monétaire égal à zéro. En outre, l'analyse des données des consommateurs, seules ou associées à d'autres types de données, par des systèmes d'intelligence artificielle (IA) permet d'émettre de nouvelles prédictions et d'apporter de nouveaux éclairages sur les domaines les plus divers. Bien que les avantages pour les consommateurs soient évidents, l'utilisation que font les entreprises des données des consommateurs suscite également des préoccupations. Par exemple, comment garantir la protection de la vie privée et s'assurer que les entreprises et autres parties prenantes n'exploitent pas les données des consommateurs d'une manière préjudiciable à ces derniers ? Face à ces problématiques, différents pays de l'OCDE ont récemment adopté, ou prévoient d'adopter, de nouvelles législations relatives aux données des consommateurs afin de renforcer la protection de la vie privée et améliorer le contrôle des consommateurs sur leurs données.

3. Les modèles économiques basés sur la collecte et l'utilisation des données des consommateurs soulèvent également des questions inédites en termes de politique de la concurrence. Ainsi, dans les marchés où les entreprises se livrent une concurrence sur la question de la protection de la vie privée, comment les autorités de la concurrence doivent-elles intégrer cette dimension dans leurs évaluations d'impact sur la concurrence ? Quand et de quelle manière les données des consommateurs pourraient-elles constituer des obstacles à l'entrée ou à l'expansion ? Dans quels cas les données des consommateurs pourraient-elles représenter une ressource essentielle pour les entreprises en aval ou ayant des activités complémentaires ou concurrentes ? Enfin, quelles répercussions peuvent avoir les décisions réglementaires et des entreprises en matière de collecte, de stockage et d'utilisation des données des consommateurs à la fois sur la concurrence et sur l'économie dans son ensemble ?

4. Le présent document examine ces questions et analyse l'impact des droits relatifs aux données des consommateurs et de leur utilisation de manière plus large sur la politique de la concurrence et son application.

1.1. Travaux antérieurs de l'OCDE

5. Ce document s'appuie sur les travaux déjà réalisés par le Comité de la concurrence, ainsi que d'autres travaux menés au sein de l'OCDE, notamment dans le domaine de la protection des données et de la vie privée, tel que décrit ci-dessous.

1.1.1. Travaux du Comité de la concurrence

6. Le Comité de la concurrence a abordé pour la première fois les questions liées aux données des consommateurs en novembre 2016 à l'occasion d'une audience sur les données massives (OCDE, 2016[4]). Ces discussions ont notamment permis d'introduire la notion de « données massives », de décrire l'écosystème des données massives et d'examiner leurs implications pour l'application du droit de la concurrence. Depuis lors, les réglementations, les marchés et le droit de la concurrence ont connu de nombreuses évolutions. Il semble ainsi opportun d'aborder à nouveau ces questions plus précisément dans le contexte des données des consommateurs.

7. Différentes tables rondes tenues en 2018 ont par ailleurs confirmé la pertinence des données des consommateurs pour les débats menés. La protection de la vie privée peut par exemple présenter un intérêt particulier en termes de concurrence lorsqu'elle constitue un facteur de qualité pour un bien ou un service donné. La question de la protection de la vie privée (y compris par le biais de la concurrence dans les niveaux de protection assurés par les entreprises) a ainsi été abordée à l'occasion de la table ronde sur les effets hors prix des fusions de juin 2018 et de la table ronde sur la problématique de la qualité dans les secteurs numériques de l'économie sans contrepartie financière de novembre 2018 (OCDE, 2018[5] ; OCDE, 2018[6]). La collecte et l'utilisation des données des consommateurs ont également été examinées lors de la table ronde sur la personnalisation des prix à l'ère numérique, partant du constat que l'augmentation de l'utilisation des données des consommateurs et les progrès réalisés en matière d'analyse ont pu susciter des préoccupations sur la capacité des entreprises à mettre en œuvre des méthodes de personnalisation des prix, et plus particulièrement dans les marchés numériques (OCDE, 2018[7]). Les problèmes liés à la protection de la vie privée ont quant à eux fait partie des sujets abordés lors de la table ronde sur la disruption numérique sur les marchés financiers, organisée à l'occasion de la Journée portes ouvertes de la concurrence à l'OCDE en février 2020 (OCDE, 2020[8]).

8. Deux autres tables rondes, prévues pour juin 2020 dans le cadre des réunions du Comité de la concurrence, auront également trait aux questions de concurrence et des données des consommateurs. Ces tables rondes auront pour objet, d'une part, les start-ups, les acquisitions anticoncurrentielles et les seuils de contrôle des fusions, et d'autre part, les effets conglomérauxdes fusions (OCDE, 2020[9] ; OCDE, 2020[10]).

1.1.2. Autres travaux de l'OCDE

9. L'OCDE a joué un rôle de pionnier dans l'élaboration des politiques de protection des données et de la vie privée au sein de ses pays membres. Les Lignes directrices de l'OCDE sur la protection de la vie privée, initialement adoptées en 1980, furent les premiers principes approuvés au niveau international relatifs à la protection des données à caractère personnel dans l'ensemble des secteurs publics et privés. Les normes minimales définies dans les Lignes directrices ont influencé l'élaboration des politiques et législations mises en œuvre dans les pays de l'OCDE et au-delà. Ces Lignes directrices ont été réexaminées en 2010, puis révisées en 2013, afin de prendre en compte l'importante évolution du rôle des données à caractère personnel dans l'économie au fil du temps (OCDE, 2013[11]).

10. Les Lignes directrices établissent huit principes de base : limitation en matière de collecte, qualité des données, spécification des finalités, limitation de l'utilisation, garanties de sécurité, transparence, participation individuelle et responsabilité. Les Lignes directrices couvrent également la mise en œuvre pratique de la protection de la vie privée et les efforts nécessaires pour faire face à la dimension mondiale de la protection de la vie privée grâce à une interopérabilité améliorée. Elles proposent également une approche modernisée des

flux transfrontières de données, développent le principe de responsabilité et renforcent les mesures de protection de la vie privée. Organe de la Direction de la science, de la technologie et de l'innovation (STI), le Groupe de travail sur la gouvernance des données et la vie privée (GTGDVP) du Comité de la politique de l'économie numérique de l'OCDE (CPEN) passe actuellement en revue les Lignes directrices. Les résultats de cet examen sont attendus avant la fin de l'année 2020.

11. Le GTGDVP a par ailleurs entrepris un projet sur la portabilité des données, lequel étudiera entre autres l'incidence de cette portabilité sur la concurrence en s'inspirant de la théorie et des données empiriques pertinentes. Ce projet devrait se poursuivre sur l'ensemble de l'année 2020, voire 2021. D'autres publications de la STI présentent un intérêt certain pour l'objet du présent document, comme un rapport datant de 2015 sur l'innovation fondée sur les données, ainsi qu'un rapport de 2018 sur l'amélioration de l'accès aux données et de leur partage (OCDE, 2015[3] ; OCDE, 2019[12]). Ces deux rapports offrent en effet un bon aperçu de la façon dont les différents acteurs recueillent, analysent et exploitent les données à l'échelle de l'économie, ainsi que des obstacles qui entravent un partage plus généralisé des données.

12. Le Comité de la politique à l'égard des consommateurs de l'OCDE a par ailleurs publié un guide de bonnes pratiques relatives aux données des consommateurs, lequel propose une approche de la politique de protection des consommateurs et de son application sur la question des données des consommateurs, notamment dans les cas où les entreprises ont adopté des pratiques trompeuses, mensongères ou déloyales, en rapport avec ce type de données (OCDE, 2019[13]). Cette problématique est abordée de façon plus approfondie dans la section 5.2.

1.2. Structure

13. Pour commencer, ce document offre une définition des données des consommateurs et présente les différents types de droits relatifs à ces données (section 2). La section 3 aborde la manière dont les entreprises recueillent et utilisent les données, ainsi que leurs motivations à les partager. Elle examine également les possibles défaillances du marché liées aux entreprises qui collectent et exploitent les données des consommateurs. La section 4 s'intéresse ensuite au rôle de l'application du droit de la concurrence, d'une part, dans la promotion de la protection de la vie privée et, d'autre part, dans l'évaluation de la concurrence dans les marchés impliquant les données des consommateurs. Elle aborde plus particulièrement les théories du préjudice possibles, les difficultés analytiques (y compris la définition du marché, les obstacles à l'entrée, l'attitude des consommateurs à l'égard de la protection de la vie privée, la mesure de la protection des données et les gains d'efficience), les mesures correctrices potentielles et le rôle éventuel de la théorie des installations essentielles. La section 5 traite ensuite de la façon dont les droits relatifs aux données affectent la concurrence et le besoin de coopération entre les autorités réglementaires compétentes. La section 6 présente enfin quelques conclusions.

2. Que sont les données des consommateurs et les droits relatifs aux données des consommateurs ?

14. La présente section propose une définition pratique des données des consommateurs, en aborde les différentes typologies et offre une vue d'ensemble des divers types de droits relatifs aux données des consommateurs disponibles dans les pays de l'OCDE.

2.1. Qu'entend-on par données des consommateurs ?

15. L'expression « données des consommateurs » se rapporte aux données relatives aux consommateurs qui ont été recueillies, échangées ou utilisées dans le cadre d'une relation commerciale.

16. Cette notion est par certains aspects plus restrictive que celle des « données à caractère personnel », lesquelles sont définies comme « *toute information relative à une personne physique identifiée ou identifiable (personne concernée)* » (OCDE, 2013, p. 13[11]). Ainsi, les « données à caractère personnel » englobent les données des individus, à la fois en leur qualité de citoyens que de consommateurs. La notion de données des consommateurs utilisée dans le présent document s'applique toutefois uniquement aux données des individus en tant que consommateurs, dans la mesure où la politique de la concurrence et son application ont pour objet les transactions commerciales. Autrement dit, les « données des consommateurs » n'incluent pas les données recueillies, échangées ou utilisées par les gouvernements ou autres agents ou organismes non commerciaux, lesquelles peuvent susciter d'autres préoccupations.

17. Les « données des consommateurs » ont néanmoins un sens plus large que les « données à caractère personnel » car elles englobent les données relatives aux consommateurs même lorsque ces données peuvent ne pas nécessairement être réattribuées aux personnes concernées. Bien que les données de ce type puissent ne pas soulever les mêmes préoccupations au regard de la législation sur la protection des données et de la vie privée (laquelle vise principalement les « données à caractère personnel »), elles peuvent présenter un intérêt pour l'évaluation d'impact sur la concurrence, comme présenté plus en détail dans la section 4.

2.2. Typologies des données des consommateurs

18. Les données des consommateurs sont hétérogènes (Crémer, de Montjoye et Schweitzer, 2019[14]) et leur valeur privée et sociale dépend de la manière dont elles sont utilisées. Cette valeur peut en outre varier d'un intervenant de la chaîne de valeur à l'autre (Acquisti, Taylor et Wagman, 2016[15]). Comprendre les différentes dimensions des données des consommateurs s'avère ainsi essentiel pour mieux appréhender la valeur potentielle des divers types de données des consommateurs. Il existe à ces fins plusieurs moyens de classer les données des consommateurs, et notamment : (i) par type de données collectées ; (ii) par origine des données ; ou (iii) selon que les données des consommateurs sont ou non de nature à permettre d'identifier les individus. Chacune de ces classifications est examinée ci-après de manière succincte.

19. Une première manière de classer les données est en fonction du type d'informations recueillies (Robertson, 2020[16] ; Kemp, 2019[17] ; OCDE, 2013[18]), lesquelles peuvent notamment prendre les formes suivantes :

- **Contenus d'utilisateur** : articles de blogs et commentaires, photos et vidéos, communications avec d'autres parties, etc. ;
- **Données liées à l'activité ou au comportement** : ce que les individus recherchent sur l'internet, les sites qu'ils consultent, les applications qu'ils utilisent, ce qu'ils achètent en ligne, combien et comment ils paient, leurs habitudes et préférences, etc. Les produits IdO peuvent également recueillir des informations comme le contenu des conversations ou des données relatives à la santé, par exemple sur le rythme cardiaque, le sommeil ou l'activité physique (voir l'Encadré 1) ;

- **Données sociales** : contacts et amis sur les sites de réseaux sociaux et sur les applications de communication ;
- **Données de localisation** : adresse du domicile, géolocalisation (p. ex. à partir d'un téléphone portable), adresse IP, proximité avec d'autres parties, etc. ;
- **Données socioéconomiques** : âge, sexe, origine ethnique, revenus, orientation sexuelle, affiliations politiques, etc. ;
- **Données officielles d'identification** : nom, informations financières et numéros de comptes, informations médicales, numéro de sécurité sociale, casier judiciaire, etc. ;
- **Données biométriques** : empreintes digitales, données de reconnaissance faciale, oculaire ou vocale, etc.

20. Cette liste montre la grande variété des données des consommateurs qui sont recueillies et utilisées par les entreprises, et met en évidence certains des problèmes délicats posés par ces données en termes de protection de la vie privée.

Encadré 1. L'internet des objets

Selon l'OCDE, l'internet des objets (IdO) désigne :

> *... les appareils et objets dont l'état peut être modifié via l'internet, avec ou sans la participation active des utilisateurs.*

Entrent également dans cette catégorie les objets et capteurs qui recueillent des données et les communiquent à d'autres dispositifs ou à des personnes. Cette communication, associée aux services infonuagiques, à l'analyse des données et à la téléopération, est ce qui donne à ces types d'applications leur caractère « intelligent ». Les technologies IdO sous-jacentes incluent les semi-conducteurs (capteurs, puces, processeurs et mémoire), les modules et appareils (logiciels), les plateformes IdO (systèmes d'exploitation) et le réseau (connectivité ; aspect susceptible de présenter des problèmes de normalisation et l'interopérabilité).

Certains de ces appareils connectés seront placés dans des habitations privées, offrant entre autres des fonctions de gestion de l'énergie, de sécurité ou de divertissement. D'autres seront associés à des initiatives de développement dans des domaines comme le transport, la santé ou les activités de fabrication. Dans les pays de l'OCDE, le nombre d'appareils connectés à l'intérieur et à proximité du domicile des utilisateurs devrait passer de 1 milliard en 2016 à 14 milliards à l'horizon 2022. On estime par ailleurs que le parc mondial d'appareils IdO connectés devrait atteindre 75.44 milliards en 2025, ce qui représente une multiplication par cinq en l'espace de dix ans. Ces appareils sont l'une des sources principales de données pour l'analyse des données massives, et une grande partie d'entre elles sont des données des consommateurs, parmi lesquelles les conversations, la localisation, l'adresse de domicile, les habitudes sportives ou de loisirs, ou encore les signes physiologiques des consommateurs.

Source : OCDE (2015[19]) ; OCDE (2018[20]) ; OCDE (2018[21]) ; Statistica (2020[22])

2.2.1. Origine des données

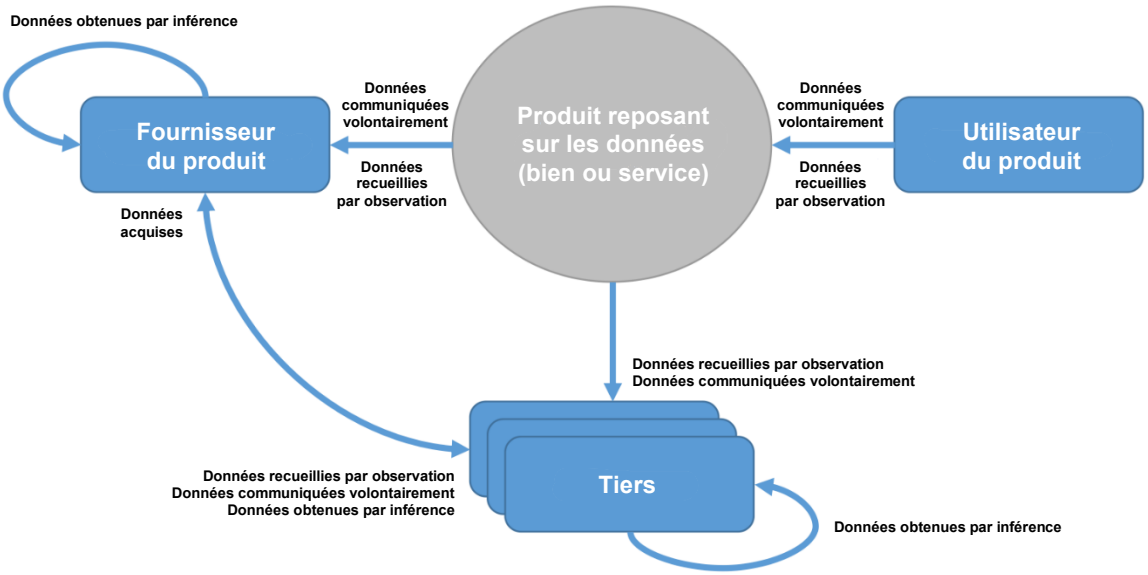
21. Les données des consommateurs peuvent également être classées en fonction de leur origine. À ces fins, l'OCDE (2019[12]) a proposé les quatre catégories suivantes[1] :

1. Les **données communiquées volontairement** sont les données fournies par les individus lorsqu'ils partagent expressément des informations sur eux-mêmes ou d'autres parties. Il peut notamment s'agir d'identifiants de connexion, de billets sur les réseaux sociaux ou d'informations de carte bancaire dans le cas d'achats en ligne.
2. Les **données recueillies par observation** sont les données créées lorsque les activités d'un individu sont enregistrées. Celles-ci sont générées de manière passive par les individus et parfois sans qu'ils en aient conscience. Il peut notamment s'agir du suivi de localisation ou des activités de navigation en ligne.
3. Les **données obtenues par inférence** sont créées à partir de l'analyse de données et incluent les données déduites automatiquement à partir d'autres données ou grâce à des techniques plus sophistiquées. Les cotes de solvabilité en sont un exemple. Les individus n'ont généralement pas connaissance de ces données, et celles-ci peuvent être générées sans même que les personnes concernées ne soient réellement informées de leur création.
4. Les **données acquises (achetées ou cédées sous licence)** sont obtenues auprès de tiers dans le cadre de contrats de licences (p. ex. : courtiers en données) ou par des moyens non commerciaux (p. ex. : initiatives d'ouverture de l'administration). Certaines obligations tant contractuelles que juridiques peuvent affecter la réutilisation et le partage de ce type de données.

22. Les relations qui existent entre les différentes catégories de données des consommateurs sont illustrées dans le Graphique 1.

[1] Cette classification s'inspire des approches d'Adams (2014[187]) et de la Commission de la productivité (2017[188]). Elle concorde également avec celle de Crémer, Montjoye et Schweitzer, dans leur rapport sur la politique de la concurrence à l'ère numérique établi pour la Commission européenne (2019[14]).

Graphique 1. Types de données des consommateurs et leurs modes de création



Source : OCDE (2019[12])

23. La pertinence de cette classification pour les pouvoirs publics est double. D'une part, la manière dont les données sont générées a une incidence sur le niveau de conscience des consommateurs vis-à-vis de leurs données, ce qui constitue un facteur important pour gérer problèmes d'asymétrie de l'information associés à la collecte et à l'utilisation des données des consommateurs. Ce niveau de conscience sera ainsi le plus élevé pour les informations que les consommateurs ont communiquées volontairement, plus limité pour les informations recueillies par observation, et encore plus faible pour les données acquises ou les données obtenues par inférence. D'autre part, on peut estimer que les données communiquées volontairement (et potentiellement les données recueillies par observation) sont moins susceptibles que les données acquises ou que les données obtenues par inférence d'être déclarées par les entreprises comme ayant été « créées » par leur soins. Cet aspect est important pour comprendre les motivations des entreprises à partager ces différents types de données, ainsi que les effets des politiques liées à la portabilité et à l'interopérabilité des données, lesquelles doivent permettre des arbitrages équilibrés entre la promotion de la concurrence et le maintien des incitations à l'investissement, sans oublier les préoccupations des tiers en matière de protection de la vie privée. Ces questions sont abordées de façon plus approfondie dans la section 5.1.1.

2.2.2. Identification des données à caractère personnel

24. Les données à caractère personnel peuvent également être classées en fonction leur capacité à permettre l'identification des individus. La norme ISO/IEC 19441 définit en la matière cinq catégories de données :

1. Les **données identifiées**, associées de manière incontestable à un individu spécifique ;
2. Les **données pseudonymisées**, dans lesquelles des alias remplacent les identifiants personnels. Ces identifiants peuvent uniquement être rétablis par la partie qui a affecté les alias utilisés ;
3. Les **données pseudonymisées sans lien**, dans lesquelles tous les identifiants sont supprimés ou remplacés par des alias dont les liens de correspondance ont été

supprimés ou dont l'affectation est irréversible, de sorte que les identifiants ne peuvent être rétablis par quelque partie que ce soit ;

4. Les **données anonymisées**, lesquelles ont été modifiées (par exemple, dont les valeurs d'attributs sont généralisées ou affectées de façon aléatoire) et dans lesquelles tout lien a été supprimé, de sorte à assurer un niveau de confiance raisonnable quant à l'impossibilité d'identifier un individu ;

5. Les **données agrégées**, qui ne contiennent aucune entrée au niveau individuel et qui rassemblent des informations relatives à suffisamment de personnes différentes pour que leurs attributs individuels ne soient pas identifiables (ISO/IEC, 2018[23]).

25. La pertinence de cette classification réside dans le fait que, lorsque les données ne peuvent être attribuées à un individu spécifique, elles sont moins susceptibles de relever de la législation sur la protection de la vie privée. Ces données peuvent ainsi générer des avantages économiques et proconcurrentiels sans pour autant susciter des préoccupations en matière de protection de la vie privée par compensation (OCDE, 2019[12]). En pratique, il peut toutefois s'avérer difficile de protéger les données anonymes d'une éventuelle réidentification (PCAST, 2013[24]). En raison des externalités associées aux données des consommateurs (voir la section 3.4.2), même les données non identifiées pourraient en outre être combinées à des données identifiées pour mieux cerner les individus ou faciliter la personnalisation des prix, par exemple.

2.2.3. Les quatre V

26. Les données des consommateurs peuvent également être abordées sous l'angle des « quatre V » : volume, vitesse, variété et valeur (OCDE, 2016[4] ; Stucke et Grunes, 2016[25]). Ainsi, la **valeur** des données, notamment en termes de précision des prédictions (laquelle peut permettre une amélioration des biens et services, ainsi qu'un meilleur ciblage des annonces pour augmenter les recettes publicitaires ; voir la section 3.3.1) a connu un croissance significative du fait de l'augmentation du volume, de la vitesse et de la variété des données (Gal et Rubinfeld, 2019[26]) :

- Deux facteurs essentiels sont à l'origine de ces augmentations importantes du **volume** disponible de données des consommateurs :
  - la baisse des coûts de la collecte, du stockage, du traitement et de l'analyse des données ;
  - l'essor de l'activité en ligne des consommateurs, encouragé par un accès renforcé à l'internet à haut débit et par la multiplication des biens et services connectés ou en ligne, y compris ceux fournis par les appareils IdO (voir l'Encadré 1) (OCDE, 2015[3]).
- Ces mêmes facteurs ont entraîné une augmentation de la **vitesse** à laquelle les données sont générées, consultées, traitées et analysées. Certaines entreprises sont aujourd'hui en mesure d'établir des prédictions en temps réel (technique appelée « prévision immédiate ») (Stucke et Grunes, 2016[25]).
- La **variété** des données joue également un rôle dans leur valeur. Cet aspect est particulièrement important dans le cas des données des consommateurs, en ce sens qu'une plus grande variété permet de renforcer la précision des efforts de personnalisation, que ce soit sous la forme de recommandations, d'offres ou d'annonces ciblées (Stucke et Grunes, 2016[25]).

27. Dans la mesure où le volume, la vitesse et la variété des données contribuent à leur valeur, ces dimensions pourraient être prises en compte dans les évaluations d'impact sur

la concurrence dans le cas des entreprises axées sur les données. Cette approche pourrait ainsi s'avérer utile lors de l'évaluation d'une fusion impliquant la mise en commun de sources de données ou lorsqu'il s'agit de déterminer si l'accès d'une entreprise à des données constitue un obstacle à l'entrée ou lui confère un avantage concurrentiel (voir la section 4.2.2).

2.3. Droits relatifs aux données des consommateurs

28. Cette section donne un aperçu des types de droits relatifs aux données des consommateurs en vigueur dans les pays membres de l'OCDE. Elle présente plus particulièrement le cadre général de protection de la vie privée appliqué dans l'OCDE et met en avant certains droits spécifiques dont bénéficient les particuliers dans les pays membres.

2.3.1. Droits généraux

29. La plupart des pays de l'OCDE ont mis en place une forme de législation pour la protection des données, conforme à la fois au cadre proposé dans les « Lignes directrices de l'OCDE sur la protection de la vie privée » et aux huit principes énoncés dans l'Encadré 2 (OCDE, 2013[11]). Ces législations visent à assurer une protection élémentaire de la vie privée, tout en octroyant aux personnes concernées des droits permettant un meilleur contrôle de leurs données. La plupart des juridictions ont notamment adopté une approche basée sur le consentement, laquelle donne aux consommateurs la possibilité de gérer la manière dont leurs données sont recueillies et utilisées en accordant ou non leur consentement. Dans certains pays, la législation sur la protection des données prévoit par ailleurs d'autres droits spécifiques, parmi lesquels :

- un droit de rectification des informations erronées, lequel permet aux personnes concernées de demander au maître du fichier la correction d'informations personnelles inexactes ;
- un droit à l'oubli, lequel permet aux personnes concernées de demander la suppression de données à caractère personnel ;
- un droit à la portabilité des données, lequel permet aux personnes concernées de demander le transfert de leurs données à caractère personnel d'un maître de fichier à un autre.

30. Ces droits sont prévus dans le Règlement général sur la protection des données (RGPD) (voir l'Encadré 3), la principale législation en matière de protection des données en Europe. Des droits comparables ont été adoptés dans certaines régions des États-Unis et notamment en Californie dans le cadre du CCPA (*California Consumer Privacy Act*).

31. Aux États-Unis, les droits relatifs aux données relèvent actuellement de la compétence des États, bien que la Commission fédérale du commerce (*Federal Trade Commission* ou FTC) ait autorité pour veiller à ce que les entreprises ne s'adonnent pas à des manœuvres ou pratiques déloyales ou trompeuses, y compris relativement aux données (voir également la section 5.2). Des législations au niveau fédéral sont par ailleurs également à l'étude, comme le *DASHBOARD Act*, qui obligerait les plateformes recueillant des données à renforcer la transparence en matière de collecte et d'utilisation des données, la loi *Own Your Own Data Act*, qui donnerait aux utilisateurs un droit de propriété exclusif sur leurs données en ligne (Chakrovorti,, 2020[27]), ou encore la loi *ACCESS Act*, qui exigerait la portabilité des données pour les plateformes de médias sociaux comptant plus de 100 millions d'utilisateurs aux États-Unis.

Encadré 2. Principes de protection de la vie privée de l'OCDE

L'OCDE a établi huit principes de protection de la vie privée :

1. **Limitation en matière de collecte :** il conviendrait d'assigner des limites à la collecte des données à caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux, après en avoir informé la personne concernée ou avec son consentement.
2. **Qualité des données :** les données à caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et elles devraient être exactes, complètes et tenues à jour.
3. **Spécification des finalités :** les finalités en vue desquelles les données à caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données, et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités.
4. **Limitation de l'utilisation :** les données à caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées, si ce n'est : a) avec le consentement de la personne concernée ; ou b) lorsqu'une règle de droit le permet.
5. **Garanties de sécurité :** il conviendrait de protéger les données à caractère personnel grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés.
6. **Transparence :** il conviendrait d'assurer la transparence des pratiques de collecte et d'utilisation des données afin de permettre aux personnes de déterminer l'existence et la nature des données à caractère personnel, et les finalités de leur utilisation, de même que l'identité du maître du fichier et le siège de ses activités.
7. **Participation individuelle :** toute personne physique devrait avoir le droit :
   a. D'obtenir du maître d'un fichier confirmation du fait qu'il détient ou non des données la concernant ;
   b. De se faire communiquer les données la concernant (i) dans un délai raisonnable, (ii) moyennant, éventuellement, une redevance modérée, (iii) selon des modalités raisonnables, et (iv) sous une forme qui lui soit aisément intelligible ;
   c. D'être informée des raisons pour lesquelles une demande qu'elle aurait présentée est rejetée et de pouvoir contester un tel rejet ;
   d. De contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.
8. **Responsabilité** : tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Source : OCDE (2013[11])

32. De la même manière, en Australie, le *Privacy Act 1988* prévoit lui aussi une série de droits pour les particuliers, y compris le droit de savoir quelles informations personnelles sont recueillies, comment elles seront utilisées et à qui elles seront divulguées, la possibilité de ne pas être identifié et de demander à avoir accès à ses informations personnelles, ou encore le droit de rectifier les informations personnelles erronées. Une nouvelle loi promulguée en 2017 a par ailleurs établi un « droit applicable aux données des consommateurs » visant à faciliter la portabilité des données (ce droit est abordé plus en détail dans la section suivante). Parmi d'autres exemples de législations comparables, citons la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* et la *Loi sur la protection des renseignements personnels* au Canada, et le *Privacy Act 1993* en Nouvelle-Zélande.

Encadré 3. Règlement général européen sur la protection des données (RGPD)

Le RGPD prévoit un certain nombre de droits pour les citoyens européens, parmi lesquels :

- le droit à l'accès aux données à caractère personnel (article 15) ;
- le droit de rectification des données à caractère personnel inexactes (article 16) ;
- le droit à l'effacement ou « droit à l'oubli » (article 17) ;
- le droit à la portabilité des données (article 20) ;
- le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, sauf exceptions (article 22).

Le RGPD inclut notamment d'autres éléments importants, dont :

- une définition révisée et élargie des données à caractère personnel (article 4) ;
- un renforcement du régime de consentement relativement à la collecte et au traitement des données à caractère personnel (articles 6 et 7) ;
- une exigence de transparence et de simplicité d'accès pour les politiques de protection de la vie privée (articles 12, 13 et 14) ;
- un champ d'application territorial élargi (article 3) ;
- une exigence de protection des données dès la conception et par défaut (article 25) ;
- des amendes administratives plus élevées (article 83).

Source : RGPD ; CMA (2015[28]) ; Moazed (2019[29])

2.3.2. Portabilité des données

33. Il a été proposé de favoriser la portabilité des données en vue d'améliorer l'« autodétermination informationnelle » et d'encourager la concurrence, par exemple en facilitant le changement de prestataires (CEPD, 2013[30]). Dans les pays membres de l'OCDE, il existe un certain nombre de programmes de portabilité des données d'application facultative et nés à l'initiative des pouvoirs publics, mais aussi des droits reconnus en la matière.

34. Les initiatives « My Data », lancées en 2010 par le gouvernement américain, sont un exemple de ces programmes basés sur le volontariat. Certaines d'entre elles simplifient notamment l'accès aux informations détenues par les organismes publics (Honey, Chrousos et Black, 2016[31]). À titre d'exemple, l'initiative « *Get Transcript* » vise à améliorer l'accès aux données de l'administration fiscale (*Internal Revenue Service*), tandis que l'initiative « *My Student Data* » garantit l'accès aux données individuelles des étudiants au niveau fédéral. Il existe également d'autres initiatives dont l'objectif est de faciliter l'accès aux données détenues par des entreprises privées, comme l'initiative « *Green Button* » relative aux données des compagnies d'électricité ou l'initiative « *Blue Button* » relative aux données de santé détenues par les prestataires de soins des secteurs privé et public (United States Department of Energy, s.d.[32]).

35. Au Royaume-Uni, le gouvernement a introduit en 2011 le programme de portabilité des données *Midata*, lequel a pour objectif de donner aux consommateurs l'accès aux informations électroniques conservées par les entreprises sur leurs transactions, et ce, dans un format informatique lisible et portable (Department for Business, Innovation & Skills, 2011[33]). L'initiative *Midata* concerne les informations des consommateurs dans les secteurs financier, de l'énergie et de la téléphonie mobile. En outre, depuis janvier 2018, toutes les banques britanniques ont pour obligation de se conformer aux règles d'ouverture des banques (*Open Banking*) ayant pour objectif de simplifier la portabilité des données dans le secteur financier au Royaume-Uni (Open Banking, s.d.[34]).

36. Différents pays de l'OCDE ont par ailleurs créé des droits spécifiques en matière de portabilité des données, dont quelques exemples sont présentés dans l'Encadré 4.

Encadré 4. Droits relatifs à la portabilité des données

En 2017, le **gouvernement australien** a annoncé l'introduction d'un droit applicable aux données des consommateurs (DDC) visant à donner aux consommateurs et aux petites entreprises un accès élargi à leurs données et un contrôle renforcé sur ces dernières. L'objectif était de favoriser la concurrence en facilitant la comparaison et le changement de fournisseurs grâce à la portabilité des données. Le DDC, qui met avant tout l'accent sur l'expérience du consommateur, a pour but de transformer le paysage économique sur la durée, en simplifiant l'utilisation des données pour les nouveaux entrants dans un grand nombre de secteurs. Le DDC s'appliquera d'abord au secteur financier, puis au secteur de l'énergie. Il est ensuite proposé qu'il s'applique au secteur des télécommunication. Dans tous les cas, son introduction se fera de manière graduelle. L'*Australian Competition and Consumer Commission* (ACCC) est l'autorité réglementaire principale en charge des DDC, en collaboration avec l'*Office of the Australian Information Commissioner* (OAIC) et le *Data Standards Body* (DSB).

En **Europe**, l'article 20 du RGPD, entré en vigueur en 2018, octroie aux citoyens européens le droit de recevoir et de transmettre leurs données à caractère personnel dans un « format structuré, couramment utilisé et lisible par machine ». Ce droit s'applique à toutes les données à caractère personnel communiquées volontairement et recueillies par observation qui sont traitées par des moyens automatisés dans le cadre de l'exécution d'un contrat. L'exercice de ce droit ne doit toutefois pas porter pas atteinte aux droits et libertés d'autrui (par exemple, à la protection de la vie privée d'autres parties). Toujours en Europe, la Directive sur les services de paiements (DPS 2) exige des banques qu'elles conditionnent l'accès aux données des comptes de paiement des consommateurs par des tiers au consentement exprès des consommateurs.

Aux **États-Unis**, le *California Consumer Privacy Act* (CCPA), entré en vigueur au début de l'année 2020, regroupe sous une même loi le droit d'accès et le droit à la portabilité des données, et donne aux consommateurs la possibilité de demander aux entreprises qu'elles leur communiquent les catégories de données et les informations personnelles spécifiques recueillies à leur sujet par les entreprises concernées. Les consommateurs peuvent en outre demander aux entreprises des informations sur les finalités professionnelles et commerciales de la collecte ou de la vente des données personnelles, sur la nature des tiers avec lesquelles elles partagent des données personnelles ou auxquelles elles vendent ce type de données, ainsi que sur les catégories de données personnelles vendues ou divulguées à des fins commerciales.

Source : ACCC (s.d.[35]) ; OCDE (2019[12]) ; *Règlement général sur la protection des données (EU) 2016/679* ; *California Consumer Privacy Act* ; Takatsuki (2019[36])

3. Comment et pourquoi les entreprises recueillent et utilisent les données des consommateurs ?

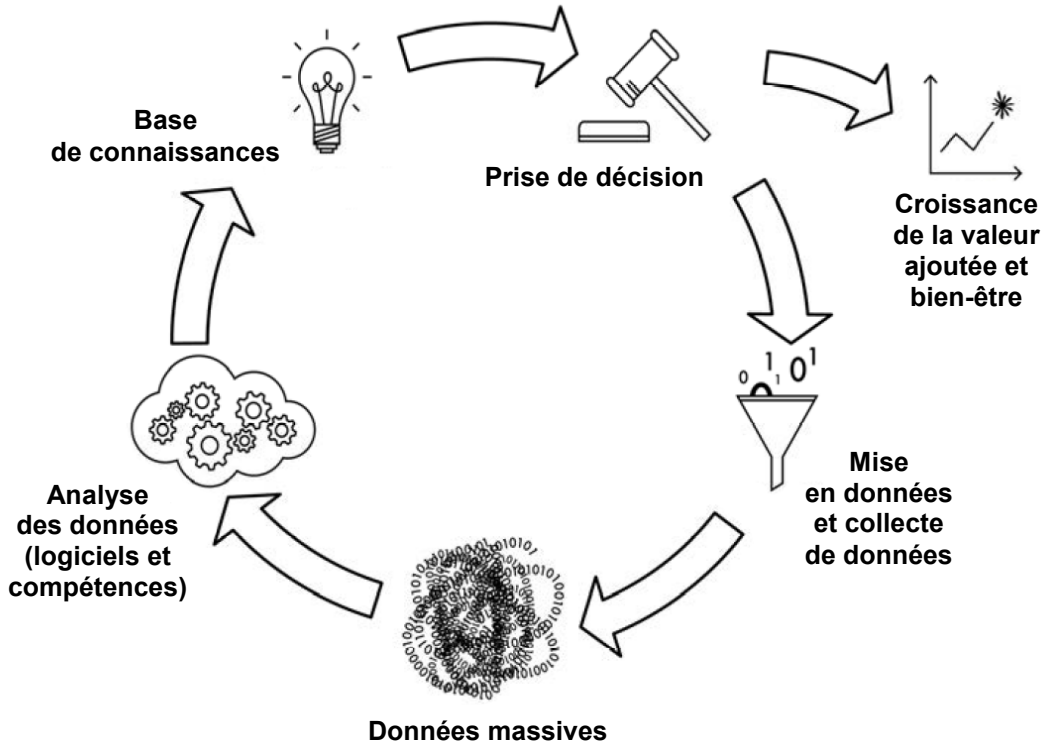
37. Cette section aborde les différentes manières dont les entreprises recueillent et utilisent les données des consommateurs. Elle présente également les raisons qui motivent des entreprises à recueillir et à partager les données des consommateurs, ainsi que les défaillances du marché potentielles associées à la collecte et à l'utilisation de ces données.

38. Le rapport de l'OCDE sur l'innovation fondée sur les données définit le cycle de valeur des données comme constitué des étapes suivantes :

- la mise en données et la collecte des données, soit la génération des données par la numérisation de contenus et la surveillance des activités, y compris d'événements et d'activités dans le monde réel (hors ligne) par le biais de capteurs (appareils IdO, par exemple) ;
- les données massives, soit le résultat de la mise en données et de la collecte des données permettant la création d'un ensemble important de données pouvant être exploitées grâce à l'analyse des données ;
- l'analyse des données, destinée à donner du sens aux données collectées. Celle-ci est de plus en plus souvent réalisée à travers des services d'infonuagique ;
- la base de connaissance, soit les connaissances accumulées sur la durée par apprentissage, que ce soit par des systèmes d'apprentissage automatique ou d'intelligence artificielle (IA) ;
- la prise de décision axée sur les données, par laquelle les décisions sont fondées sur l'utilisation des données, l'analyse des données et la base de connaissance (OCDE, 2015[3]).

39. Ces différentes étapes sont illustrées dans le Graphique 2.

Graphique 2. Cycle de valeur des données



Source : OCDE (2015[3])

40. Relativement aux effets sur la concurrence, la chaîne de production peut être réduite à : i) la génération et la collecte de données ; et ii) l'analyse et l'exploitation des données. Ces aspects sont examinés ci-dessous.

3.1. Génération et collecte de données

41. De manière générale, les données des consommateurs peuvent être considérées soit comme un produit dérivé des fonctions principales d'une entreprise, soit comme une ressource qu'une entreprise a activement cherché à obtenir en parallèle à ses fonctions principales, voire de façon totalement indépendante (Rubinfeld et Gal, 2017[37]). Autrement dit, la collecte des données peut aussi bien être une activité active que passive. Dans certains cas, cette collecte peut avoir commencé de manière passive, avant que l'entreprise ne réalise la valeur de telles données. Les entreprises de détail ont par exemple mis un certain temps à se rendre compte de la valeur des données scannées dans le cadre de leurs activités (Turow, 2017[38]). Après avoir compris leur valeur, beaucoup d'entreprises de détail ont créé de programmes de fidélité afin de recueillir d'importants volumes de données sur leurs clients (voir l'Encadré 5). De la même manière, Google n'avait à l'origine pas saisi la valeur (lucrative) des données des consommateurs recueillies dans le cadre de l'utilisation de ses moteurs de recherche, mais elles sont depuis devenues l'un de ses principaux actifs (Zuboff, 2019[39]). Dans de nombreux cas, lorsque les entreprises commencent à réaliser la valeurs des données dérivées de leurs activités, elles ont tendance à passer d'une collecte de données passive à des pratiques de collecte plus actives.

Encadré 5. Programmes de fidélité

Bon nombre d'entreprises ont mis en place des programmes de fidélité, récompensant leurs clients avec des avantages sous forme de points, de remises ou autres offres, et ce, en échange de l'adhésion ou de la participation au programme (la plupart du temps sans contrepartie financière). Les compagnies aériennes, les banques, les cinémas, les hôtels, les restaurants et les détaillants, par exemple, proposent souvent ce type de programmes. Ces programmes sont avant tout des arguments commerciaux destinés à attirer et à fidéliser les consommateurs. Les entreprises ont toutefois de plus en plus recours à ces programmes dans le but de recueillir des données sur les consommateurs, lesquelles peuvent ensuite être utilisées pour développer la perception des consommateurs et mieux cibler les annonces publicitaires. À titre d'exemple, la chaîne de supermarchés britannique Tesco recueille d'importants volumes de données grâce à son programme de carte de fidélité. Ces données représentent plus de 100 « paniers d'achat » par seconde et plus de 6 millions de transactions par jour, et ont sans doute apporté une valeur ajoutée considérable à son activité.

En 2019, l'ACCC a entrepris un examen des programmes de fidélité, lesquels posaient un certain nombre de problèmes relatifs à la politique à l'égard des consommateurs, et plus particulièrement sur la manière dont les entreprises recueillent et utilisent les données des consommateurs dans le cadre des programmes de fidélité. En vertu de sa mission de politique à l'égard des consommateurs, l'ACCC craignait ainsi que ces derniers ne disposent que d'un contrôle limité sur la manière dont les entreprises utilisent de telles données, et redoutait le manque de transparence envers les consommateurs dans la collecte et l'utilisation de leurs données. La compréhension des consommateurs des pratiques de collecte des données est abordée plus en détail dans la section 4.2.3.

Source : ACCC (2019[40]) ; OCDE (2015[3])

3.1.1. Collecte de données de première partie et collecte par des tiers

42. Lorsqu'il est question de la collecte des données des consommateurs, il est souvent utile d'observer une différence entre la collecte de données de première partie et la collecte par des tiers. On parle ainsi de collecte de données de première partie quand une entreprise recueille des informations directement auprès des consommateurs ou utilisateurs dans le cadre de l'utilisation de ses produits ou services. Par exemple, les données de première partie de Google sont les données que l'entreprise récupère auprès de ses utilisateurs lorsqu'ils utilisent son moteur de recherche, Google Photos, Gmail et tout autre service proposé ou assuré par Google. À titre de comparaison, Robertson (2020, p. 162[16]) définit le pistage par des acteurs tiers comme :

> *… une pratique permettant à un moniteur de collecter d'importants volumes de données à caractère personnel à partir d'un grand nombre de sources de première partie dans l'environnement en ligne et depuis une grande variété d'appareils différents (smartphones, tablettes, ordinateurs portables et de bureau, etc.), et ce, afin de définir à terme des profils utilisateurs complets.*

43. Pour reprendre le même exemple, outre les données que Google recueille avec ses propres sites internet et applications, l'entreprise collecte également un large éventail de données sur les consommateurs grâce au pistage par des acteurs tiers à partir d'un grand nombre d'applications et de sites internet (non détenus par Google) (Robertson, 2020[16]).

Les acteurs tiers peuvent accepter d'opérer ce type de pistage dans le cadre d'accords commerciaux afin de bénéficier, par exemple, de services de diffusion publicitaire ou d'analyses de sites internet, ainsi que d'interfaces de programmation (API) propriétaires (lesquelles sont examinées plus en détail dans la section 5.1.1). Différentes technologies facilitent par ailleurs le pistage par des acteurs tiers (voir l'Encadré 6).

Encadré 6. Technologies de pistage

Pendant longtemps, les « cookies » (sorte de code numérique enregistrant certaines actions effectuées par les utilisateurs) ont été utilisés pour suivre le comportement en ligne des utilisateurs par le biais de leurs navigateurs informatiques. Ces cookies peuvent être tiers ou de première partie. Les cookies de première partie proviennent des sites internet consultés par un consommateur (ou sont envoyés vers ces sites), alors que les cookies tiers proviennent de sites internet sans rapport avec les sites consultés (ou sont envoyés vers ces sites). Sur les appareils mobiles, les cookies ne sont toutefois pas aussi performants pour suivre les activités en ligne. Cela tient au fait que les cookies ne sont pas nécessairement partagés entre les applications mobiles et que certains navigateurs mobiles, comme Safari, bloquent par défaut les cookies tiers.

Dans la mesure où les consommateurs ont aujourd'hui tendance à utiliser plusieurs appareils différents pour accéder à des services en ligne, les entreprises ont adopté de nouvelles méthodes pour suivre les activités des consommateurs sur l'internet. On distingue ainsi deux types de méthodes, que l'on qualifie de « déterministes » et de « probabilistes ». Les méthodes déterministes s'appuient sur les caractéristiques d'identification des consommateurs, comme leurs informations de connexion, pour suivre les utilisateurs d'un appareil à l'autre. À l'inverse, les méthodes probabilistes déduisent l'identité des consommateurs à partir d'informations comme leur adresse IP (étant donné qu'un ordinateur, un smartphone et une tablette connectés à la même adresse IP publique sont susceptibles d'appartenir au même foyer), leurs informations de géolocalisation, les empreintes digitales de leurs navigateurs ou appareils, ou encore les habitudes générales d'utilisation. La Commission fédérale du commerce américaine (*Federal Trade Commission* ou FTC) a découvert que sur 100 sites internet populaires consultés sur deux appareils différents, au moins 87 sites avaient recours à un pistage multi-appareils, 96 sites permettaient aux consommateurs de saisir leur nom d'utilisateur ou leur adresse de messagerie électronique, et 16 sites partageaient leurs noms d'utilisateur ou leurs adresses de messagerie électroniques avec des acteurs tiers.

Les entreprises utilisent également de plus en plus des pixels espions pour faciliter le pistage par des acteurs tiers. Ces pixels sont de minuscules images (pratiquement invisibles) intégrant un fragment de code, lequel est exécuté dès qu'un utilisateur consulte une page internet ou ouvre un message électronique. De la même manière que les cookies, les pixels facilitent le pistage en détectant certaines actions, puis en les enregistrant dans les fichiers journaux du serveur.

Source : Beal (2008[41]) ; IAB (2013[42]) ; FTC (2017[43]) ; Boerman et al. (2017[44]) ; OCDE (2019[45]) ; Ryte (2019[46]).

44. Le pistage par des acteurs tiers est une pratique courante aussi bien sur les sites internet qu'avec les applications pour appareils mobiles. En 2018, 95 % des 10 000 sites internet les plus populaires et plus de 90 % des applications gratuites proposées par la boutique Google Play intégraient au moins un agent de pistage tiers (Binns et al., 2018[47] ; Purra et Carlsson, 2016[48]). Cependant, bien que de nombreux acteurs s'adonnent à des

pratiques de pistage, *« la majorité de ces agents restent contrôlés par un petit nombre de poids lourds de l'industrie des données »* (Ezrachi et Roberston, 2019[49]). Alphabet/Google arrive en tête à la fois pour les applications et pour les sites internet. Facebook et Twitter sont également bien positionnés pour les sites internet et les applications, même si Microsoft (LinkedIn inclus) arrive en deuxième place pour les applications (Binns et al., 2018[47] ; Purra et Carlsson, 2016[48]). Par ailleurs, environ 18 % des applications gratuites proposées dans la boutique Google Play comprenaient plus de vingt agents de pistage différents (Binns et al., 2018[47]).

45. Comme mentionné précédemment, la manière dont les données des consommateurs sont recueillies a une incidence non négligeable en termes de concurrence et de protection de la vie privée. Cela s'applique non seulement à la manière dont les consommateurs fournissent leurs données (ou dont les entreprises créent les données), mais aussi à qui les consommateurs les fournissent. En termes de protection de la vie privée, la conscience qu'ont les consommateurs des pratiques de collecte a une incidence sur leur capacité à contrôler leurs données à caractère personnel. Plus précisément, les consommateurs auraient tendance à accepter plus facilement que des données qu'ils ont communiquées volontairement soient collectées et utilisées directement par des premières parties. La situation serait d'ailleurs relativement identique dans le cas des données recueillies par observation par des premières parties. Les consommateurs peuvent toutefois avoir moins conscience des données collectées via des pratiques de pistage par des acteurs tiers, même lorsqu'ils fournissent ces données de façon volontaire ou lorsqu'ils savent que leurs données sont scrutées par les entreprises (de première partie) concernées. Les consommateurs peuvent en effet accepter de fournir des informations dans un contexte spécifique, alors que ces informations seront par la suite utilisées dans un autre contexte qui aurait suscité un refus de leur part s'ils avaient pleinement eu conscience de cette nouvelle utilisation. Ce comportement tient au fait que la valeur des consommateurs, selon qu'ils partagent ou protègent leurs informations personnelles, dépend énormément du contexte (Acquisti, Taylor et Wagman, 2016[15]). Ces problématiques ont également un intérêt du point de vue de la concurrence : si les consommateurs ne comprennent pas la manière dont leurs données sont recueillies et exploitées, ils seront moins susceptibles de pouvoir stimuler une saine concurrence par rapport à ces pratiques (voir également la section 4.2.3).

46. La capacité d'une entreprise à recréer des données de consommateurs comparables à celles détenues par des concurrents, ou même à accéder à des données comparables, est également un facteur important à prendre en compte dans un certain nombre de scénarios, notamment lorsqu'il s'agit de déterminer si une entreprise se trouve en position dominante ou si l'accès aux données d'un concurrent peut être une condition préalable à une saine concurrence (voir également la section 4.2.2). Même dans les cas où certaines données des consommateurs sont collectées facilement, de différentes manières et par différentes parties, l'accès à des techniques de pistage par des acteurs tiers, ainsi qu'à une importante base de consommateurs identifiables, peut fournir à une entreprise un ensemble de données extrêmement précieux et particulièrement difficile à reproduire pour ses concurrents. Binns et Bietti (2019[50]) considèrent que, dans les affaires de concurrence et notamment dans le cas de fusions entre entreprises s'adonnant au pistage par des acteurs tiers, cette pratique ne fait pas l'objet d'une attention suffisante. Cette problématique est abordée de façon plus approfondie dans la section 4.

3.1.2. Stockage

47. Les décisions des entreprises relatives aux modalités et à l'emplacement de stockage des données ont également une incidence sur la protection de la vie privée et la

bonne marche de la concurrence. À titre d'exemple, la décision de conserver des données à caractère personnel recueillies depuis des appareil IdO directement sur ces appareils ou de manière externe (p. ex. du côté du fabricant ou dans le nuage) aura nécessairement un impact sur la concurrence et sur la protection de la vie privée. Les données enregistrées localement sur les dispositifs des consommateurs, et qui ne sont accessibles par aucune autre partie sans leur consentement exprès, sont moins susceptibles de susciter des préoccupations en termes de protection de la vie privée. Toutefois, les retombées sociales plus générales qui pourraient découler de l'analyse et de l'exploitation de ces données risqueraient de ne jamais se concrétiser, y compris la concurrence favorisée par une utilisation plus large de ces informations (p. ex. : la concurrence dans les offres de prêt à partir des informations connues sur la cote de solvabilité des consommateurs). À l'inverse, les données détenues par les fabricants ou conservées dans le nuage sont quant à elles plus susceptibles de soulever des préoccupations en termes de protection de la vie privée. Par ailleurs, si les entreprises ne partagent pas leurs données plus largement, il existe un risque que les retombées sociales qui pourraient découler de leur utilisation généralisée s'en trouvent encore une fois limitées. Cette problématique est abordée dans l'Encadré 7 avec l'exemple des véhicules connectés.

Encadré 7. Gouvernance des données dans les véhicules connectés

Les véhicules autonomes et connectés génèrent différents types de données, parmi lesquels des données techniques, météorologiques et de circulation routière, mais aussi relatives au comportement au volant, à la géolocalisation et aux préférences des conducteurs en matière de navigation et de divertissement, par exemple. La connectivité des véhicules fait que ces données peuvent être communiquées en temps réel à des entités extérieures. Ces données sont particulièrement utiles non seulement pour les constructeurs, mais aussi pour les fournisseurs de services complémentaires et après-vente (services de navigation, de divertissement ou d'assurance, par exemple).

Les véhicules autonomes et connectés peuvent également être source de nombreux avantages pour les consommateurs et pour la société dans son ensemble. La réalisation de ces avantages est toutefois conditionnée à la mise en place de mécanismes appropriés de gouvernance des données visant à gérer l'accès aux données embarquées dans les véhicules et leur contrôle (y compris les données des consommateurs). La question des meilleurs moyens d'y parvenir demeure toutefois sujette à débat. Comme indiqué par Kerber (2019[51]), les constructeurs de véhicules cherchent à promouvoir le concept de « véhicule étendu », lequel repose sur le transfert de l'ensemble des données du véhicule aux équipementiers d'origine pour leur utilisation exclusive. À l'inverse, les prestataires de services indépendants plaident pour un accès non discriminatoire aux données par le biais d'une solution de « serveur partagé » ou à plus long terme au développement d'une « plateforme d'applications embarquée ». Cette plateforme permettrait aux consommateurs de décider de l'emplacement de stockage de leurs données et à qui ils en autorisent l'accès.

Ces solutions ont des incidences très différentes du point de vue de la concurrence. En théorie, la concurrence entre équipementiers devrait permettre de stimuler la concurrence dans les services après-vente. Kerber (2019[51]) précise toutefois qu'en pratique les consommateurs ont tendance à ne pas prendre en compte les services après-vente dans leur décision d'achat de véhicules. Il indique par ailleurs que la concurrence entre équipementiers n'est pas suffisante pour résoudre les défaillances du marché associées à la sélection des technologies optimales en vue de parvenir à l'interopérabilité

et à l'adoption de normes techniques. Il est donc peu probable que le concept de « véhicule étendu » encourage réellement la concurrence dans les marchés des services complémentaires et après-vente. Par opposition, les solutions proposées par les prestataires de services indépendants ont plus de chances de favoriser la concurrence dans les marchés connexes, même si, dans la mesure où les équipementiers conservent le contrôle de l'accès dans le cadre de la solution du « serveur partagé », ils auraient la capacité de bloquer l'accès à des concurrents potentiels, ce qui aurait des répercussions sur la concurrence.

Les équipementiers défendent leur position sur la base de considérations de sécurité et sûreté. Les recherches de Kerber (2019[51]) suggèrent néanmoins que cela ne peut justifier de laisser le contrôle exclusif des données aux équipementiers. Dans l'ensemble, Kerber (2019[51]) considère que malgré les avantages et inconvénients évidents de chaque solution, celle de la « plateforme d'applications embarquée » présente les avantages potentiels les plus importants. Cette solution semble en effet permettre à la fois aux consommateurs de contrôler leurs données et de protéger leur vie privée, mais aussi de favoriser la concurrence.

Source : Kerber (2019[51])

3.2. Analyse et utilisation

48. La baisse des coûts associés au traitement et au stockage des données a permis l'apparition de solutions d'analyse plus performantes et abordables, notamment grâce à l'infonuagique (OCDE, 2015[3]). Les entreprises utilisent les données des consommateurs à des fins très diverses, y compris en interne pour :

- améliorer la qualité ou les fonctionnalités de leurs produits ou services principaux ;
- permettre une personnalisation renforcée (dont, éventuellement, la personnalisation des prix ou des offres) ;
- entraîner les systèmes d'apprentissage automatique et autres systèmes d'analyse à l'appui de l'IA (voir l'Encadré 8) ;
- vendre des produits publicitaires et autres services ciblés, impliquant généralement des marchés bifaces ou multifaces.

49. Les entreprises peuvent également vendre les données des consommateurs à des acteurs tiers (sous réserve d'anonymisation ou de consentement des consommateurs en fonction du régime réglementaire adopté) (Gilbert et Pepper, 2015[52]). Les marchés des données des consommateurs et des rapports sur les consommateurs sont apparus il y a quelque temps déjà. Ces marchés sont toutefois complexes, tendent à être décentralisés, couvrent de nombreux modèles économiques et rassemblent un grand nombre d'acteurs différents (CMA, 2015[28]).

50. En raison de leurs utilisations très variées, les données des consommateurs peuvent avoir une valeur économique non négligeable, ce qui peut encourager les entreprises à en collecter les plus grands volumes possibles. Comme le décrit Kemp (2019, p. 10[17]) :

> *Les prestataires ont été incités à « tout mesurer », afin d'établir des profils sur leurs clients, de cibler les campagnes de commercialisation, de personnaliser leurs offres, d'opérer une discrimination par les prix, de mieux analyser les risques et d'appuyer d'autres applications éventuelles de l'intelligence artificielle dans leurs entreprises. Dans cette optique, les entreprises ont tout intérêt à disposer de*

toujours plus de données. L'apprentissage automatique est une technologie qui nécessite de grandes quantités de données. Les concurrents bénéficient ainsi de millions d'« indications » sur les consommateurs présents sur leur marché d'origine, mais aussi de possibilités de développement dans d'autres marchés.

Encadré 8. Intelligence artificielle et apprentissage automatique

D'après les Principes de l'OCDE sur l'IA :

> *Un système d'intelligence artificielle est un système automatisé qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure d'établir des prévisions, de formuler des recommandations, ou de prendre des décisions influant sur des environnements réels ou virtuels. Les systèmes d'IA sont conçus pour fonctionner à des degrés d'autonomie divers.*

Autrement dit, l'IA est une science consacrée à la reproduction des capacités humaines par des machines, appuyée par des systèmes d'IA. Ces systèmes peuvent ensuite utiliser différentes méthodes pour mettre en œuvre cette IA. L'apprentissage automatique, qui fait partie de ces méthodes, « *exploite des techniques des réseaux de neurones, des statistiques, de la recherche opérationnelle et des sciences physiques pour induire des informations cachées à partir de données, sans que soit expressément programmé l'emplacement où chercher ou le résultat escompté* ». Il existe d'autres méthodes contribuant à l'enrichissement de l'IA, par exemple :

- les réseaux de neurones, qui sont une variante de l'apprentissage automatique inspirée du cerveau humain ;
- l'apprentissage profond, qui exploite des réseaux de neurones sur plusieurs couches afin de détecter des formes complexes dans des volumes importants de données ;
- la vision artificielle, qui s'appuie sur la reconnaissance des formes et l'apprentissage profond pour identifier le contenu d'une image ou d'une séquence vidéo ;
- le traitement automatique du langage naturel, qui correspond à la capacité des ordinateurs à analyser, comprendre et reproduire le langage humain, et ce, grâce à l'apprentissage profond.

Source : OCDE (2019[53]) ; Thomson, Li et Bolen (s.d.[54]) ; Marr (2016[55])

51. Par ailleurs, le fait que les entreprises n'aient pas toujours conscience des avantages potentiels des données des consommateurs et des utilisations qu'elles peuvent en faire au moment de la collecte de ces données a une incidence non négligeable sur les évaluations d'impact sur la concurrence, y compris mais sans s'y limiter, sur la définition du marché (Maggiolino et Ferrari, 2020[56]). Cette problématique est abordée plus en détail dans la section 4.2.

52. Il semble également exister une boucle de rétroaction entre les capacités à recueillir des données des consommateurs, accélérer l'apprentissage et améliorer les algorithmes, renforcer la qualité des biens et services, attirer davantage de consommateurs, et recueillir encore plus de données des consommateurs (Gal et Rubinfeld, 2019[26] ; Pecman, Johnson et Reisler, 2020[57]). Tel que précisé par l'ACCC dans son étude sur les plateformes numériques (*Digital Platforms Inquiry*) (ACCC, 2019, p. 7[58]) :

Le modèle économique fondamental de Google et Facebook est d'attirer le plus grand nombre d'utilisateurs possible, et d'obtenir ainsi des ensembles de données abondantes sur leurs utilisateurs. L'omniprésence de ces plateformes et leur présence dans les marchés connexes leur permet de constituer des ensembles de données extrêmement précieux. Elles sont ainsi en mesure de proposer aux annonceurs des opportunités de campagnes publicitaires hautement ciblées et personnalisées.

Les recettes publicitaires qui en découlent peuvent ensuite être investies dans les fonctionnalités et services qu'elles proposent, améliorant ainsi l'expérience du consommateur et attirant toujours plus d'utilisateurs, et ce, tout en renforçant leurs techniques de collecte de données.

53. Naturellement, l'utilisation et l'analyse des données des consommateurs ont un coût. Elles génèrent notamment des dépenses informatiques, mais aussi de personnel dédié. Bon nombre d'observateurs ont avancé que la valeur des données des consommateurs ne réside pas dans les données elles-mêmes, mais dans leur intégration à des bases de données exploitables et dans l'application d'algorithmes et autres techniques d'analyse pour en extraire des indications sur les consommateurs (Körber, 2018[59]). Lambrecht et Tucker (2017[60]) considèrent que c'est l'accès à une main-d'œuvre qualifiée, plutôt qu'à des données brutes (dont elles ont déterminé que ces données pouvaient généralement être reproduites facilement), qui donne aux entreprises un avantage concurrentiel dans l'économie numérique. Il s'agit ainsi d'un facteur à prendre en compte pour déterminer si l'accès à des données des consommateurs ou leur détention confère un pouvoir de marché, tel qu'abordé ci-après dans la section 4.2.2.

3.2.1. Incitations au partage de données

54. La décision des entreprises de partager ou non des données a également une incidence sur la concurrence dans les marchés concernés. Il est donc utile d'examiner les incitations que peuvent avoir les entreprises à partager leurs données.

55. Sur cette question, Engles (2016, p. 5[61]) indique que ce qui motive le partage de données peut dépendre de la finalité pour laquelle une entreprise demande ces données. Par exemple, si les données sont demandées dans le but de développer un bien ou service concurrent, l'entreprise sollicitée peut être moins encline à les partager. Toutefois, si les données sont demandées dans le but de développer un bien ou service complémentaire, leur partage peut être dans l'intérêt de l'entreprise sollicitée. Une évaluation des effets sur la concurrence d'un partage obligatoire de telles données devra vraisemblablement se faire au cas par cas et prendre en compte non seulement les avantages d'une utilisation plus générale des données, mais aussi de l'impact des incitations à l'investissement dans la collecte de telles données. Cet aspect est abordé de façon plus approfondie dans les sections 4.3 et 4.4.

56. En pratique, de nombreuses entreprises ont développé des API qui facilitent l'interopérabilité des données, tout en leur permettant de garder le contrôle de l'accès aux données et de la manière dont elles sont utilisées (voir la section 5.1.1).

3.3. Avantages et risques potentiels pour les consommateurs

57. La collecte et l'utilisation de données des consommateurs par les entreprises génèrent de nombreux avantages et risques potentiels pour les consommateurs.

3.3.1. Avantages

58. La *Competition and Markets Authority* (CMA) du Royaume-Uni (2015[28]) identifie les avantages potentiels suivants comme découlant de la collecte des données des consommateurs par les entreprises :

- la capacité d'augmenter les ventes grâce à des annonces ciblées, lesquelles peuvent également réduire les coûts et permettre le développement d'offres ciblées pour les consommateurs ;
- une meilleure analyse des profils de consommateurs à l'appui des opérations de commercialisation et de l'évaluation des risques (p. ex. dans les marchés des services financiers) ;
- la personnalisation des produits et services ;
- l'amélioration et le développement de produits ;
- l'amélioration des processus d'entreprise ;
- le financement de services proposés gratuitement.

3.3.2. Risques

59. Les atteintes à la protection de la vie privée, mais aussi la collecte et l'utilisation des données des consommateurs, peuvent entraîner des préjudices matériels et moraux pour les consommateurs. Comme le décrit Kemp (2019, p. 19[17]) :

> *Plus le volume d'informations personnelles collectées et enregistrées est important, plus elles sont diffusées largement et plus elles sont conservées pendant une période prolongée, plus la probabilité qu'elles soient piratées, divulguées de façon accidentelle ou utilisées à des fins illégales est importante.*

60. L'un des principaux risques réside dans le fait que les données d'un consommateur soient utilisées pour usurper son identité, ce qui pourrait avoir de graves conséquences pour la personne concernée (Anderson, 2019[62] ; Acquisti, Taylor et Wagman, 2016[15] ; CMA, 2015[28]). Les consommateurs peuvent par ailleurs subir des pertes de données, voir leurs données recueillies, exploitées ou partagées de façon inattendue ou non approuvée, ou encore faire l'objet de sollicitations intempestives (CMA, 2015[28]). Même lorsque les consommateurs ont volontairement communiqué leurs informations dans un contexte spécifique, il existe un risque que les entreprises exploitent ces données dans un autre contexte, voire qu'ils les partagent. Cet aspect est particulièrement problématique dans la mesure où les avantages pour les consommateurs découlant du partage et de la protection des informations personnelles dépendent en grande partie du contexte (Acquisti, Taylor et Wagman, 2016[15]). Le fait que la plupart des données anonymisées des consommateurs puissent techniquement être réidentifiées pose également des difficultés dans ce contexte (PCAST, 2013[24]).

61. Ensuite, les entreprises pourraient utiliser les données des consommateurs pour opérer une discrimination à leur encontre, les manipuler ou les exclure de certains marchés ou de l'accès à certains produits (CMA, 2015[28] ; OCDE, 2016[4] ; OCDE, 2018[7]). Une collecte et une utilisation plus généralisées des données à caractère personnel pourraient en effet permettre aux entreprises de personnaliser plus facilement les prix et les types de produits proposés à leurs clients, ou d'exclure plus facilement certains consommateurs d'offres spécifiques. Tel qu'abordé dans le rapport de 2018 de l'OCDE sur « La personnalisation des prix à l'ère numérique », cette pratique entraîne généralement des gains d'efficience et profite souvent aux consommateurs, dans la mesure où elle encourage

les entreprises à innover et à se livrer une concurrence plus intense à la conquête de chaque client (OCDE, 2018[7]). Dans certains cas toutefois, la personnalisation des prix peut avoir une incidence préjudiciable pour les consommateurs si elle est mise en œuvre par des entreprises disposant d'un fort pouvoir de marché (OCDE, 2018[7]). Les consommateurs ont malgré tout tendance à avoir une perception négative de la personnalisation des prix, principalement car ils trouvent cette pratique injuste. D'aucuns s'inquiètent également de la capacité des entreprises à recourir au profilage et au micro-ciblage pour tirer parti des faiblesses des consommateurs, y compris de leurs biais comportementaux et de leurs dépendances (Calo, 2013[63] ; Calo et Rosenblat, 2017[64] ; Zuboff, 2019[39]).

62. Cohen (2013[65]) souligne également l'importance de la protection de la vie privée et de la liberté de n'être soumis à aucune surveillance, d'une part, pour garantir une citoyenneté « informée et réfléchie » et, d'autre part, pour renforcer la capacité d'innovation. Tout affaiblissement de la protection de la vie privée pourrait également affecter la confiance des consommateurs dans les marchés, et entraîner ainsi un engagement moindre des consommateurs, associé une forte augmentation des coûts. L'utilisation des données des consommateurs par les entreprises peut par ailleurs poser des risques sociaux plus sérieux, dont éventuellement *« une manipulation des dépêches d'information et des résultats de recherche, l'émergence de chambres d'écho et, plus largement, le marché des idées »* (Ezrachi et Roberston, 2019, p. 6[49]). Certains ont également exprimé leurs inquiétudes quant à la capacité d'une utilisation généralisée des données des consommateurs et de la publicité en ligne à favoriser la diffusion d'informations de propagande et à influencer les processus démographiques (Stucke, 2018[66]). Si un nombre relativement faible d'entreprises détiennent la majorité des données des consommateurs, tout en étant concurrentes pour les marchés publics, il existe un risque que celles-ci finissent par devenir dépendantes des gouvernements, ce qui pourrait alors faciliter une surveillance généralisée par les États (Stucke, 2018[66]).

3.4. Défaillances du marché

63. Différentes défaillances du marché peuvent être associées à la collecte et à l'utilisation des données des consommateurs, parmi lesquelles i) l'asymétrie de l'information ; ii) les externalités ; et iii) un possible manque de concurrence. Ces trois types de défaillances du marché sont abordés de façon plus approfondie ci-dessous.

3.4.1. Asymétrie de l'information

64. Un phénomène d'asymétrie de l'information peut se produire lorsqu'il existe un déséquilibre entre les vendeurs et les acheteurs, lequel est susceptible de conduire à une inefficacité des marchés. Ainsi, si les consommateurs ne peuvent vérifier les informations avant de procéder à un achat, des problèmes d'« antisélection » ou de « tacots »[2] peuvent apparaître, auquel cas des biens de qualité supérieure (p. ex. : des biens et services plus protecteurs pour la vie privée des consommateurs) finissent par être écartés du marché (Akerlof, 1970[67]). Une réaction réglementaire courante à l'asymétrie de l'information consiste à exiger des entreprises qu'elles publient certaines informations afin de permettre aux consommateurs de prendre des décisions plus éclairées, et ainsi de stimuler une saine concurrence. Par ailleurs, les législations en matière de consommation intègrent souvent des dispositions de protection à l'encontre de pratiques trompeuses des entreprises (voir également la section 5.2). L'efficacité des dispositions, en ce sens qu'elles prennent en compte la capacité des consommateurs à réellement considérer la protection de la vie privée comme un facteur essentiel de la qualité d'un bien ou service, peut présenter un intérêt dans

[2] Le terme « tacot » désigne des biens immobilisés qui se révèlent défectueux après l'achat.

le cadre des évaluations d'impact sur la concurrence, tel que décrit plus en détail dans la section 4.2.3.

3.4.2. Externalités et non-rivalité

65. Les données des consommateurs sont des biens non rivaux (Acquisti, Taylor et Wagman, 2016[15]). Autrement dit, leur utilisation pour une finalité spécifique n'altère en rien leur capacité à être utilisées à d'autres fins, à l'inverse des biens rivaux, tels que l'essence qui perd toute valeur dès lors qu'elle a été extraite et consommée (OCDE, 2019[12]). Il a également été avancé qu'une fois partagées les données des consommateurs pouvaient être considérées comme non exclusives, en cela que les entreprises peuvent éprouver des difficultés à exclure certaines données des consommateurs d'une potentielle utilisation par d'autres acteurs du marché (voir, par exemple, Acquisti, Taylor et Wagman (2016[15])). Cela ne semble toutefois pas être une règle absolue, tel que décrit de manière plus approfondie dans la section 4.2.2.

66. Par ailleurs, comme le soulignent Acquisti et al. (2016, p. 445[15]), *« des externalités aussi bien positives que négatives découlent de l'interaction complexe qui existe entre la création et la transmission de données »*. Ces externalités positives et négatives tiennent au fait que les données d'un consommateur peuvent être utilisées pour déduire des informations sur les autres consommateurs à l'aide d'algorithmes et de systèmes d'apprentissage automatique et d'IA. Ces techniques permettent d'obtenir des indications sur les consommateurs même lorsqu'ils veillent à ne pas révéler ces informations. Par exemple, si une entreprise détient certaines informations sur un consommateur, elle peut être en mesure de catégoriser ce consommateur afin de déduire d'autres données à son sujet sur la base de ce qu'elle sait plus généralement sur le type de consommateur auquel il correspond. La capacité à combiner des données sur plusieurs individus, afin de créer un ensemble de données massives à partir duquel il est possible d'extraire des inférences utiles sur les individus ou la société dans son ensemble, peut avoir des incidences positives comme négatives, aussi bien pour les personnes qui ont fourni des données que pour la société tout entière, suivant l'utilisation qui est faite de ces données. Par exemple, l'utilisation d'un ensemble de données combinées par une entreprise dans le but de prédire l'état du trafic ou d'améliorer les résultats pourrait générer des externalités positives. À l'inverse, l'exploitation par une entreprise d'un ensemble de données des consommateurs dans le but de cibler ou de discriminer des personnes à un niveau individuel (dans le cas où celles-ci ont refusé de dévoiler des informations spécifiques qui ont pu être déduites par inférence à partir de données d'autres consommateurs) pourrait entraîner des externalités négatives (Gal et Rubinfeld, 2019[26]). Compte tenu de ces externalités, il n'est pas étonnant qu'Acquisti et al. (2016[15]) estiment que les répercussions économiques d'une baisse de la protection de la vie privée et d'un renforcement du partage des informations puissent aussi bien être favorables que défavorables au bien-être des consommateurs et de la société au sens large.

67. L'existence d'externalités peut laisser penser que les données des consommateurs sont recueillies et échangées à des niveaux inférieurs à ce qu'ils devraient être pour réellement permettre une optimisation du bien-être. Choi, Jeon et Kim (2019[68]) montrent par exemple que si les externalités négatives liées à la collecte et à l'utilisation de données dépassent les externalités positives, les entreprises auront tendance à collecter des données à un niveau supérieur au niveau socialement optimal, même si les consommateurs sont pleinement informés et que leur consentement est acquis.

3.4.3. Concurrence imparfaite

68. D'autres universitaires considèrent qu'un défaut de protection de la vie privée dans certains marchés peut être une conséquence de l'existence d'un pouvoir de marché. Robertson (2020, p. 165[16]) indique ainsi que *« les consommateurs ont rarement leur mot à dire en matière de protection de la vie privée en tant que composante de la qualité d'un produit en ligne, dans la mesure où ils n'ont généralement pas la possibilité d'éviter certains fournisseurs de services numériques de premier plan »*. Si l'on considère que les fusions, les pratiques et les accords anticoncurrentiels entraînent des niveaux sous-optimaux de protection des données et de la vie privée, alors la politique de la concurrence et son application peuvent avoir un rôle important à jouer. Il en va de même pour la concurrence (et éventuellement d'autres domaines de l'action publique), qui peut permettre d'agir sur les facteurs liés à la demande, comme les obstacles comportementaux au changement de prestataires, l'asymétrie de l'information ou les effets de réseau. Ces questions sont abordées plus en détail dans la section 4 ci-dessous.

4. Rôle de l'application du droit de la concurrence

69. Bien que les entreprises recueillent et utilisent les données des consommateurs depuis longtemps, ces pratiques ont connu un essor exponentiel au cours des dernières années, et constituent même l'activité principale de nombreuses entreprises. Dans ce contexte, les données des consommateurs présentent un intérêt croissant pour les évaluations d'impact sur la concurrence. Cela peut se manifester principalement sous deux formes : i) la protection des données et de la vie privée peuvent constituer un aspect de la qualité sur lequel les entreprises sont en concurrence ; et ii) la collecte et la détention de données des consommateurs (et l'accès à ces informations) peuvent avoir une incidence sur la concurrence.

70. Au fil du temps, les appels visant à accorder une importance plus grande aux enjeux de la protection des données et de la vie privée dans les évaluations d'impact sur la concurrence se sont multipliés. En 2014, le Contrôleur européen de la protection des données (CEPD) a préconisé une approche plus coordonnée de la protection des données dans son avis préliminaire intitulé « Vie privée et compétitivité à l'ère de la collecte de données massives : l'interaction entre le droit à la protection des données, le droit de la concurrence et la protection des consommateurs dans l'économie numérique » (CEPD, 2013[30]). Il y soulignait notamment certains problèmes associés aux marchés sans contrepartie financière, dans lesquels les consommateurs « paient » avec leurs données, ainsi qu'aux incidences de la protection de la vie privée sur le bien-être du consommateur. Il estimait par ailleurs qu'en ignorant les répercussions de la combinaison des données des consommateurs dans le cadre de la fusion *Google/DoubleClick* (abordée plus en détail dans la section 4.1.1), la Commission européenne (CE) :

> *… n'avait […] pas tenu compte de l'impact à plus long terme sur le bien-être de millions d'utilisateurs dans l'éventualité où les informations de l'entreprise issue de la fusion générées par la recherche (Google) et la navigation (DoubleClick) feraient l'objet d'un traitement ultérieur à des fins incompatibles. (CEPD, 2013, p. 30[30])*

71. De la même manière, en 2015, la CMA a publié un rapport sur l'utilisation commerciale des données des consommateurs, lequel examinait certaines des interactions qui existent entre la concurrence et l'application de la législation sur la protection de la vie privée, y compris les obstacles potentiels liés à la demande qui nuisent à une meilleure efficacité de la protection de la vie privée (CMA, 2015[28]). Ces problématiques ont

également été abordées dans le rapport de l'OCDE sur les données massives publié en 2016 (OCDE, 2016[4]). La même année, un rapport conjoint établi par les autorités de la concurrence allemande et française abordait également les interactions entre le droit de la concurrence et les données. Bien qu'il indiquât que les problèmes de protection de la vie privée n'entraient pas *« dans le champ d'action des autorités de la concurrence »*, il précisait également que (Bundeskartellamt et Autorité de la concurrence, 2016, pp. 22-24[69]) :

> *… les politiques de protection de la vie privée pourraient être examinées sous l'angle de la concurrence lorsque celles-ci sont susceptibles d'avoir une incidence sur les conditions de concurrence, notamment dans les cas où elles sont mises en œuvre par une entreprise dominante qui exploite les données comme principale ressource pour ses produits ou services.*

72. La protection de la vie privée en tant qu'aspect de la concurrence a aussi été traitée dans le rapport de 2018 de l'OCDE sur la « Problématique de la qualité dans les secteurs numériques de l'économie sans contrepartie financière » (OCDE, 2018[6]). Et en 2019, le rapport Furman du Royaume-Uni consacré à la libération de la concurrence sur les marchés du numérique établissait que *« les utilisations abusives de données des consommateurs et les atteintes à la protection de la vie privée peuvent être considérées comme des indicateurs d'une mauvaise qualité provoquée par un manque de concurrence »* (Furman et al., 2019, p. 43[70]).

73. Il subsiste toutefois certaines situations dans lesquelles les problèmes liés aux droits relatifs aux données des consommateurs ont été acceptés comme tels ou s'avèrent déterminants. Ces cas sont abordés plus en détail ci-dessous. On observe néanmoins que ces problématiques sont de plus en plus considérées comme présentant un intérêt dans le cadre des évaluations d'impact sur la concurrence (OCDE, 2016[4] ; OCDE, 2018[6] ; OCDE, 2018[5] ; Robertson, 2020[16] ; Kemp, 2019[17]). Cette section examine le rôle de l'application du droit de la concurrence par rapport aux droits relatifs aux données des consommateurs, et aborde en premier lieu les théories du préjudice potentielles. Ensuite, elle traite des questions analytiques, comme la définition du marché, les obstacles à l'entrée, l'attitude des consommateurs à l'égard de la protection de la vie privée, les méthodes d'évaluation des niveaux de protection des données et de la vie privée, et les possibles gains d'efficience. Cette section d'intéresse enfin aux mesures correctrices potentielles et au possible rôle de la théorie des installations essentielles.

4.1. Théories du préjudice

74. Différentes théories du préjudice peuvent être associées aux données des consommateurs et aux droits relatifs aux données des consommateurs, comme présenté ci-dessous. Celles-ci ont trait aux fusions, à l'abus de position dominante et aux affaires d'entente.

4.1.1. Fusions

75. Les fusions unissant des entreprises qui exploitent des données de consommateurs pourraient avoir des effets négatifs sur la concurrence, et ce, par deux biais différents : i) en entraînant une baisse de la qualité de la protection des données et de la vie privée proposée sur les marchés concernés ; et ii) en dressant des obstacles à l'entrée ou en augmentant les coûts des concurrents par la combinaison des données de consommateurs détenues par les entreprises parties à la fusion.

76. Les inquiétudes sur la capacité des fusions à limiter la concurrence relativement à la collecte et à l'utilisation des données des consommateurs pourraient s'avérer

particulièrement justifiées dans les marchés sans contrepartie financière, où la concurrence s'exerce plus largement sur des éléments de qualité plutôt que sur les prix (OCDE, 2018[6]). Gilbert et Pepper (2015, p. 5[52]) suggèrent par ailleurs que : « *La disparition d'un « franc-tireur » important ayant développé des systèmes innovants de contrôle et de protection des données serait susceptible de poser des problèmes de concurrence en limitant l'innovation dans la protection des données, même si les parties à la fusion n'étaient auparavant pas en concurrence directe.* » Condorelli et Padilla (2019[71]) défendent également une stratégie d'enveloppement de « liaison des politiques de protection de la vie privée », laquelle pourrait permettre d'augmenter le volume des données des consommateurs recueillies dans le cadre d'une fusion conglomérale. Selon cette théorie, une entreprise dominante pourrait acquérir un consentement général de ses utilisateurs, lui permettant d'utiliser ce consentement dans les nouveaux marchés auxquels elle accède suite à une fusion, dans les cas où les mêmes consommateurs sont présents sur les deux marchés. Cette théorie du préjudice est abordée plus en détail dans une note de référence de l'OCDE consacrée aux effets congloméraux des fusions (OCDE, 2020[10]).

77. La protection de la vie privée semble de plus en plus considérée comme présentant un intérêt pour les évaluations de fusions, dans la mesure où elle constitue un aspect de la qualité qui importe aux consommateurs, et donc sur lequel les entreprises rivalisent. Il apparaît toutefois qu'aucune fusion n'ait jusqu'alors été empêchée par les autorités de la concurrence sur la seule base de préoccupations de cet ordre, tel que décrit ci-après.

78. Les fusions pourraient par ailleurs avoir des effets anticoncurrentiels dans les cas où la combinaison des données des consommateurs détenues par les parties aux fusions est susceptible de créer des obstacles à l'entrée ou d'augmenter les coûts pour les concurrents. Une mesure correctrice possible pourrait alors consister à exiger de l'entreprise issue de la fusion qu'elle permette l'accès à son ensemble de données combinées. En pratique, de nombreuses fusions ont été bloquées, ou autorisées sous condition, au motif qu'elles soulevaient des inquiétudes relatives aux potentiels effets anticoncurrentiels des ensembles de données des consommateurs détenus par les entreprises issues de fusion dans les marchés concernés. Différents exemples sont présentés ci-après.

79. Certaines fusions peuvent d'ailleurs être motivées par le souhait d'accéder aux ensembles de données d'une entreprise concurrente. Il s'agit en effet d'une motivation sous-jacente dans nombre d'acquisitions anticoncurrentielles et d'acquisitions d'entreprises naissantes, par exemple. Les problèmes liés aux acquisitions anticoncurrentielles et d'entreprises naissantes, y compris mais sans s'y limiter aux seuils de notification préalable à une fusion, seront abordés à l'occasion d'une table ronde dédiée, prévue pour juin 2020, axée sur les start-ups, les acquisitions anticoncurrentielles et les seuils de contrôle des fusions (OCDE, 2020[9]).

Affaires pertinentes

80. Dans son évaluation de la fusion *Google/DoubleClick* en 2008, la Commission européenne a considéré que les considérations de protection de la vie privée relevaient de la législation sur la protection des données, conformément à la jurisprudence établie par l'affaire *Asnef-Equifax* (voir la section suivante). La fusion *Google/DoubleClick* impliquait deux parties ayant la capacité de recueillir et d'exploiter des volumes très importants de données des consommateurs : Google, par le biais de ses services de recherche en ligne, et DoubleClick, par le biais de ses services de diffusion publicitaire. Bien que la Commission européenne ait examiné la manière dont ces entreprises utilisent les données des consommateurs, elle considère que c'est la législation sur la protection des données qui doit s'appliquer (plutôt que le droit de la concurrence) pour garantir la protection de la vie privée, précisant que (2008, p. 98[72]) :

> *Indépendamment de l'approbation de la concentration, la nouvelle entité est tenue, dans son activité journalière, de respecter les droits fondamentaux reconnus par tous les instruments pertinents à ses utilisateurs, notamment, mais sans que cela se limite à la protection de la vie privée et à la protection des données.*

81. Aux États-Unis, la FTC a pris une position du même ordre suite à son évaluation de la fusion *Google/DoubleClick*. Bien qu'elle n'eût pas considéré que le droit de la concurrence ne pouvait ni ne devait prendre en compte les répercussions en matière de protection de la vie privée, la FTC a toutefois estimé que cette fusion ne porterait pas préjudice aux aspects non tarifaires de la concurrence (2007, pp. 1-2[73]) :

> *Non seulement la Commission ne possède pas l'autorité juridique lui permettant d'imposer des conditions à la fusion qui ne relèvent pas du domaine antitrust, mais réglementer les obligations relatives à la vie privée d'une seule entreprise pourrait porter un préjudice grave à la concurrence dans ce secteur vaste et qui évolue rapidement. Nous avons toutefois étudié la possibilité que cette transaction puisse affecter de manière négative les aspects non tarifaires de la concurrence, parmi lesquels la protection de la vie privée des consommateurs. Nous observons toutefois que cette hypothèse n'est pas corroborée par des données concrètes. Nous avons ainsi conclu que les considérations de protection de la vie privée, en tant que telles, ne permettent pas de s'opposer à cette transaction.*

82. Même dans sa déclaration de dissentiment relative à la fusion *Google/DoubleClick*, et tout en soulignant les problèmes potentiels de protection de la vie privée, la commissaire Pamela Jones Harbour concède finalement qu'« *une approche plus globale de la protection de la vie privée reste préférable* » (Jones Harbour, 2007[74]). Autrement dit, selon elle, la protection de la vie privée doit être mise en œuvre dans l'ensemble de l'économie et pas uniquement relativement à des affaires de concurrence spécifiques. D'aucuns considèrent néanmoins que les fusions pourraient avoir pour effet de réduire le niveau de protection des données proposé sur les marchés concernés, même dans les cas où la législation sur la protection des données définit des normes minimales, dans la mesure où la concurrence pourrait entraîner une augmentation du niveau de protection au-dessus de ces normes.

83. Ces décisions ont depuis été contestées, entre autres car elles ne prenaient pas en compte les incidences du pistage par des acteurs tiers (Ezrachi et Roberston, 2019[49] ; Binns et Biettib, 2019[50]). Sur cette question, Ezrachi et Robertson (2019, p. 11[49]) se demandent si la fusion *Google/DoubleClick* ne reflétait pas « *une sous-estimation du réel avantage représenté par les données (agrégées)* ».

84. La Commission européenne a confirmé cette séparation juridique entre les problèmes de concurrence et les problèmes relatifs aux données des consommateurs lors de l'examen de la fusion *TomTom/TeleAtlas*, laquelle consistait en une fusion verticale entre un fournisseur de services de navigation et un fournisseur de plans numériques. Dans sa décision, la CE avait choisi de ne pas prendre en compte les incidences de cette fusion sur la protection de la vie privée et des données à caractère personnel (EC, 2008[75]). Dans différentes décisions qui ont suivi, la CE semble s'être appuyée sur les législations européennes sur la protection des données pour limiter l'ampleur de la réduction de la protection de la vie privée pouvant découler des fusions pertinentes que ce soit par une augmentation de la collecte, de l'agrégation ou de l'utilisation des données des consommateurs.

85. Dans l'affaire *Telefonica UK / Vodafone UK / Everything Everywhere* de 2012, la Commission européenne a choisi de prendre en compte les effets sur la concurrence d'une entreprise commune visant à proposer différents services de commerce mobile au Royaume-Uni (Commission européenne, 2012[76]). Ce faisant, la CE a établi que cette

entreprise commune serait contrainte par la législation sur la protection des données, dans la mesure où celle-ci conditionne la collecte et l'utilisation de données à une participation volontaire des consommateurs aux formes proposées (Zanfir-Fortuna et Ianc, 2019[77]).

86. Toujours en 2012, la FTC et l'ancien *Office of Fair Trading* du Royaume-Uni ont autorisé la fusion *Facebook/Instagram*, sans qu'aucune de ces deux autorités de la concurrence ne semble se préoccuper des incidences potentielles de cette fusion sur la protection des données et de la vie privée (OFT, 2012[78] ; FTC, 2012[79]).

87. En 2014, la Commission européenne (2013[80]) a quant à elle autorisé la fusion *Facebook/WhatsApp*, unissant un réseau social et une application de communication qui tous deux recueillent et utilisent des volumes variés de données des consommateurs. Dans son évaluation de cette fusion, la CE a pris en compte la capacité de l'entité issue de la fusion à combiner les données des consommateurs détenues à la fois par Facebook et par WhatsApp. La CE a pris note de la déclaration des parties à la fusion indiquant que cette combinaison serait techniquement difficile à mettre en œuvre, et a estimé que, dans tous les cas, les effets sur la concurrence seraient limités étant donné la part importante d'utilisateurs que les deux plateformes avaient en commun. La CE a également estimé que les considérations de protection de la vie privée relevaient de la législation sur la protection des données, en précisant que (2013, p. 29[80]) :

> *Les préoccupations relatives à la protection de la vie privée suscitées par la concentration accrue des données contrôlées par Facebook consécutivement à la Transaction ne relèvent pas du droit de la concurrence de l'UE mais des règles de la protection des données de l'UE.*

88. Lors des débats menant à cette décision, les représentants de la Commission européenne ont noté que la protection de la vie privée pouvait être un paramètre non tarifaire de la concurrence et qu'un nombre croissant de consommateurs accordaient de l'importance à cette protection de la vie privée. Ils ont toutefois également indiqué que la majorité des applications de communication grand public ne se livrent aucune concurrence sur la protection de la vie privée, et ont par conséquent conclu qu'il n'était pas pertinent de prendre en compte cette forme de concurrence dans le cadre de l'évaluation de la fusion *Facebook/WhatsApp* (Ocello, Sjödin et Subočs, 2015[81]). Les écarts dans les niveaux proposés de protection de la vie privée ont aussi été interprétés par la Commission européenne comme confirmant que Facebook et WhatsApp intervenaient sur des marchés différents. Lynskey (2018[82]) a déploré ce « raisonnement faussement logique » de la Commission européenne, en ce sens qu'elle négligé la possibilité que WhatsApp se fût différencié relativement au respect de la protection des données.

89. En 2017, faisant suite à la fusion *Facebook/WhatsApp*, la Commission européenne a imposé à Facebook une amende de 110 millions EUR pour avoir fourni des informations erronées ou trompeuses aux fins de son évaluation de 2014 (Commission européenne, 2017[83]). En effet, la Commission européenne a découvert que Facebook avait connaissance, au moment de la fusion, d'une possible solution technique permettant de faire correspondre automatiquement les identités des utilisateurs de Facebook et de WhatsApp. La CE a toutefois indiqué que ce nouveau fait n'affecterait pas son évaluation de 2014, notamment car elle avait déjà pris en compte cette possibilité avant de valider la fusion.

90. La fusion *Facebook/WhatsApp* avait également été validée par les États-Unis, mais ce faisant la FTC avait adressé aux deux parties une note visant à leur rappeler leurs obligations de protection de la vie privée des consommateurs (Rich, 2013[84] ; FTC, 2013[85]). Cette note précisait notamment la nécessité pour les entreprises d'obtenir le consentement des consommateurs avant de modifier leurs pratiques de collecte et

d'utilisation de leur données. Elle soulignait également que les entreprises ne devaient en aucun cas présenter de façon trompeuse la manière dont elles assurent la confidentialité ou la sécurité des données des utilisateurs, et recommandait aux entreprises d'offrir aux consommateurs la possibilité de ne plus autoriser l'utilisation de leurs données en cas de modification de cette utilisation.

91. Körber (2018, p. 14[59]) précise que l'intégration de bases de données séparées est, de manière générale, une « *opération particulièrement complexe, longue et onéreuse* ». Malgré cela, Lynskey (2018[82]) suggère que l'hypothèse de départ devrait être que les parties à la fusion ont la capacité de combiner leurs ensembles de données et le feront à terme. Cette approche semble avoir été celle adoptée par la Commission européenne et par la FTC dans leurs décisions de valider la fusion *Facebook/WhatsApp*.

92. La même année, la FTC a également validé la fusion *Google/Nest Labs*, laquelle avait pour objectif d'intégrer à la marque Google la société Nest, un fabricant d'appareils domestiques intelligents susceptibles de recueillir des volumes importants de données des consommateurs (FTC, 2013[86]). On ignore toutefois si la FTC a ou non pris en compte les effets potentiels de cette fusion sur la protection de la vie privée avant de finalement l'autoriser.

93. En 2014, la capacité des données des consommateurs à constituer un obstacle à l'entrée a été l'un des facteurs examinés dans l'évaluation de la fusion *Bazaarvoice/PowerReviews*, consistant en une fusion horizontale entre deux plateformes de notation et d'avis de consommateurs (United States v. Bazaarvoice, 2014[87] ; Ohlhausen, 2019[88]). Le ministère de la Justice des États-Unis s'est toutefois opposé à cette fusion en raison de problèmes horizontaux plus généraux (Ohlhausen, 2019[88]).

94. En 2016, la Commission européenne a autorisé la fusion *Microsoft/LinkedIn*, soulignant que même si la protection de la vie privée est un facteur de qualité essentiel dans le marché des réseaux sociaux professionnels, la législation européenne sur la protection des données limitera la manière dont l'entité issue de la fusion pourra combiner les données des deux entreprises (2016, p. 55[89]) :

> *Microsoft est soumis à la législation européenne sur la protection des données, laquelle limite sa capacité à réaliser quelque traitement que ce soit de l'ensemble des données de LinkedIn. Même si la politique actuelle de protection de la vie privée de LinkedIn lui permet de partager les données à caractère personnel que l'entreprise recueille, conserve et exploite avec les sociétés qui la contrôlent, ces pratiques sont uniquement autorisées aux fins décrites dans la politique de protection de la vie privée[. Le] Règlement général sur la protection des données, adopté récemment, […] peut encore restreindre la capacité de Microsoft à traiter de quelque manière que ce soit l'ensemble des données de LinkedIn en renforçant les droits existants et en octroyant aux individus un contrôle accru de leurs données à caractère personnel (grâce notamment à un accès simplifié à leurs données à caractère personnel, à un droit à la portabilité des données, etc.).*

95. Dans son communiqué de presse relatif à l'autorisation de la fusion *Microsoft/LinkedIn*, la Commission européenne a précisé sa position sur la prise en compte des considérations de protection de la vie privée dans les affaires de fusion (CE, 2016[90]) :

> *Les questions liées à la protection de la vie privée en tant que telles ne relèvent pas du droit européen de la concurrence, mais peuvent être prises en compte dans le cadre de l'appréciation réalisée sous l'angle de la concurrence, dans la mesure où les consommateurs les considèrent comme un facteur de qualité important et où les parties à la concentration se livrent concurrence sur ce facteur.*

96. Au-delà de ses effets potentiels sur la protection de la vie privée, il a été reproché à la Commission européenne de ne pas avoir suffisamment pris en compte les incidences de la fusion *Microsoft/LinkedIn* sur le pistage par des acteurs tiers (Binns et Biettib, 2019[50]). Ezrachi et Robertson (2019, p. 9[49]) considèrent ainsi que la fusion *Microsoft/LinkedIn* « *a augmenté de manière significative la portée et la variété des données collectées grâce aux pratiques de pistage par des acteurs tiers* » pour l'entité issue de la fusion. Ezrachi et Robertson (2019, pp. 8-9[49]) soulignent par ailleurs que :

> *Un pistage par des acteurs tiers à grande échelle, contrôlé par une seule et unique société, peut avoir pour effet d'accentuer les avantages liés aux données dont certaines entreprises des nouvelles technologies profitent déjà.*

97. En 2016, la Commission européenne (2016[91]) s'est également appuyée sur le droit à la portabilité des données au titre du RGPD pour protéger les consommateurs d'un effet potentiel de captivité découlant de la création d'une entreprise commune entre des filiales de Google et de Sanofi, laquelle visait à proposer des services de gestion et de traitement du diabète reposant sur la collecte, le traitement et l'analyse de données. En l'espèce, d'aucuns considèrent que l'application de mesures correctrices relevant du droit de la concurrence aurait permis de résoudre plus rapidement et plus directement les problèmes potentiels de captivité (voir la section 4.3).

98. Dans son évaluation de la fusion *Apple/Shazam* en 2018, la Commission européenne a étudié le rôle des données des consommateurs dans les marchés concernés (CE, 2018[92]). Elle a noté que les parties rassemblaient une grande variété de données, et souligné le rôle important et croissant des données des utilisateurs dans le secteur de la musique. Elle a ensuite examiné la capacité d'Apple à exploiter les données des utilisateurs détenues par la société pour renforcer la position de Shazam relativement à la publicité en ligne pour les amateurs de musique. La CE a toutefois estimé que cela ne nuirait pas de manière significative à la concurrence, dans la mesure où plusieurs acteurs du marché importants pouvaient se livrer concurrence sur cet aspect. Elle a également cherché à déterminer si les données des utilisateurs de Shazam pouvaient être considérées comme une ressource pertinente pour les fournisseurs d'applications de diffusion de musique numérique, mais a conclu que, même si l'entité issue de la fusion venait à refuser aux concurrents d'Apple l'accès aux données des utilisateurs de Shazam, il était peu probable que cela constitue un obstacle à l'entrée et porte préjudice à la concurrence.

99. Comme le montre cet exemple, il semblerait qu'on assiste à une prise de conscience de la capacité des entreprises à se livrer une concurrence sur le niveau de protection des données assuré, en tant qu'aspect de la qualité des biens et services qu'elles proposent. Certains se sont en outre interrogés sur les incidences, en termes de concurrence, de la combinaison des ensembles de données des consommateurs détenus par les parties à la fusion. Il semblerait que les autorités de la concurrence prennent de plus en plus en compte ces préoccupations dans leurs évaluations des fusions. À ce jour, néanmoins, aucune fusion n'a été contestée car elle aurait eu pour effet de réduire le niveau de protection des données dans le marché concerné. Dans de nombreuses affaires, les autorités de la concurrence se sont appuyées sur la nécessité d'obtenir le consentement des consommateurs pour la collecte et l'utilisation de leurs données afin de limiter la capacité des entités issues de fusions à combiner les ensembles de données des consommateurs dont elles disposaient. Autrement dit, elles ont compté sur la législation sur la protection des données pour encadrer la capacité des entreprises parties à une fusion à exploiter les données des consommateurs ou à altérer la protection des données de sorte à entraîner une réduction de la concurrence. La validité de cette hypothèse est abordée plus en détail dans la section 4.2.3.

4.1.2. Abus de position dominante

100. En théorie, une entreprise dominante pourrait tirer parti de sa position en réduisant le niveau de protection des données et de la vie privée qu'elle offre à ses clients (Kemp, 2019[17] ; Ezrachi et Roberston, 2019[49]). Dans certaines juridictions, cela pourrait être considéré comme une pratique d'exploitation abusive. Stucke (2018, pp. 285-286[66]) défend par exemple l'idée suivante : « *Un monopoleur de données, dans la mesure où son modèle économique repose sur la collecte et l'exploitation de données à caractère personnel, peut avoir intérêt à baisser le niveau de protection de la vie privée au-dessous des niveaux concurrentiels et à recueillir des données à caractère personnel au-delà des niveaux concurrentiels.* » Certains considèrent par ailleurs que, dans les juridictions où il est possible de poursuivre les entreprises dominantes pratiquant des prix excessifs, les mêmes lois pourraient être utilisées pour protéger les individus contre la collecte déloyale de données par une entreprise dominante (Ezrachi et Roberston, 2019[49]). En pratique, cependant, il n'existe que peu d'exemples d'affaires de ce type, tel qu'exposé ci-après.

101. Outre la théorie du préjudice abordée précédemment qui reposait sur des pratiques d'exploitation, on pourrait assister à l'émergence d'une théorie du préjudice basée sur l'abus de position dominante à caractère d'éviction. Un verrouillage du marché pourrait ainsi se produire lorsqu'une entreprise dominante met en œuvre des pratiques d'éviction qui limitent l'accès de ses concurrents aux données des consommateurs. De la même manière, lorsqu'une entreprise dominante dispose d'un accès exclusif à des données de consommateurs, elle pourrait être tentée d'augmenter les coûts de ses concurrents ou de renforcer les obstacles à l'entrée au moyen de ventes liées ou groupées.

Affaires pertinentes

102. Pour lutter contre les pratiques d'éviction dans le secteur de l'énergie, les autorités de la concurrence de la France et du Royaume-Uni ont exigé des fournisseurs d'énergie au détail qu'ils mettent à la disposition de leurs concurrents les données qu'ils recueillent sur leur consommateurs (par le biais d'Ofgem dans le cas du Royaume-Uni) afin d'encourager une meilleure concurrence (CMA, 2016[93] ; Autorité de la concurrence, 2014[94]). Pour répondre aux inquiétudes suscitées dans ces cas en termes de protection de la vie privée, il a été donné aux consommateurs la possibilité de suspendre volontairement le partage de leurs données. De son côté, l'autorité de la concurrence italienne a établi que le contrôle exclusif de listes de consommateurs par deux fournisseurs d'énergie réglementés pouvait avoir pour effet de verrouiller la concurrence dans la fourniture de services libéralisés d'énergie (Maggiolino et Ferrari, 2020[56]).

103. Néanmoins, à ce jour, on ne compterait qu'une seule affaire de pratiques d'exploitation en lien avec les données des consommateurs. En 2019, l'autorité de la concurrence allemande, le Bundeskartellamt, a déterminé que Facebook avait abusé de sa position dominante sur le marché des réseaux sociaux relativement à la collecte de données « en dehors de Facebook » (voir l'Encadré 9). Il s'agissait alors de la première décision s'appuyant sur une théorie du préjudice par laquelle la baisse de la protection de la vie privée était considérée comme relevant d'un abus de position dominante.

Encadré 9. Affaire Bundeskartellamt contre Facebook

En mars 2016, le Bundeskartellamt a ouvert une enquête pour abus de position dominante à l'encontre de Facebook, ciblant ses pratiques de gestion des données. En février 2019, l'autorité de la concurrence a déterminé que Facebook avait abusé de sa

position dominante sur le marché des réseaux sociaux en recueillant des données « en dehors de Facebook » (soit des données provenant d'acteurs tiers sans lien avec la plateforme). Pour utiliser les services de Facebook, les utilisateurs devaient accepter que l'entreprise recueille leurs données à la fois sur Facebook et sur un vaste ensemble d'applications et de sites internet tiers.

Le Bundeskartellamt a établi que Facebook disposait d'une position dominante sur le marché des réseaux sociaux en Allemagne, et que la plateforme n'avait pas obtenu un consentement éclairé des utilisateurs relativement à ses pratiques de pistage des données et à la fusion de ces données avec les profils Facebook des utilisateurs. Dans le cadre de l'évaluation des pratiques de Facebook en matière de données, le Bundeskartellamt a appliqué les normes du RGPD européen et conclu à l'insuffisance de ces pratiques, et donc à un abus de position dominante. L'autorité de la concurrence a justifié sa décision en indiquant que la position dominante de Facebook sur le marché plaçait les consommateurs dans une situation de type « à prendre ou à laisser » et que les pratiques de Facebook en matière de données contribuaient à renforcer sa position dominante. Au cours de son enquête, le Bundeskartellamt a entretenu des contacts réguliers avec les autorités chargées de la protection des données. Dans sa décision, l'autorité allemande de la concurrence exigeait que Facebook rectifie ses pratiques de collecte et de traitement des données sous 12 mois.

Facebook fit appel de la décision du Bundeskartellamt auprès du Tribunal de grande instance de Düsseldorf, lequel suspendit cette décision en août 2019. Le Tribunal n'acceptait notamment pas qu'une éventuelle violation des règles de la protection de la vie privée pût automatiquement entraîner une infraction au droit de la concurrence dans le cas d'une entreprise dominante. La cour considérait par ailleurs que les utilisateurs décident d'eux-mêmes s'ils acceptent ou non les conditions d'utilisation de Facebook lorsqu'ils s'inscrivent sur la plateforme. Le Tribunal détermina également que la collecte des données mise en œuvre par Facebook n'avait pas de caractère d'exploitation, dans la mesure où les consommateurs pouvaient continuer de partager les mêmes données avec d'autres entreprises. Il considérait enfin que le Bundeskartellamt n'était pas parvenu à prouver que les pratiques de Facebook en matière de données pouvaient nuire à la concurrence. La suspension de cette décision exemptait ainsi Facebook de mettre en œuvre les recommandations du Bundeskartellamt. L'autorité de la concurrence fit à son tour appel de cette suspension auprès de la Cour fédérale. Cet appel est toujours en cours.

Source : Bundeskartellamt (2019[95]) ; Bundeskartellamt (2019[96]) ; *Facebook/Bundeskartellamt*, décision interlocutoire du Tribunal de grande instance de Düsseldorf, 26 août 2019, affaire Vi-Kart 1/19 (V) ; CPI (2019[97]) ; Colangelo et Maggiolino (2018[98]) ; Këllezi (2019[99])

104. Dans cette procédure contre *Facebook*, l'une des principales difficultés pour le Bundeskartellamt était de montrer que l'entreprise avait abusé de son pouvoir de marché en forçant les utilisateurs à accepter des pratiques de collecte de données immodérées. Pour cela, l'autorité s'était appuyée sur le RGPD en tant que norme. Cependant, comme souligné dans l'Encadré 9, le Tribunal de grande instance de Düsseldorf a finalement invalidé cette approche. Le Bundeskartellamt a également suscité bien des critiques pour n'avoir proposé aucune analyse contradictoire et pour ne pas avoir démontré que les consommateurs portent un intérêt réel à la protection de la vie privée sur le marché des réseaux sociaux en Allemagne (Këllezi, 2019[99]). D'aucuns lui ont également reproché de ne pas avoir souligné les effets anticoncurrentiels des pratiques de Facebook (Këllezi, 2019[99]). Cette décision a néanmoins fait l'objet d'un appel et l'affaire est toujours en cours.

105. Plus largement toutefois, les facteurs liés à la demande pourraient rendre les affaires de ce type particulièrement difficiles à traiter, tel qu'exposé plus en détail dans la section 4.2.3. Ainsi, le fait qu'un nombre si faible de consommateurs s'intéressent aux notices d'informations sur la protection de la vie privée et les comprennent réellement, qu'elles proviennent ou non d'entreprises dominantes, représente une véritable difficulté dans les affaires dont l'enjeu consiste à prouver que les pratiques de collecte de données d'entreprises dominantes sont des pratiques abusives (Höppner, 2019[100] ; Colangelo et Maggiolino, 2018[98] ; Chirita, 2018[101]).

4.1.3. Ententes et collusion

106. Bien qu'aucune affaire de ce type ne se soit produite jusqu'à présent, une collusion basée sur l'établissement d'un niveau commun de protection de la vie privée des consommateurs pourrait constituer une infraction au droit des ententes, comme tout autre accord sur la qualité, la production ou les prix. De la même manière, tout accord visant à la fourniture de services sans contrepartie financière dans l'optique d'optimiser la collecte et l'utilisation des données des consommateurs pourrait entraîner l'apparition de problèmes de concurrence (OCDE, 2018[6]).

107. En outre, le partage de données entre concurrents peut parfois également susciter des préoccupations en matière de concurrence. Il n'est toutefois pas certain que le partage de données des consommateurs entre concurrents soit, par nature, susceptible de faciliter les collusions. Ainsi, dans les cas où les données n'incluent aucune information sur les prix, la qualité, les innovations ou les choix des consommateurs, il n'est pas évident que le partage de données des consommateurs permette de faciliter les collusions. En pratique, dans les affaires de concurrence pertinentes, la tendance a été d'autoriser le partage de données des consommateurs, dans la mesure où il a été montré que cette pratique pouvait stimuler la concurrence.

Affaires pertinentes

108. L'affaire *Asnef-Equifax* de 2006 est souvent citée comme l'une des toutes premières affaires dans lesquelles des considérations de protection de la vie privée furent prises en compte par la Cour européenne de justice, avant de décider que ces considérations relevaient de la législation sur la protection des données et non du droit de la concurrence. Cette affaire *Asnef-Equifax* concernait un accord établi entre des institutions financières concurrentes dans le but de créer un registre partagé réunissant des informations bancaires et sur la solvabilité des consommateurs, et ce, afin de déterminer leur niveau de risque pour l'octroi de crédits et de prêts (Cour de justice de l'Union européenne, 2006[102]). Dans son évaluation du potentiel anticoncurrentiel de cet accord, lequel facilitait le partage de données à caractère personnel, la Cour européenne de justice (2006, p. 20[102]) indiquait que :

> *... les éventuelles questions relatives à l'aspect sensible des données à caractère personnel ne relevant pas, en tant que telles, du droit de la concurrence, elles peuvent être résolues sur le fondement des dispositions pertinentes en matière de protection de telles données.*

109. Cet accord fut finalement validé au motif qu'il permettrait de stimuler la concurrence dans la fourniture des services financiers qui s'appuient sur de telles informations.

110. En 2019, le gouvernement brésilien a promulgué une loi ayant pour objet de développer une cote de solvabilité personnelle. Cette cote fut mise en œuvre avec une possibilité de non-participation, même si l'objectif était qu'elle s'appliquât par défaut à

tous les consommateurs (Banco Central do Brasil, 2019[103]). Cette loi faisait suite à une décision de l'autorité de la concurrence brésilienne (CADE) datant de 2016, validant la création d'une entreprise commune entre Banco do Brasil, Bradesco, Caixa Econômica, Itaú et Santander, sous la forme d'un nouveau bureau de crédit. L'autorité considérait ainsi que les avantages générés par un registre de solvabilité consolidé compenseraient largement les incidences potentielles sur la concurrence (CADE, 2016[104]). Ces effets potentiels sur la concurrence furent abordés dans le cadre d'un accord de contrôle de fusion, lequel garantissait un accès non discriminatoire aux informations sur les crédits et aux mécanismes de gouvernance des entreprises pour les bureaux de crédit concurrents, et ce, afin d'éviter les échanges d'informations entre les banques associées et l'entreprise commune.

4.2. Difficultés analytiques

111. Comme illustré par certains des exemples mentionnés ci-dessus, les affaires ayant trait aux données des consommateurs peuvent présenter des difficultés analytiques spécifiques. Celles-ci sont notamment liées à la définition du marché, aux obstacles à l'entrée, aux facteurs liés à la demande, à la mesure de la protection des données ou encore à l'évaluation des gains d'efficience proconcurrentielle. Chacune d'entre elle est abordée plus en détail ci-dessous.

4.2.1. Définition du marché

112. La nécessité de définir, dans certains cas, ce qui constitue un « marché des données » a fait l'objet de différents débats dans la littérature relative à la concurrence (Costa-Cabral et Lynskey, 2017[105]). À titre d'exemple, Jones Harbour et Koslov (2010, p. 773[106]) indiquent que :

> *La définition d'un marché des données permettrait de marquer la différence entre la collecte des données à un moment donné et leur utilisation élargie ultérieure […]. Les entreprises œuvrant sur l'internet tirent souvent un profit conséquent des données des utilisateurs […] et leur exploitation a souvent des répercussions importantes sur la concurrence. À l'inverse, les définitions de marché de produits s'appuyant uniquement sur un instantané de l'utilisation ponctuelle des données pourraient ne pas donner une représentation fiable de cet aspect de la concurrence.*

113. De la même manière, Forrest (2019[107]) considère que les données d'une entreprise et sa capacité algorithmique à analyser ces données constituent en soi des produits. Ainsi, « *la banalisation potentielle d'un ensemble de données a pour effet de permettre indirectement la définition d'un univers concurrentiel* » (Forrest, 2019, p. 12[107]). À l'inverse, selon Körber (2018, p. 2[59]), « *il ne peut y avoir un et unique* « *marché des données », de la même manière qu'il ne peut exister un seul et unique « marché des matières premières* ».

114. Jones Harbour et Koslov (2010[106]) considèrent quant à elles que les effets sur la concurrence dans les marchés à forte intensité de données pouvaient être évalués par la prise en compte des obstacles à l'entrée. Elles donnent ainsi l'exemple de différentes fusions dans le cadre desquelles les autorités de la concurrence ont examiné l'impact sur la concurrence de la combinaison d'ensembles de données issus d'entreprises concurrentes. Il s'agissait notamment de données financières, de santé, liées aux divertissements ou encore générées par des systèmes électroniques d'estimation des coûts (2010[106]). Dans la mesure où il existe un certain degré de substituabilité entre l'évaluation des effets sur la concurrence par le biais d'une définition du marché et l'évaluation des obstacles à l'entrée,

cette seconde option apparaît comme l'approche la moins controversée. Cet aspect est abordé plus en détail ci-dessous.

115. Par ailleurs, dans la mesure où un grand nombre de marchés bifaces et multifaces dépendent des données des consommateurs, il peut être pertinent de prendre en compte la complexité d'une définition du marché dans ces types de marchés. Pour plus d'informations à ce sujet, reportez-vous au rapport de l'OCDE de 2018 consacré à la révision des outils du droit de la concurrence pour les plateformes multifaces (OCDE, 2018[108]).

4.2.2. Obstacles à l'entrée

116. Différentes caractéristiques des marchés numériques laissent penser que les obstacles à l'entrée pourraient être nombreux dans les marchés impliquant les données des consommateurs. Les rendements d'échelle croissants, les économies de gamme et les effets de réseau peuvent en effet souvent être observés dans ces marchés (Kemp, 2019[17]). Lorsqu'une entreprise doit supporter des coûts irrécupérables importants pour pénétrer sur un marché spécifique, ceux-ci peuvent constituer un véritable obstacle à l'entrée. Rubinfeld et Gal (2017[37]) ont procédé à une analyse approfondie de la chaîne d'approvisionnement des données afin d'identifier les possibles obstacles à l'entrée associés à la collecte, au stockage, au traitement et à l'exploitation des données. Ces obstacles sont répertoriés dans le Tableau 1 et décrits plus en détail ci-dessous.

Tableau 1. Obstacles à l'entrée dans la chaîne d'approvisionnement des données

	Obstacles techniques	Obstacles juridiques	Obstacles comportementaux
Collecte	• Caractère unique des données ou accès à ces données • Du côté de l'offre : économies d'échelle, gamme, apprentissage empirique et rapidité • Du côté de la demande : effets de réseau et marchés bifaces	• Législation relative à la protection des données et de la vie privée • Propriété des données	• Accords d'exclusivité • Prix et conditions d'accès • Désactivation des logiciels de collecte de données
Stockage	• Coûts	• Législation relative à la protection des données et de la vie privée	• Phénomène de captivité et coûts de conversion
Synthèse et analyse	• Défaut d'interopérabilité (manque de normalisation y compris) • Outils d'analyse		
Exploitation	• Incapacité à localiser et contacter les consommateurs cibles • Défaut d'interopérabilité (manque de normalisation y compris)	• Législation relative à la protection des données et de la vie privée • Législation anti-discrimination	• Limitations contractuelles

Source : Rubinfeld et Gal (2017[37]) ; Gal et Rubinfeld (2019[26]) ; CMA (2016[93])

117. Concernant la collecte des données, Rubinfeld et Gal (2017[37]) indiquent que si une entreprise dispose d'un accès exclusif à des données uniques, celles-ci pourraient s'avérer difficiles à reproduire sans entraîner des coûts irrécupérables importants. Par exemple, accéder aux publications et commentaires de consommateurs sur un réseaux social en position dominante peut être une configuration particulièrement difficile à reproduire. Comme l'indiquent Maggiolino et Ferrari (2020, p. 41[56]) :

> *… une analyse empirique et au cas par cas des circonstances de fait devrait être systématiquement réalisée pour déterminer s'il est possible d'obtenir les mêmes données (c'est-à-dire des données répondant aux mêmes besoins) à partir d'une autre source sur le marché.*

118. Cette analyse devrait par ailleurs prendre en compte l'accès des entreprises à la fois aux données de première partie et aux données de tiers.

119. Rubinfeld et Gal (2017[37]) précisent également que des obstacles technologiques liés à l'offre pourraient apparaître lorsque des entreprises en place ont déjà réalisé des économies d'échelle ou de gamme, ou tirent parti d'un « apprentissage empirique ». Les importants coûts fixes et irrécupérables induits par la collecte de données à haute vitesse peuvent également représenter des obstacles à l'entrée (Pecman, Johnson et Reisler, 2020[57]). L'une des difficultés pratiques principales consiste à déterminer à quel moment des déséconomies d'échelle et de gamme peuvent apparaître. Les travaux de Chiou et Tucker (2017[109]) suggèrent, au moins dans le cas des moteurs de recherche en ligne, que l'accès à des données historiques sur des périodes plus longues ne présente pas nécessairement un avantage significatif. De la même manière, Körber (2018[59]) indique que les données présentent généralement un rendement marginal décroissant et donc que chaque élément supplémentaire apporte chaque fois moins d'informations. Certains défendent toutefois l'idée selon laquelle les données pourraient en réalité proposer des rendements d'échelle croissants (Gal et Aviv, 2020[110]). Ainsi, la capacité d'un concurrent potentiel à recréer le corpus de données d'une entreprise en place, aussi bien termes de volume, de vitesse et de variété des données, est d'une importance essentielle, comme cela est décrit dans la section 2.2.3.

120. En matière de collecte de données, il peut également exister des obstacles à l'entrée liés à la demande, notamment lorsque des effets de réseau peuvent être observés. La présence de marchés bifaces, ainsi que la nécessité de pouvoir accéder à un marché connexe pour recueillir certains types de données (phénomène qualifié par Rubinfeld et Gal (2017[37]) d'« entrée à deux niveaux »), peut également entraîner une augmentation des coûts irrécupérables induits pour pénétrer sur le marché concerné. Certains obstacles juridiques, comme la législation relative à la protection des données et de la vie privée, peuvent en outre s'ajouter aux obstacles à l'entrée. Des obstacles comportementaux, comme les accords d'exclusivité et les conditions ou prix d'accès discriminatoires, peuvent également apparaître dans certains marchés impliquant les données. De la même manière, les ventes liées ou groupées associées à la collecte des données des consommateurs peuvent nécessiter des analyses complémentaires afin de déterminer leur impact sur la concurrence.

121. En matière de stockage, Rubinfeld et Gal (2017[37]) indiquent que les coûts tendent à baisser, ce qui les rend moins susceptibles de constituer un obstacle à l'entrée que par le passé (notamment dans les situations où ces coûts ne sont pas irrécupérables). Ils mentionnent également les obstacles juridiques, comme les restrictions juridiques applicables aux emplacements physiques où les données à caractère personnel des individus peuvent être conservées. Ils notent par ailleurs que des coûts élevés de conversion en matière de stockage pourraient entraîner un phénomène de captivité. Quant à la synthèse et à l'analyse des données, Rubinfeld et Gal répertorient un certain nombre d'obstacles techniques potentiels, parmi lesquels une interopérabilité incomplète des données ou encore les coûts associés au développement des outils d'analyse. Enfin, concernant les obstacles potentiels liés à l'exploitation des données, ils notent les difficultés à localiser les consommateurs ciblés et les limitations contractuelles restreignant l'utilisation éventuelle des données de manières différentes, mais aussi certains obstacles juridiques encadrant la façon dont ces données peuvent être utilisées.

122. Plusieurs autorités de la concurrence ont déterminé que l'accès aux données des consommateurs dont bénéficie une entreprise en place est également susceptible de dresser des obstacles à l'entrée dans différents marchés de plateformes numériques. Dans sa décision sur l'affaire *Facebook*, le Bundeskartellamt (2019[95]) indique ainsi :

> *L'intérêt non négligeable en termes de concurrence que représente pour un fournisseur de réseaux sociaux sa base de données constituera cependant un obstacle supplémentaire à l'entrée sur le marché […].*

123. Dans son étude sur les plateformes numériques (ACCC, 2019, p. 11[58]), l'ACCC déclare :

> *L'étendue et la portée des données d'utilisateurs collectées par les plateformes numériques de premier plan leur octroient un avantage concurrentiel important, créant ainsi des obstacles à l'entrée et à l'expansion pour les plateformes concurrentes dans les marchés concernés, et permettant aux plateformes numériques établies de se développer dans les marchés voisins […].*

124. La conclusion de l'ACCC met en avant la nécessité de prendre en compte l'ensemble des sources de données auxquelles une entreprise a accès et de déterminer si cet accès est unique ou s'il peut être reproduit. Il convient par ailleurs de noter l'importance des données des consommateurs dans l'amélioration des biens et services sous-jacents et dans la conquête de nouveaux consommateurs (phénomène de la « boucle de rétroaction »). Sur ce point, Colangelo et Maggiolino (2018, p. 2[98]) précisent que :

> *… la collecte et l'agrégation de données, y compris de données à caractère personnel, par les entreprises dominantes permettent de renforcer leur position dominante[. P]lus le volume de données recueillies et analysées par une entreprise est important, meilleurs seront ses produits, plus elle attirera d'utilisateurs, plus elle sera en capacité de collecter et traiter d'autres données, et ainsi de suite.*

125. Acquisti et al. (2016, p. 444[15]) notent également que :

> *… quelques entreprises « contrôleuses d'accès » sont en mesure de gérer le pistage et les liaisons de ces comportements entre les plateformes, les services en ligne et les sites internet, et ce, pour des milliards d'utilisateurs. Des registres complets des actions, souhaits, intérêts ou simples intentions des individus sont par conséquent recueillis par des acteurs tiers, souvent sans que ces individus en aient conscience ou aient donné leur consentement formel, et ce, dans une ampleur, avec une portée et avec un niveau de détail probablement sans précédents dans l'histoire de l'humanité.*

126. Pour résumer, toute évaluation visant à déterminer, d'une part, si la combinaison d'ensembles de données des consommateurs ou, d'autre part, si tout effort pour restreindre l'accès aux données des consommateurs est susceptible de créer des obstacles à l'entrée doit être réalisée au cas par cas sur la base des caractéristiques de chaque affaire. Lors de l'examen des éventuels obstacles à l'entrée, il peut être intéressant de prendre en compte les facteurs répertoriés dans le Tableau 1, dans la mesure où ceux-ci représentent des coûts irrécupérables.

4.2.3. Attitude des consommateurs à l'égard de la protection de la vie privée

127. Pour comprendre les dynamiques concurrentielles qui existent dans les marchés impliquant des données des consommateurs, il convient d'abord de comprendre les attitudes et comportements des consommateurs relativement à la protection des données et de la vie privée dans les marchés pertinents (Manne et Sperry, 2015[111]). De manière générale, bien que les attitudes envers la protection de la vie privée varient d'un individu à

l'autre et en fonction de nombreux facteurs, différentes études ont montré que les consommateurs portent un intérêt réel à la protection de la vie privée, notamment en ligne (Cisco, 2019[112] ; Auxier et al., 2019[113] ; RSA, 2019[114]). Néanmoins, dans le contexte des évaluations d'impact sur la concurrence, certaines particularités au niveau de la demande peuvent nuire à une bonne appréciation de l'importance de la protection des données et de la vie privée pour les consommateurs dans les marchés considérés.

128. Premièrement, l'attitude des consommateurs envers la protection de la vie privée est à la fois *« subjective et idiosyncrasique »* (Acquisti, Taylor et Wagman, 2016, p. 446[15]). Les consommateurs ont en effet tendance à avoir des préférences hétérogènes à l'égard de la protection de la vie privée (Walters, Zeller et Trakman, 2018[115]). Par ailleurs, pour un même individu, la décision de partager ou non certaines informations personnelles dépendra du contexte dans lequel ces informations sont demandées (Acquisti, Taylor et Wagman, 2016[15]). En pratique, cela s'applique souvent à de nombreux aspects des offres concurrentielles proposées par les entreprises, ce qui veut dire que les autorités de la concurrence ont déjà une expérience solide en la matière.

129. Les biais comportementaux peuvent également inciter les consommateurs à partager plus de données ou à accepter un plus faible niveau de protection de la vie privée qu'ils l'auraient normalement fait. L'une des difficultés est que la protection de la vie privée offre des contreparties à très long terme, alors que le partage de données est susceptible de générer un avantage immédiat (et plus certain), contrairement aux risques encourus dont le prix reste indéfini et pouvant se produire dans un avenir indéterminé (Acquisti, Taylor et Wagman, 2016[15]). Cela peut poser des problèmes particulièrement épineux car les consommateurs ont tendance à se placer dans une optique assez étroite et à faire preuve d'une certaine incohérence temporelle dans leurs préférences (Choi, Jeon et Kim, 2019[68]). La manière dont les options de protection de la vie privée sont présentées peut également entraîner un partage de données plus important, dans la mesure où le biais en faveur du *statu quo* pousse généralement les consommateurs à valider les paramètres par défaut (Costa-Cabral et Lynskey, 2017[105]). Les consommateurs peuvent ailleurs sous-estimer l'importance de la protection de la vie privée dans les marchés sans contrepartie financière (et à surestimer les avantages offerts par les biens ou services à prix nul) en raison de l'« effet de gratuité » (OCDE, 2018[6]).

130. Les observateurs ont également exprimé leurs inquiétudes quant au manque de pouvoir de négociation des consommateurs concernant les notices d'informations sur la protection de la vie privée, lesquelles sont la plupart du temps proposées sur le principe « à prendre ou à laisser » (Hull, 2014[116] ; Costa-Cabral et Lynskey, 2017[105]). On peut supposer que ces inquiétudes reflètent l'absence de concurrence efficace sur le marché concerné. L'incapacité des consommateurs à interagir avec les politiques de protection de la vie privée ou à s'y intéresser et la limitation de cette capacité en raison des biais comportementaux peuvent faire en sorte que les consommateurs acceptent des conditions auxquelles ils ne consentent en réalité aucunement. Ces travers pourraient nuire à l'efficacité de législation sur la protection des données, laquelle repose principalement sur le consentement des consommateurs. Devant cette situation, certains se sont inquiétés de la capacité des consommateurs à comprendre les notices d'informations sur la protection de la vie privée et à agir en conséquence (Hoofnagle et Whittington, 2014[117]). Dans son étude sur les plateformes numériques (ACCC, 2019, p. 2[58]), l'ACCC indique que :

> *… peu de consommateurs apprécient pleinement, comprennent intégralement ou contrôlent réellement l'ampleur des données collectées et le marché qu'ils acceptent avec les plateformes numériques lorsqu'ils souscrivent ou utilisent leurs services.*

131. Différentes études menées par l'ACCC ont par exemple montré que 36 % des consommateurs pensent (à tort) que la simple existence d'une politique de protection de la vie privée signifie que les entreprises ne partageront pas leurs informations personnelles avec des acteurs tiers (ACCC, 2019[58]).

132. Cette problématique peut prendre la forme de ce que l'on appelle le « paradoxe de la vie privée ». Il désigne le fait que les consommateurs s'inquiètent de la protection de leur vie privée et la considèrent comme un aspect important, mais ne semblent prendre aucune décision en fonction de ce critère (Norberg, Horne et Horne, 2007[118] ; Kokolakis, 2017[119] ; OCDE, 2018[6]). Ainsi, en 2019, 79 % des Américains exprimaient des inquiétudes sur la façon dont les entreprises utilisent leurs données et 81 % estimaient que les risques potentiels associés à la collecte des données étaient supérieurs aux avantages escomptés (Auxier et al., 2019[113]). Il se peut également que, même si les consommateurs attachent de l'importance à la protection de la vie privée, ils la considèrent comme secondaire par rapport à d'autres caractéristiques des produits, comme un prix plus faible ou de meilleures fonctionnalités. C'est ainsi ce qu'a révélé une expérience réalisée par Preibusch, Kübler et Beresford (2013[120]), au cours de laquelle une écrasante majorité des participants acceptaient d'acheter des DVD auprès d'un marchand en ligne assurant un plus faible de niveau de protection de la vie privée simplement parce que les prix pratiqués étaient inférieurs. Même lorsque le niveau de protection de la vie privée était le seul élément distinctif, le choix du détaillant apparaissait relativement aléatoire. Cela peut expliquer que si peu d'entreprises aient choisi de se différencier des autres sur le seul critère de la protection de la vie privée (OCDE, 2018[5]). Cela peut également expliquer pourquoi les entreprises offrant un niveau supérieur de protection de la vie privée ne sont pas parvenues à remporter des parts de marché significatives dans leurs marchés respectifs (à titre d'exemple, DuckDuckGo, un moteur de recherche sur l'internet dont la caractéristique est de ne recueillir aucune information sur les consommateurs, peine encore à gagner des parts de marché).

133. Ces problématiques pourraient par ailleurs limiter la possibilité d'une réelle concurrence en matière de protection de la vie privée, même si les consommateurs y attachent de l'importance. Tel que souligné par la CMA (2015[28]), les consommateurs devraient en théorie pouvoir sanctionner les entreprises relativement à leurs pratiques de collecte et d'exploitation des données des consommateurs. Autrement dit, si des consommateurs ne sont pas satisfaits de la manière dont une entreprise utilise leurs données, ils devraient pouvoir changer facilement de prestataire. Malheureusement, si les consommateurs ne comprennent pas quelles données sont recueillies par une entreprise, comment elles sont utilisées et quelle est leur valeur réelle, ils risquent de ne pas être à même de prendre des décisions dans l'intérêt de la protection de leur vie privée. Les incitations pour les entreprises à se livrer une concurrence sur l'aspect de la protection de la vie privée semblent donc particulièrement limitées (Farrell, 2012[121] ; Lynskey, 2018[82]). Cela peut être encore plus marqué lorsque le marché concerné est peu concurrentiel et que les consommateurs n'ont accès à aucune alternative viable (Costa-Cabral et Lynskey, 2017[105] ; Lynskey, 2018[82]). Dans ce contexte, il semble difficile de déterminer dans quelles circonstances et dans quels marchés les consommateurs comprennent et accordent réellement une importance aux enjeux de protection de la vie privée, que ce soit en théorie comme en pratique. Ces problématiques peuvent par ailleurs nuire à l'efficacité des modèles de protection des données basés sur le consentement, modèles sur lesquels les autorités de la concurrence ont pu s'appuyer pour promouvoir une protection efficace des données dans les cas où une fusion ou un fort pouvoir de marché était susceptible de nuire à cette efficacité.

134. Pour mieux comprendre la perception des consommateurs sur la protection de la vie privée, il pourrait être intéressant pour les autorités de la concurrence de réaliser des

études auprès des consommateurs pour compléter les évaluations des affaires de concurrence dans lesquelles la protection de la vie privée est susceptible de constituer un aspect de la qualité d'un produit ou service. Par exemple, pour évaluer les incidences d'une fusion sur la concurrence, il peut s'avérer utile de déterminer si toute différence visible dans le niveau de protection de la vie privée proposé par les parties à la fusion présente une importance significative pour les consommateurs. À l'inverse, dans le cas des abus de position dominante, des études menées auprès des consommateurs pourraient permettre de déterminer si les consommateurs sont satisfaits du niveau de protection de la vie privée proposé, et dans le cas contraire, sur quoi repose cette insatisfaction. Naturellement, si les autorités de la concurrence viennent à utiliser ce type de données, elles doivent veiller à prendre en compte que les préférences déclarées ont tendance à être supérieures aux préférences révélées. Cet effet semble aller dans le sens du paradoxe de la vie privée. Néanmoins, dans la mesure où les autorités de la concurrence sont moins soucieuses de déterminer dans quelle proportion les consommateurs accordent de l'importance à la protection de la vie privée plutôt que d'établir si une part suffisante des consommateurs accordent de l'importance à la protection de la vie privée, ces limitations pourraient s'avérer moins significatives en pratique. De telles études ont également l'avantage de pouvoir être adaptées sur mesure aux marchés ciblés. Cet aspect est d'autant plus important que la perception de la protection de la vie privée dépend du contexte et peut évoluer au fil du temps et en fonction de la sensibilisation des consommateurs aux pratiques des entreprises (Gilbert et Pepper, 2015[52]).

135. Les réactions des consommateurs face aux changements (même uniquement potentiels) du niveau de protection de la vie privée assuré par les entreprises dans un marché spécifique peuvent également être une source utile d'informations sur l'importance qu'ils accordent à la protection de la vie privée sur ce marché. À titre d'exemple, dans son évaluation de la fusion *Facebook/WhatsApp*, la Commission européenne (2013[80]) a fait état des « milliers » d'utilisateurs qui ont téléchargé d'autres applications de messagerie (Telegram, en particulier) et du grand nombre d'utilisateurs allemands qui ont délaissé WhatsApp au profit de Threema après l'annonce de l'acquisition de WhatsApp par Facebook. La CE a souligné que ce basculement de WhatsApp vers des applications assurant une meilleure protection de la vie privée reflétait la valeur qu'au moins une partie des consommateurs accordaient à cet enjeu sur ce marché spécifique. Les réactions des consommateurs suscitées par différents scandales liés à la protection de la vie privée, comme l'affaire *Facebook-Cambridge Analytica*, peuvent aussi apporter des informations utiles.

4.2.4. Comment évaluer la concurrence en matière de protection des données

136. Lors de l'évaluation d'une fusion entre deux parties qui semblent se livrer une concurrence sur la protection de la vie privée, il peut s'avérer utile de comparer les pratiques de chaque partie en la matière et de déterminer l'importance des différences observées en termes de concurrence. De la même manière, dans les affaires d'abus de position dominante liées à une diminution de la protection de la vie privée ou à une collecte abusive des données des consommateurs, il sera important d'examiner les pratiques des entreprises dominantes en matière de protection des données et de la vie privée.

137. L'une des principales difficultés dans ce type d'affaires d'abus de position dominante consiste à déterminer « *où s'arrête la légitimité de la collecte de données et où commence l'excès dans la collecte des données* » (Robertson, 2020, p. 173[16]). Autrement dit, en l'absence d'une concurrence efficace, il est difficile de savoir si des pratiques de partage des données des consommateurs, et plus généralement de protection de la vie privée, sont réellement concurrentielles (Colangelo et Maggiolino, 2018[98]).

138. Lorsque les autorités de la concurrence sont en capacité de traiter les affaires d'abus de position dominante, Robertson (2020[16]) considère que les principes de proportionnalité et d'équité, la nécessité de conditions commerciales loyales et le pouvoir de négociation des parties sont tous des facteurs à prendre à compte pour démontrer le caractère excessif du niveau de données exigé. Colangelo et Maggiolino (2018, p. 21[98]) précisent également que la notion de déloyauté englobe par ailleurs les dispositions « *sans aucun lien défendable avec l'objet du contrat, limitant indûment la liberté des parties, disproportionnées, imposées de façon unilatérale ou fortement opaques* ». Ces critères s'appuient sur les arrêts de la Cour européenne de justice et les décisions de la Commission européenne dans les affaires *Tetra Pak II*, *Duales System Deutschland (DSD)*, *United Brands* et *Michelin II*, et s'avéreront essentiels pour déterminer si les pratiques d'entreprises dominantes doivent être considérées comme « abusives ».

139. Par ailleurs, les huit principes définis dans les « Lignes directrices de l'OCDE sur la protection de la vie privée » (voir l'Encadré 2) peuvent fournir certaines orientations sur la manière d'évaluer la qualité de la protection de la vie privée assurée par les différents acteurs d'un marché, que ce soit dans le cadre de fusions ou d'affaires d'abus de position dominante (OCDE, 2013[11]). Sur la base de ces principes et des approches proposées par Esayas (2018[122]) et Waehrer (2016[123]), la qualité de la protection de la vie privée pourrait éventuellement être évaluée selon les catégories suivantes :

- **Minimisation de la collecte** – Quelles données sont recueillies ? L'entreprise pratique-t-elle la minimisation des données (c.-à-d. la collecte du volume minimum de données nécessaire à la mise en œuvre d'un bien ou service) ? Une réponse peut être obtenue par le biais de demandes d'informations, adressées aux entreprises concernées ou grâce à des avis d'experts.
- **Minimisation de l'utilisation** – À quelles fins les données sont-elles utilisées ? Combien de temps seront-elles conservées ? Avec qui seront-elles partagées ? À nouveau, les autorités de la concurrence pourraient obtenir des réponses en adressant aux entreprises concernées des demandes d'informations ou grâce à des avis d'experts.
- **Transparence** – Quelles informations sont fournies à l'utilisateur concernant la collecte et l'utilisation de données ? Sous quelle forme ces informations sont-elles fournies ? Les politiques de protection de la vie privée et autres garanties connexes pourraient être évaluées selon des critères de lisibilité et d'intelligibilité.
- **Contrôle des utilisateurs** – Les utilisateurs peuvent-ils accéder facilement à leurs données, les modifier, les supprimer et les transférer ? Quels sont les choix dont disposent les utilisateurs ? Des évaluations d'experts pourraient contribuer à répondre à ces questions.
- **Sécurité et protection de la vie privée dès la conception** – Quelles mesures de sécurité ont été mises en place pour protéger les données de tout accès non autorisé ou de toute altération, perte ou destruction accidentelle ? L'entreprise a-t-elle recours à des technologies protectrices de la vie privée, comme le chiffrement de bout-en-bout des données, la pseudonymisation ou l'anonymisation ? Des avis d'experts peuvent être nécessaires pour répondre à ces questions, appuyés par les réponses des entreprises aux demandes d'informations.
- **Protection de la vie privée par défaut** – Les entreprises mettent-elles en œuvre par défaut des dispositifs de protection de la vie privée ? Là encore, des avis d'experts peuvent être nécessaires pour répondre à cette question, appuyés par les réponses des entreprises aux demandes d'informations.

140. Il existe de nombreuses sources de données susceptibles de contribuer à la réalisation de ce type d'évaluations. Dans le cadre de l'examen de fusions, par exemple, de nombreuses autorités de la concurrence envoient des questionnaires aux parties à la fusion et, dans certains cas, à leurs concurrents. Ces enquêtes pourraient notamment inclure des questions visant à déterminer si la protection de la vie privée est un aspect important de la concurrence dans les marchés concernés, et s'il s'agit ou non d'une priorité pour les consommateurs. À titre d'exemple, lors de son examen de la fusion *Microsoft/LinkedIn* en 2016, la Commission européenne a mené une enquête par questionnaire auprès des entreprises de réseaux sociaux afin, entre autres, de mieux comprendre si la protection de la vie privée constituait un facteur significatif de concurrence et influait sur le choix des consommateurs sur ce marché (Commission européenne, 2016[89]).

141. Dans le cas des fusions, tout document montrant que certaines entreprises sont attentives aux politiques de protection de la vie privée d'autres entreprises peut témoigner d'un certain niveau de concurrence sur cette question, surtout si les entreprises réagissent et s'adaptent aux modifications apportées par des concurrents à leurs politiques de protection de la vie privée (sauf si ces modifications visent à intégrer une évolution des prescriptions réglementaires) (Waehrer, 2016[123]). Jones Harbour et Koslov (2010[106]) notent ainsi qu'après l'annonce de Google indiquant que la société allait raccourcir la durée de conservation des données des consommateurs, Microsoft a réduit cette durée à six mois et Yahoo! à trois mois. Certaines évaluations internes concernant les réactions des consommateurs face à l'évolution du niveau de protection de la vie privée peuvent laisser penser qu'il s'agit d'un aspect important de la concurrence dans les marchés concernés, que ce soit dans le cadre d'une fusion ou en lien avec une situation d'abus de position dominante.

142. Dans le cas des affaires d'abus de position dominante, tout élément montrant que les pratiques des entreprises dominantes en matière de protection de la vie privée se sont adaptées à l'évolution des niveaux de concurrence sur le marché cible peut également s'avérer particulièrement utile. D'après Srinivasan (2019[124]), la dégradation récente de la protection de la vie privée sur les réseaux sociaux est la conséquence de hauts niveaux de pouvoir de marché, lesquels ne laissent aux consommateurs aucune alternative viable (en tout cas aucune disposant d'une base existante d'utilisateurs, ce qui souligne bien l'importance des effets de réseau dans ces marchés). Srinivasan fait ainsi état d'une concurrence supérieure en matière de protection de la vie privée dans les premiers temps des réseaux sociaux, lorsque l'enjeu de cette concurrence était de s'imposer comme la plateforme dominante. Encore une fois, comme dans toute affaire d'abus de position dominante, prouver qu'une entreprise dominante a abusé de sa position à des fins anticoncurrentielles reste malgré tout particulièrement difficile.

4.2.5. Gains d'efficience potentiels

143. Dans certains cas, comme lors de l'évaluation de fusions, il convient de déterminer si certaines pratiques sont susceptibles de générer des gains d'efficience compensatoires. Cela inclut les situations où la protection de la vie privée peut être affectée de manière négative. Comme l'indiquent Manne et Sperry (2015, p. 4[111]) :

> *Un affaiblissement de la protection de la vie privée n'est pas un simple transfert des consommateurs vers les producteurs qui entraînerait cette fameuse perte sèche pour l'économie dont font état les manuels spécialisés en droit de la concurrence. La collecte et l'exploitation de volumes importants d'informations par une entreprise comme Google ont la capacité d'améliorer la qualité même de ses produits, que ce soit en renforçant la pertinence de ses résultats de recherche ou du ciblage de ses publicités.*

144. Manne et Sperry (2015[111]) considèrent ainsi que toute évaluation de la protection de la vie privée en tant qu'aspect de qualité devrait prendre en compte les gains d'efficience qui découlent d'une collecte plus importante des données (en termes d'amélioration des biens/services et du ciblage des publicités) et d'une tarification plus faible (souvent nulle) des biens et services. De la même manière, Cooper (2013, p. 1135[125]) estime que « *recueillir toujours plus de données sur les consommateurs ne revient pas à lésiner sur la qualité, car la collecte, le stockage et l'analyse de ces données représentent des coûts supplémentaires* ».

145. Par ailleurs, dans le cas de fusions impliquant des ensembles de données des consommateurs, il conviendra également de déterminer si la combination des données générera des gains d'efficience sous la forme d'une amélioration de la productivité dans les activités de production ou de distribution, ou par la fourniture de produits et services conçus sur mesure (Haucap, 2019[126]). Par exemple, l'une des critiques formulées à l'encontre du Bundeskartellamt dans l'affaire visant Facebook est qu'il n'avait pas pris en compte les avantages qu'offrait à Facebook la collecte des données des consommateurs en termes de publicité ciblée (Höppner, 2019[100]).

146. Dans l'idéal, les autorités de la concurrence devraient prendre en considération l'ensemble des gains d'efficience potentiels, lorsque cela est permis par leurs tests législatifs et dans la mesure où ces gains d'efficience ont été générés par les pratiques ciblées.

4.3. Mesures correctrices potentielles

147. La nature des mesures correctrices que devraient mettre en place les autorités de la concurrence au titre du droit de la concurrence dépend de la théorie du préjudice envisagée.

148. Concernant les fusions, aussi bien des mesures structurelles que comportementales pourraient s'avérer efficaces. À titre d'exemple, des mesures correctrices comportementales permettraient de limiter la capacité d'une entité issue d'une fusion à combiner les données des consommateurs des deux parties d'origine. Elles pourraient également exiger que l'accès à cet ensemble de données soit accordé aux concurrents selon des conditions équitables, raisonnables et non discriminatoires (ou conditions « FRAND », pour *fair, reasonable and non-discriminatory*). À l'inverse, des mesures correctrices structurelles pourraient obliger l'entité issue de la fusion à céder son ensemble de données, lorsque l'accès à ce dernier soulève des problèmes de concurrence qui ne peuvent être réglés autrement[3]. Si des inquiétudes apparaissent quant au manque potentiel de pression concurrentielle dont ferait l'objet une entité issue d'une fusion pour garantir un niveau compétitif de protection de la vie privée, les autorités de la concurrence pourraient bloquer cette fusion sur la base que celle-ci entraînerait potentiellement une réduction du bien-être du consommateur.

149. En pratique, il existe de nombreux exemples de cas où les autorités de la concurrence ont imposé le partage des données comme condition à la validation d'une fusion. Ainsi, pour autoriser la fusion *Ticketmaster/Live Nation*, tous deux opérateurs sur le marché de la vente de billets de spectacles, le ministère de la Justice des États-Unis a exigé de l'entreprise issue de la fusion qu'elle fournisse sur demande à ses clients les données relatives à leurs achats de billets dans un format exploitable (Department of Justice, 2010[127]). Autrement dit, il s'agissait d'une obligation de portabilité des données (Jones Harbour et Koslov, 2010[106]). Des mesures correctrices du même ordre ont pu être

[3] De manière plus générale, les restrictions applicables aux branches d'activité seront examinées de façon plus approfondie en juin 2020 dans le cadre des débats du Groupe de travail nº 2 du Comité de la concurrence.

mises en œuvre dans le cas de fusions impliquant des entreprises qui disposaient de bases de données de registres fonciers (Ohlhausen, 2019[88]).

150. Dans les affaires d'abus de position dominante à caractère d'éviction, ce type de mesure peut présenter un intérêt lorsque les inquiétudes en matière de concurrence concernent l'accès à un ensemble de données des consommateurs. Les affaires relatives au secteur de l'énergie mentionnées dans la section 4.1.2 sont des exemples intéressants de cas où des entreprises dominantes en amont ont été contraintes de fournir des informations à leurs concurrents potentiels en aval afin de faciliter la concurrence au niveau du commerce de détail dans les marchés de l'énergie.

151. L'un des avantages du recours au droit de la concurrence dans l'optique de faciliter les mouvements de données entre entreprises, par rapport à une obligation expresse de portabilité des données, est que le droit de la concurrence peut s'appliquer à tous les types de données, alors que la portabilité des données se limite généralement aux données à caractère personnel (Graef, Verschakelen et Valcke, 2013[128] ; Engels, 2016[61]). Par ailleurs, dans la mesure où le droit de la concurrence est plus ciblé, il permet d'imposer des coûts de mise en conformité uniquement dans les affaires suscitant des inquiétudes en matière de concurrence. Il a également la particularité d'être relativement flexible et donc de pouvoir s'ajuster aux exigences des marchés concernés, et ainsi d'exiger un accès continu aux données des consommateurs dans certains cas et un accès ponctuel exceptionnel dans d'autres cas. Les mesures correctrices relevant du droit de la concurrence ne sont toutefois pas dénuées d'inconvénients, en ce sens qu'elles s'appliquent plus souvent *a posteriori*, sont plus susceptibles d'être contestées et s'avèrent difficiles à généraliser. Des exigences de portabilité des données ciblées mais systématiques pourraient par conséquent être plus pertinentes dans certains marchés (voir la section 5.1.1). Une autre solution possible au titre du droit de la concurrence consiste à s'interroger sur la possible application de la théorie des installations essentielles, tel qu'abordé ci-après.

152. Il semble plus difficile de savoir de quelle manière les affaires d'abus de position dominante visant des acteurs dominants ayant recours à des pratiques abusives de collecte, d'exploitation ou de partage de données des consommateurs peuvent être réglées par l'application de mesures correctrices relevant du droit de la concurrence. Comme dans toute affaire d'abus de position dominante, il n'est pas évident de déterminer le niveau de protection des données qui existerait si la concurrence était plus efficace sur le marché concerné. Par ailleurs, il est peu probable que s'appuyer sur des modèles de protection des données basés sur le consentement s'avère réellement efficace dans les marchés peu concurrentiels.

153. Enfin, lorsque la théorie du préjudice concerne un cas d'entente ou de collusion, il semblerait que la principale mesure correctrice à prendre soit de mettre fin à la pratique visée.

154. De manière plus générale, les autorités de la concurrence devraient collaborer avec les autorités en charge de la protection des données et de la vie privée, mais aussi avec les autorités de la protection du consommateur, afin de déterminer quels types d'affaires doivent donner lieu à des poursuites et comment développer les mesures correctrices appropriées (voir la section 5.4).

4.4. La théorie des installations essentielles

155. Comme l'indiquent Crémer et al., (2019, p. 73[14]), « *la compétitivité des entreprises dépendra de plus en plus de leur capacité à accéder rapidement à des données pertinentes et à exploiter ces données pour développer des produits et applications nouveaux et innovants* ». De nombreux observateurs se sont interrogés sur la pertinence de

considérer les données comme un « service essentiel », auquel pourrait donc éventuellement s'appliquer la théorie des installations essentielles.

156. Dans le droit de la concurrence de la plupart des pays de l'OCDE, certaines dispositions permettant aux entreprises de demander l'accès aux ressources d'autres entreprises si cet accès est nécessaire à la fourniture d'un bien ou service. La théorie des installations essentielles, élaborée aux États-Unis en 1912, a traditionnellement été appliquée aux infrastructures matérielles qui ne peuvent raisonnablement pas être dupliquées pour des raisons techniques, juridiques ou économiques, comme les ports, les aéroports, les réseaux ferroviaires ou les systèmes de transport d'eau et de gaz. Un accès au titre de la théorie des installations essentielles n'est généralement accordé que lorsque : 1) la partie qui en fait la demande ne peut obtenir les biens ou services concernés d'une autre manière ; 2) elle ne peut les concevoir ou les créer elle-même ; et 3) la partie qui en est propriétaire ne peut présenter aucune justification commerciale légitime pour en refuser l'accès.

157. Sur la question des données et de la théorie des installations essentielles en Europe, Diker Vanberg et Ünver (2017, p. 9[129]) considèrent qu'en théorie :

> *… si une entreprise dominante détient des données spécifiques qui s'avèrent indispensables à l'entrée d'autres entreprises sur un nouveau marché, et que le refus de cette entreprise dominante de transmettre ces données a pour effet d'éliminer toute concurrence potentielle, alors, en l'absence de toute justification objective, l'article 102 du TFUE peut être invoqué.*

158. En pratique, cependant, il n'existe encore aucune jurisprudence en la matière. Diker Vanberg et Ünver (2017, p. 11[129]) reconnaissent donc qu'« *il serait particulièrement difficile pour une entreprise de prouver qu'elle ne peut développer sa propre base de données d'informations personnelles sans un accès aux données du concurrent dominant* ». Dans le cas des plateformes en ligne, par exemple, Körber (2018, p. 12[59]) considère qu'« *il n'est pas du tout évident que les « mines d'informations » détenues par des entreprises comme Google ou Facebook soient réellement des ressources non redondantes, et qu'elles constituent donc des ressources essentielles* ». Aux États-Unis, les tribunaux ont en outre eu tendance à refuser d'imposer l'ouverture de l'accès à des bases de données spécifiques, en particulier suite à la décision dans l'affaire *Trinko*, laquelle a restreint la portée de la théorie des installations essentielles[4].

159. Pour déterminer si les données devraient entrer dans le champ d'application de la théorie des installations essentielles, Lambrecht et Tucker (2017[60]) ont examiné si les données (au sens général) sont suffisamment précieuses, uniques et rares pour constituer un « avantage concurrentiel durable». D'après elles, il est peu probable que ce soit réellement le cas, et ce, pour la plupart des types de données. Elles concluent ainsi que l'accès à une main-d'œuvre qualifiée et la capacité d'anticiper la demande des consommateurs sont généralement des ressources plus importantes que l'accès à des données. De la même manière, Gilbert et Pepper (2015[52]) estiment que l'accès aux données est rarement susceptible de constituer un obstacle significatif à l'entrée, dans la mesure où les données sont des biens non rivaux et peu onéreux, que la propriété des données est dispersée, que les données anciennes n'ont que peu de valeur et que leur

[4] Voir *Verizon Communs., Inc. contre Law Offices of Curtis contre Trinko*, LLP - 540 U.S. 398, 124 S. Ct. 872 (2004) (trinko). Voir également Diker Vanberg et Ünver (2017[129]) pour une discussion sur les affaires *LiveUniverse, Inc. contre MySpace, Inc.*, 2008 WL 5341843 (9th Cir. Dec. 22, 2008), *Facebook contre Power Ventures Inc.*, No. 17-16161 (9th Cir. 2019), et *Peoplebrowsr, Inc., et al. contre Twitter, Inc.*, No. C-12-6120 EMC, United States District Court, N.D. California (2013).

rendement tend à être décroissant. Ils précisent également que le facteur de rareté déterminant est les « ressources humaines » nécessaires pour traiter et analyser les données.

160. Haucap (2019[126]) suggère toutefois qu'il peut exister de bonnes raisons économiques pour justifier une baisse du seuil à partir duquel l'accès aux données peut être accordé à des tiers. Ainsi, parce que les données sont des biens non rivaux, permettre leur accès à des tiers n'empêche aucunement le maître du fichier d'exploiter ces mêmes données. À l'inverse, dans le cas des infrastructures, il n'est pas rare que différentes entreprises ne puissent utiliser la même infrastructure au même moment (par exemple, en accostant au même port en même temps ou atterrissant sur la même piste au même moment). Par ailleurs, étant donné que les coûts induits par la collecte et la gestion des ensembles de données seront probablement moindres, l'ouverture de l'accès à des tiers devrait limiter les incitations pour les entreprises à investir dans la collecte des données et la gestion des ensembles de données.

161. Dans la mesure où les données des consommateurs prennent une importance grandissante, la théorie des installations essentielles reste un moyen possible de faciliter le partage de données des consommateurs lorsque cela s'avère nécessaire pour stimuler la concurrence. En principe, il ne semble exister aucun obstacle à l'application de la théorie des installations essentielles aux données des consommateurs, même si aucune affaire ne permet à ce jour d'illustrer cette pratique et qu'il est possible que différents obstacles jurisprudentiels doivent au préalable être contournés. Il sera intéressant de suivre l'évolution de ce pan de la législation relativement à l'essor des données des consommateurs.

5. Coopération et sensibilisation

162. Bien que les politiques de la concurrence, de protection du consommateur et de protection des données partagent toutes un objectif commun d'amélioration des résultats pour les consommateurs, des tensions peuvent apparaître sur la manière d'y parvenir dans la pratique. Ainsi, la politique de la concurrence contribue à cet objectif en favorisant la concurrence et par conséquent le bien-être du consommateur. Les politiques de protection du consommateur et de protection des données visent quant à elles plus à protéger et autonomiser directement les consommateurs.

163. La promotion de la concurrence peut à cet égard permettre de garantir que les politiques de protection du consommateur et de protection des données ne s'exercent pas au détriment de la concurrence. Il convient par ailleurs d'encourager la coopération afin que le meilleur instrument d'action publique soit utilisé chaque fois que plusieurs options sont disponibles.

5.1. Impact des droits relatifs aux données des consommateurs sur la concurrence

164. Comme pour de nombreuses autres formes de réglementation, les coûts de mise en conformité associés à la législation sur la protection des données et de la vie privée peuvent constituer un obstacle à l'entrée. Lorsque ces coûts sont principalement fixes, ils peuvent désavantager les petites entreprises de façon disproportionnée. À titre d'exemple, les estimations des coûts de mise en conformité au RGPD s'avèrent particulièrement élevées. Au Royaume-Uni, ils représenteraient en moyenne 1.7 million GBP par entreprise, allant d'un peu moins de 1 million GBP pour les entreprises de 100 à 249 salariés pour atteindre 2.3 millions GBP pour les entreprises de plus de 1 000 salariés (Calgigo, 2017[130]). Même aux États-Unis, une étude réalisée par PwC a montré que 68 % des entreprises américaines devraient dépenser entre 1 et 10 millions USD, et que 9 % d'entre elles devraient dépenser

plus de 10 millions USD pour assurer leur conformité au RGPD (PWC, 2017[131]). Quant aux petites et moyennes entreprises européennes, on estime leurs coûts informatiques annuels de mise en conformité au RGPD entre 3 000 EUR et 7 200 EUR, soit 17 à 40 % de leur budget informatique annuel avant l'adoption du GDPR) (Christensen et al., 2013[132]). Cela ne signifie pas pour autant que les avantages de telles réglementations ne sont pas à la hauteur des investissements nécessaires, mais plutôt que de tels coûts de mise en conformité peuvent avoir une incidence sur la concurrence dans les marchés où les entreprises doivent se conformer à ces réglementations. La question reste pour les autorités de la concurrence de déterminer s'il est possible d'atteindre les objectifs de la législation sur la protection des données tout en réduisant au minimum les impacts (négatifs) sur la concurrence.

165. Certains ont également exprimé leurs inquiétudes sur la possibilité que les formes de réglementation sur la protection de la vie privée basées sur le consentement avantagent et renforcent les entreprises en place, notamment celles qui œuvrent sur plusieurs marchés (Campbell, Goldfarb et Tucker, 2015[133] ; Marthews et Tucker, 2019[134]). Cet effet serait particulièrement marqué dans les marchés où la flexibilité tarifaire est limitée, comme les marchés sans contrepartie financière (Campbell, Goldfarb et Tucker, 2015[133]). Marthews et Tucker (2019[134]) précisent par ailleurs que le besoin de consentement et de conformité à chaque étape de la chaîne d'approvisionnement de la publicité en ligne ne fait qu'accroître les pressions en faveur d'une intégration verticale.

166. Picker (2008, pp. 11-12[135]) soulève également un autre problème :

> *… les règles de protection de la vie privée qui limitent la manière dont les informations peuvent être utilisées et partagées entre les entreprises ne feront que contribuer artificiellement à une plus grande consolidation, ce qui s'avère généralement préjudiciable au maintien d'une concurrence efficace.*

167. Campbell, Goldfarb et Tucker (2015[133]) précisent ainsi que les systèmes à participation par consentement pourraient avoir un impact disproportionné sur les petites entreprises et les entreprises nouvelles, ce qui, d'après eux, nuirait certainement à la concurrence. Cette situation serait plus susceptible de se produire lorsque les coûts de mise en conformité sont principalement fixes (quelle que soit la taille de l'entreprise), imposant un fardeau plus lourd aux petites entreprises qu'aux grandes entreprises. Comme le soulignent Gal et Aviv (2020[110]), obtenir le consentement des consommateurs pourrait permettre de réaliser des économies d'échelle et de gamme. Ohlhausen (2019[88]) indique également que, dans la mesure où la législation sur la protection des données et de la vie privée limitent les capacités des entreprises à acquérir et exploiter des données des consommateurs qu'elles n'ont pas elles-mêmes recueillies, les entreprises en place qui ont déjà obtenu le consentement nécessaire pour collecter et utiliser d'importants volumes de données de consommateurs pourraient voir leur position renforcée.

168. Les premiers travaux sur les incidences du RGPD suggèrent qu'il a permis d'améliorer la protection de la vie privée et de renforcer la capacité des individus à contrôler leurs données, mais qu'il aurait peut-être aussi entraîné une baisse de la concurrence dans les marchés exploitant de manière importante les données des consommateurs. À titre d'exemple, sur un échantillon constitué des plus importants sites internet d'actualité de sept pays européens, le nombre de cookies tiers par page a connu une baisse de 22 % entre avril et juillet 2018 (Libert, Graves et Nielsen, 2018[136]). Cependant, bien que la plupart des sites internet et applications intègrent toujours des cookies et des contenus tiers, les parts de marché des plus grandes plateformes ont continué d'augmenter après la mise en place du RGPD (Greif, 2018[137]). Ainsi, alors que dix entreprises avaient pisté au moins 50 % des sites internet d'actualité les plus importants au mois d'avril, leur nombre était passé à seulement cinq au mois de juillet (Libert, Graves et Nielsen, 2018[136]). Une autre étude a

montré par ailleurs que le RGPD avait entraîné une concentration plus intense de la publicité en ligne en Europe (Moazed, 2019[29]).

169. Gal et Aviv (2020[110]) précisent qu'en plus de potentiellement favoriser les grandes entreprises (comme indiqué précédemment), le RGPD pourrait également réduire les incitations au partage de données et restreindre l'exploitation des données. Plus précisément, la nécessité de garantir que toute partie avec laquelle une entreprise partage des données de consommateurs respecte les dispositions du RGPD représente un engagement particulièrement onéreux et susceptible de nuire au partage de données. Par ailleurs, dans la mesure où les données des consommateurs peuvent uniquement être utilisées aux fins pour lesquelles les utilisateurs ont à l'origine donné leur consentement, leurs possibilités d'utilisation seront d'autant plus limitées. Pour conclure, Gal et Aviv indiquent que ces effets sont susceptibles de limiter la concurrence dans les marchés exploitant les données des consommateurs, et ce, en renforçant la concentration du marché et en réduisant l'efficience productive et dynamique.

170. Civot et Castro (2019[138]) ont également exprimé leur crainte que le RGPD n'entrave le développement et l'utilisation de l'IA en Europe. Le RGPD limite la capacité des entreprises à exploiter les données à d'autres fins que celles pour lesquelles elles ont été collectées, ce qui empêche de fait l'utilisation des données des consommateurs dans des applications liées à l'IA que les entreprises n'avaient pas envisagées au moment où ces données ont été recueillies. D'aucuns soutiennent par ailleurs que l'article 22 du RGPD, lequel exige que les décisions automatisées puissent être justifiées, impose des contraintes supérieures à ce type de décisions qu'aux décisions non automatisées.

171. À l'inverse, l'amélioration des niveaux de protection de la vie privée et du contrôle des données, rendue possible par les réformes récentes, pourrait permettre de résoudre certains problèmes liés à la demande considérés comme potentiellement préjudiciables à une concurrence efficace en matière de protection des données et de la vie privée. En outre, si la réglementation sur la protection de la vie privée limite la concurrence alors qu'elle remplit ses objectifs, il est possible que les responsables de l'action publique ne la considèrent pas moins comme une réussite. Il est essentiel que les autorités de la concurrence déterminent les moyens d'atteindre ces objectifs en créant le moins possible de distorsions de concurrence. Elles doivent également étudier la possibilité d'introduire d'autres politiques favorables à la concurrence afin de contrebalancer les effets négatifs de l'adoption de normes minimales sur la concurrence. En pratique, il est peut-être trop tôt pour saisir toutes les implications de certaines des réformes qui ont récemment été mises en œuvre. Au cours des prochaines années, il sera important d'évaluer l'efficacité de ces réformes en termes de protection de la vie privée, de protection du consommateur et de stimulation de la concurrence. L'un des domaines qui présente un enjeu particulier en termes de politique de la concurrence est celui de la portabilité des données. Cet aspect est abordé de façon plus approfondie ci-dessous.

5.1.1. Portabilité et interopérabilité des données

172. La section 2.3.2 a déjà permis de présenter différents exemples de droits relatifs à la portabilité des données. La manière dont ces droits et les responsabilités y afférentes sont mis en œuvre a une incidence sur la bonne marche de la concurrence. De nombreux observateurs ont ainsi fait part de leur crainte que la portabilité des données, telle que définie par le RGPD, n'entraîne d'importantes dépenses de mise en conformité qui, parce qu'elles devront également être supportées par des entreprises non dominantes, pourraient nuire à la concurrence et par conséquent au bien-être du consommateur (Swire et Lagos, 2013[139] ; Lyons, 2018[140]). Diker Vanberg et Ünver (2017[129]) considèrent que ces effets pourraient être évités par l'adoption d'une exemption pour les petites et moyennes

entreprises, et pour les entreprises disposant d'une faible part de marché ou présentant un chiffre d'affaires insuffisant. Engles (2016[61]) va même plus loin en suggérant que la portabilité des données devrait être limitée aux situations dans lesquelles un acteur du marché a acquis une position dominante du fait de pratiques anticoncurrentielles.

173. D'aucuns ont également reproché aux dispositions de portabilité des données prévues dans le RGPD qu'elles permettent uniquement la transmission de données historiques à un moment précis, ce qui risque de rendre difficile le multihébergement ou la fourniture de services complémentaires s'appuyant sur une transmission continue, voire en temps réel, de données des consommateurs (Crémer, de Montjoye et Schweitzer, 2019[14]).

174. Par ailleurs, suivant que la portabilité des données est initiée par un consommateur ou par une entreprise (cherchant à obtenir des données avec le consentement des consommateurs), on peut s'attendre à ce que cela affecte la bonne marche de la concurrence (Diker Vanberg et Ünver, 2017[129]). Dans certains cas, les obstacles liés à la demande peuvent limiter l'efficacité de la portabilité des données induite par les consommateurs. Ainsi, à moins que les consommateurs ne sachent exactement comment exercer leurs droits à la portabilité des données et comprennent les avantages de ces droits, ils pourraient ne jamais tirer parti de la portabilité des données. On peut d'ailleurs considérer que la portabilité des données aura une valeur supérieure pour les concurrents potentiels que pour chaque consommateur de manière individuelle (Nicholas et Weinberg, 2019[141]). Ainsi, dans le cas des entreprises nécessitant un volume important d'utilisateurs (par exemple, dans les marchés marqués par les effets de réseau), une portabilité des données induite par les consommateurs telle que définie par le RGPD pourrait ne pas permettre des changements de prestataires à grande échelle (Gal et Aviv, 2020[110]). À cet égard, Diker Vanberg et Ünver (2017[129]) considèrent ainsi que le droit de la concurrence, et en particulier la théorie des installations essentielles (voir la section 4.4), constitue un moyen plus efficace de stimuler la concurrence dans les marchés qui dépendant de l'accès aux données. Toutefois, dans d'autres cas, la portabilité des données induite par les consommateurs présenterait un intérêt non négligeable, notamment lorsqu'il existe un avantage significatif à permettre aux consommateurs d'accéder à leurs données et de les transmettre à un autre prestataire. À titre d'exemple, la portabilité des numéros de téléphone portable et des numéros de compte bancaire a permis justement de générer des avantages significatifs (voir l'Encadré 10).

Encadré 10. Avantages supposés de la portabilité

Il a été prouvé que la **portabilité des numéros de téléphone portable** avait permis de réduire les prix sur le marché des forfaits de communications téléphoniques. Une étude a montré que la baisse moyenne des tarifs a été d'environ 1 % pour les forfaits de base, 4.8 % pour les forfaits intermédiaires et 6.8 % pour les forfaits à volume élevé de communications. Une autre étude a estimé les réductions à hauteur de 6.6 % à 12 % selon les méthodologies de calcul utilisées.

Portabilité dans les marchés financiers : en septembre 2013, le *Payments Council* du Royaume-Uni a mis en place un nouveau service de changement de compte courant, appelé *Current Account Switch Service* (CASS). Ce programme à participation volontaire, disponible auprès d'une quarantaine de banques et de sociétés de crédit immobilier représentant plus de 99 % du marché, a pour objectif de simplifier et d'accélérer le changement de comptes courants pour les consommateurs. Une évaluation du CASS réalisée en 2015 a permis de montrer une augmentation du taux de

changement de prestataires, inférieure toutefois aux attentes en raison d'une mauvaise connaissance de ce programme par les consommateurs.

Systèmes bancaires ouverts (*Open Banking*) : les travaux du *Centre for Economics and Business Research* montrent que la portabilité des données rendue possible par l'ouverture des systèmes bancaires avait entraîné une baisse de 7 % des écarts de rémunération (taux de rendement sans risque complété par une prime de risque) sur les prêts hypothécaires, pour un total de 1 milliard GBP. Sur la base de ces observations et pour le compte du ministère du Numérique, de la Culture, des Médias et des Sports du Royaume-Uni, Ctrl-Shift a estimé que l'impact économique de la mobilité des données s'élèverait à 28 milliards GBP répartis sur l'ensemble de l'économie du pays.

Source : Park (2011[142]) ; Lyons (2006[143]) ; FCA (2015[144]) ; Trustpilot (2018[145]) ; Ctrl-Shift (2018[146])

175. De nombreuses entreprises proposent depuis déjà un certain temps une forme de portabilité des données. Facebook, par exemple, permet depuis 2010 à ses utilisateurs d'accéder à leurs informations par le biais de la fonction « Télécharger vos informations » (Egin, 2019[147]). De la même manière, les utilisateurs de Google ont depuis 2011 la possibilité de télécharger les données à caractère personnel détenues par la société grâce à son outil « Takeout », depuis rebaptisé « Télécharger vos données » (Google, 2018[148]).

176. Un certain nombre de questions restent toutefois en suspens quant à la manière dont les entreprises parviendront à mettre en œuvre la portabilité des données telle que définie par les différents régimes réglementaires appliqués à travers le monde (Egin, 2019[147]). Ainsi, assurer le transfert des données des consommateurs d'une entreprise à une autre (plutôt que directement au consommateur) pose des problèmes spécifiques. L'une des principales questions est de déterminer quelles données à caractère personnel devraient être couvertes par la portabilité des données. Certains s'accordent à penser que la portabilité des données devrait s'appliquer à la fois aux données communiquées volontairement et aux données recueillies par observation (Article 29 Data Protection Working Party, 2016[149]). Il semble par ailleurs généralement admis que la portabilité des données ne devrait pas concerner les données obtenues par inférence (Article 29 Data Protection Working Party, 2016[149]). Il n'est toutefois pas certain que la portabilité des données doivent s'appliquer dans le cas des données acquises. Un arbitrage doit également être fait entre garantir, d'une part, que les données fournies permettront d'éviter le phénomène de captivité, les coûts de conversion et les obstacles à l'entrée, et, d'autre part, que les exigences de portabilité des données ne limiteront pas les incitations à investir dans la collecte et le traitement des données. À cet égard, ne pas inclure les données obtenues par inférence dans les données soumises à la portabilité, notamment dans les transferts entre entreprises, semble une option appropriée pour préserver les incitations à l'investissement. À l'inverse, fournir ces informations aux individus auxquels elles se rapportent contribuerait vraisemblablement à un renforcement de l'autodétermination informationnelle.

177. Le format et la teneur des données détermineront également leur utilité pour les objectifs d'autodétermination informationnelle et de stimulation de la concurrence. S'il venait à recevoir l'ensemble des données collectées à son sujet par une entreprise, un consommateur pourrait vite se sentir dépassé, surtout si ces données ne sont pas structurées. Néanmoins, l'accès à un vaste ensemble de données de consommateurs peut s'avérer particulièrement précieux pour un concurrent potentiel si les obstacles à l'entrée associés à la collecte des données sont élevés. À titre d'illustration, Nicholas et Weinberg (2019[141]) ont réuni différents membres de la communauté technologique de la ville de New York afin de déterminer quels nouveaux produits ils seraient en mesure de développer à partir de données anonymisées obtenues grâce à la fonction « Télécharger vos informations » de

Facebook. D'après les participants, les données disponibles n'étaient pas suffisantes pour développer un réseau social concurrent. Comme le soulignent Nicolas et Weinberg (2019, p. 2[141]), « *tenter d'utiliser des données d'utilisateurs exportées pour reproduire une plateforme comme Facebook revient à utiliser des meubles pour tenter de reproduire l'immeuble d'où ces meubles proviennent* ». Les participants éprouvaient même des difficultés à concevoir de nouveaux produits concurrentiels sur la base de ces informations.

178. Une autre question clé à se poser concerne l'équilibre à trouver entre la protection de la vie privée des autres consommateurs et les demandes de portabilité (Egin, 2019[147]). Par exemple, si un consommateur demande la portabilité de ses données sur un site de réseaux sociaux, comment les entreprises vont-elles assurer la protection de la vie privée de ses contacts, tout en lui fournissant des données réellement utiles ? Cette question sera d'autant plus pertinente dans les marchés où la valeur des données repose en partie sur les interactions entre consommateurs, comme pour les réseaux sociaux et les applications ou services de communication (Nicholas et Weinberg, 2019[141]). À l'inverse, cette question sera moins pertinente dans les marchés où les données concernent uniquement un seul individu. Il est en effet peu probable, par exemple, que les préférences et habitudes d'un consommateur en matière de musique, d'exercice physique ou de contenus vidéo impliquent d'autres consommateurs. De manière plus générale, la responsabilité du maintien de la protection de la vie privée et de la sécurité lors du transfert de données entre entreprises est un élément important à prendre en considération (Egin, 2019[147]).

179. D'autres types d'interopérabilité, comme l'interopérabilité des protocoles (standard ou complète) ou l'interopérabilité des données, pourraient s'avérer plus efficaces pour promouvoir la concurrence lorsqu'est nécessaire un flux de données de consommateurs en continu, voire en temps réel (Crémer, de Montjoye et Schweitzer, 2019[14]). Ces mesures vont au-delà de la portabilité des données et pourraient en effet stimuler la concurrence dans les marchés connexes, ainsi qu'entre concurrents déjà existants. L'interopérabilité des protocoles correspond au développement de protocoles dans le but de faire fonctionner ensemble des systèmes différents (p. ex. : les systèmes d'exploitation ou les protocoles de chargement entre téléphones et chargeurs). L'interopérabilité des données permet quant à elle un accès en temps réel aux données, généralement dans un format normalisé. Naturellement, les coûts de mise en conformité associés à ces différentes formes d'interopérabilité ne sont pas les mêmes. Les entreprises facilitent actuellement l'interopérabilité des données principalement à l'aide d'API propriétaires. Celles-ci permettent notamment aux développeurs tiers d'accéder aux données des entreprises pour développer des biens et services complémentaires. À titre d'exemple, les fonctionnalités des applications de mobilité, comme CityMapper, Transit ou Moovit, s'appuient sur des API développées par les opérateurs de transport, dont *Transport for London* (TfL), et dans de nombreux cas sur des API permettant l'intégration de Google Maps (altexsoft, 2018[150]). Ces applications de mobilité ont tiré parti de l'adoption, par les organismes de transport, d'un format normalisé pour les calendriers des notifications et les informations géographiques, contribuant ainsi aux efforts d'interopérabilité (Gal et Rubinfeld, 2019[26] ; GTFS, s.d.[151]). Évidemment, ces exemples n'impliquent pas nécessairement des données à caractère personnel, lesquelles posent pourtant des difficultés particulières en termes de protection de la vie privée.

180. Bien que les API puissent contribuer à améliorer la portabilité des données, d'aucuns se sont interrogés sur la capacité des propriétaires d'API à surveiller, voire bloquer, l'accès à leurs API à des concurrents potentiels (Nicholas et Weinberg, 2019[141]). À titre d'exemple, Twitter été accusé par certains d'avoir rejeté des demandes d'accès à son API ou révoqué l'accès à cette API pour des applications en concurrence directe avec ses services. En 2012, Twitter a également apporté des modifications à son API, exigeant de ses utilisateurs qu'ils demandent une autorisation d'accès spéciale si leur base

d'utilisateurs dépassait le seuil de 100 000 comptes (OCDE, 2015[3]). Les utilisateurs de l'API Graph de Facebook ont également fait part de leurs inquiétudes concernant la possibilité que Facebook surveille, voire copie, l'utilisation qu'ils font de l'API, que la société suspende unilatéralement leur accès à l'API ou encore qu'elle modifie la structure des données (augmentant par là même les coûts indirects associés à l'utilisation de cette API) (Nicholas et Weinberg, 2019[141]). De tels comportements sont susceptibles de limiter les avantages proconcurrentiels que l'on peut attendre de l'interopérabilité des données appuyée par les API.

181. De nouvelles méthodes visant à faciliter l'interopérabilité des données continuent toutefois d'être développées. Ainsi, Apple, Facebook, Google, Windows et Twitter œuvrent actuellement à la création d'une plateforme de portabilité des données *open source* et de service à service, à travers le projet « Data Transfer Project » (Data Transfer Project, 2018[152]). Gal et Rubinfeld (2019[26]) avancent également que le développement de la normalisation des données pourrait contribuer à renforcer l'interopérabilité, à baisser les coûts de conversion et à limiter les doublons, comme cela a été le cas dans le secteur des transports publics (tel qu'indiqué précédemment). Ils considèrent toutefois qu'une norme inefficace entraînerait des coûts induits supplémentaires et augmenterait le risque d'effets de captivité.

182. D'autres méthodes visant à permettre aux individus d'accéder aux données sans porter atteinte à la protection de la vie privée sont également en cours de développement. Les salles d'accès aux données (*open data rooms*) sont un exemple concret de ces nouveaux moyens de partager des données de consommateurs tout en assurant la protection de la vie privée (Robertson, 2020[16]). La Banque de France met ainsi son « Open Data Room » à la disposition des chercheurs. Cette salle est équipée de postes de travail donnant accès à un vaste ensemble de données granulaires anonymisées et de séries agrégées, collectées ou produites par la Banque de France (Banque de France, 2019[153]). Les bacs à sable de données constituent également une piste intéressante pour le partage de données sensibles (OCDE, 2019[12] ; Ctrl-Shift, 2019[154]). L'adoption de nouveaux cadres de gouvernance des données pourraient en outre avoir des répercussions sur la propriété et le partage de données des consommateurs, tel qu'abordé ci-dessous.

5.1.2. Autres approches de la propriété et du contrôle des données

183. Différentes solutions innovantes visant à améliorer la gouvernance des données ont été proposées pour mieux résoudre les problèmes de propriété et de contrôle des données que peuvent rencontrer les utilisateurs. Ces nouvelles approches pourraient ainsi permettre : i) d'internaliser les effets externes suscités par la demande des individus, de tirer parti de l'effet de réseau qu'ils procurent aux plateformes, et ainsi de bénéficier d'une valeur supérieure pour chaque utilisateur qui génère des données ; et ii) de faciliter les actions collectives et les changements de prestataires susceptibles de représenter des menaces concurrentielles crédibles pour les entreprises en place. À titre d'exemple, les fiducies de données ont été présentées comme un moyen de faciliter les échanges de données de manière « *loyale, sécurisée et efficace* » (Hall et Pesenti, 2017[155]). La start-up Streamr, qui propose une infrastructure permettant à ses utilisateurs de monétiser collectivement leurs données, a ainsi développé une application appelée « Swash » qui a pour objectif de faciliter l'unification des données (Chakrovorti,, 2020[27]). Autre exemple, la *Tide Foundation* permet le chiffrement des informations personnelles des consommateurs de sorte que seul la personne propriétaire des données peut y accorder l'accès, et éventuellement recevoir une rémunération en échange (Tide, 2019[156]).

184. Posner et Weyl (2019[157]) ont quant à eux proposé que les données soient considérées comme un « travail » et ont donc défendu la création de « syndicats de

travailleurs des données » agissant collectivement au nom des consommateurs afin de négocier des accords et une rémunération pour l'accès à leurs données. Citons aussi un autre projet, « Ocean Protocol », qui a pour objectif de faciliter le partage de données en s'appuyant sur une infrastructure de registre distribué autogéré de chaînes de blocs (Chakrovorti,, 2020[27]). De nouvelles solutions ont également été proposées pour améliorer la vérification et la gestion de l'identité des consommateurs, parmi lesquelles le concept d'identité auto-souveraine (voir l'Encadré 11).

Encadré 11. L'identité auto-souveraine

L'identité auto-souveraine (IAS) a été mise en avant comme un moyen possible pour les individus de gérer leur identité. L'IAS pourrait s'appuyer sur une application sur smartphone ou sur ordinateur faisant office de « portefeuille d'identité ». Les données relatives à l'identité seraient alors enregistrées sur le disque dur de l'appareil, avec éventuellement une sauvegarde supplémentaire sur autre appareil ou via une solution personnelle, mais en aucun cas conservées de manière centralisée (par exemple, dans le nuage).

Ce portefeuille d'identité serait au départ vide, doté uniquement, d'une part, d'un numéro d'identification généré automatiquement à partir d'une clé publique et, d'autre part, de la clé privée correspondante (comme un mot de passe, utilisé pour créer des signatures numériques). Dans la mesure où chaque individu crée son propre numéro d'identification, on parle alors d'« auto-souveraineté ». Ce numéro d'identification, accompagné des revendications de la personne concernée quant à son identité, pourraient alors être utilisés pour obtenir des attestations auprès des autorités compétentes.

Ces attestations pourraient alors servir à différentes fins (par exemple, pour confirmer la majorité d'un individu ou qu'il est bien titulaire d'un permis de conduire) et limiteraient donc le volume d'informations partagées avec des tiers. Pour partager les données ou attestations requises, l'utilisateur n'aurait qu'à approuver le recueil de ces informations spécifiques au tiers demandeur, par exemple par le biais d'une notification sur l'un de ses appareils.

Source : Lewis (2017[158])

185. De la même manière, la *Unique Identification Authority of India* (UIDAI) est un organisme officiel créé pour fournir à tous les habitants de l'Inde un numéro d'identification unique, appelé « Aadhaar » (UIDAI, s.d.[159]). Dans le cadre du projet « Solid », Tim Berners-Lee, fondateur de l'internet, travaille également sur une solution ayant pour objectif d'améliorer le contrôle des consommateurs sur leurs données en décentralisant la collecte de ces données et en donnant aux consommateurs la capacité d'autoriser ou non l'accès à leurs données (Berners-Lee, 2018[160]). En outre, dans certains pays comme le Japon, des « banques d'informations » sont actuellement développées pour permettre aux consommateurs de contrôler la manière dont leurs informations sont utilisées, tout en les récompensant pour le partage de ces informations (Hemmi, 2020[161]). Dans le rapport intérimaire qu'elle a établi pour son étude de marché sur les plateformes en ligne et la publicité numérique, la CMA a par ailleurs étudié différents moyens d'appuyer le développement des services de gestion des informations personnelles, des banques de données personnelles et des technologies protectrices de la vie privée (CMA, 2019[162]). Il conviendra ainsi de surveiller l'évolution de ces solutions, notamment de sorte

à garantir qu'aucun obstacle concurrentiel ou juridique ne vienne entraver leur développement ou leur adoption.

5.2. Rôle de la politique à l'égard des consommateurs

186. Tel qu'abordé dans la section 3.3.1, l'asymétrie de l'information reste l'une des possibles défaillances du marché associées à la protection de la vie privée et aux données des consommateurs. Face aux problèmes d'asymétrie de l'information, des mesures relevant de la politique à l'égard des consommateurs pourraient avoir un rôle plus déterminant que l'application du droit de la concurrence. Autrement dit, si les entreprises tirent parti de l'asymétrie de l'information pour tromper les consommateurs, des actions pourraient être engagées au titre de la politique à l'égard des consommateurs. La *Recommandation du conseil sur la protection du consommateur dans le commerce électronique* précise par exemple que les entreprises ne doivent en aucun cas soumettre les consommateurs à des pratiques trompeuses ou mensongères, y compris relativement à la collecte et à l'exploitation des données à caractère personnel des consommateurs (OCDE, 2016[163]). Ce texte établit également que les entreprises ne doivent pas mettre en œuvre de pratiques déloyales, ni appliquer des conditions contractuelles abusives (OCDE, 2016[163]). La plupart des pays membres de l'OCDE ont déjà adopté des lois de protection des consommateurs qui donnent effet à ces recommandations.

187. Ohlhausen et Okuliar (2015[164]) estiment que le droit de la consommation constitue un moyen bien plus efficace de protéger la vie privée des consommateurs que chercher à atteindre des objectifs de protection de la vie privée en s'appuyant sur l'application du droit de la concurrence. En pratique, de nombreuses autorités de la protection du consommateur ont ouvert des procédures liées aux pratiques des entreprises en matière de protection de la vie privée et des données à caractère personnel, tel que décrit dans le guide de bonnes pratiques de l'OCDE relatives aux données des consommateurs (*Good Practice Guide on Consumer Data*) (2019[13]). Dans le cas de pratiques mensongères liées à la protection de la vie privée et à la sécurité des données, on trouve plusieurs exemples aux États-Unis, où la FTC a engagé des procédures à l'encontre d'Uber (application de co-voiturage), Facebook (application de réseaux sociaux ; voir l'Encadré 12), une société de commercialisation ou encore un fournisseurs de technologie (OCDE, 2019[13]). Les pratiques trompeuses peuvent également prendre la forme de fausses déclarations par omission. Des procédures visant de telles pratiques liées aux données ont ainsi été ouvertes en Australie, au Canada, aux États-Unis, en Hongrie, en Italie (à l'encontre de Facebook ; voir l'Encadré 12), en Norvège, au Royaume-Uni et par la Commission européenne (OCDE, 2019[13]). Certaines juridictions ont par ailleurs la possibilité de prendre des mesures répressives en cas de pratiques « déloyales » en matière de données des consommateurs. De telles procédures ont ainsi pu être engagées aux États-Unis et par la Commission européenne (OCDE, 2019[13]).

Encadré 12. Mesures répressives contre les pratiques de Facebook en matière de protection de la vie privée au titre du droit de la protection du consommateur

Aux **États-Unis**, la FTC a ouvert un certain nombre de procédures à l'encontre de Facebook concernant ses pratiques en matière de protection de la vie privée et des données à caractère personnel. En 2012, l'autorité est parvenue à un règlement avec Facebook sur huit chefs d'accusation liés à des pratiques qu'elle considérait comme des méthodes de concurrence déloyale. En 2019, elle a infligé à Facebook une sanction pécuniaire de 5 milliards USD pour avoir violé l'arrêté de 2012 en trompant les

utilisateurs sur leur capacité à contrôler la confidentialité de leurs informations personnelles. La FTC a par ailleurs prononcé une ordonnance de règlement sur 20 ans afin de contraindre Facebook à revoir « *la manière dont l'entreprise prend des décisions en matière de protection de la vie privée, d'une part, en renforçant la transparence du processus décisionnel et, d'autre part, en responsabilisant Facebook par l'application de différents mécanismes de conformité* ».

Au cours de l'année 2018, en **Italie**, l'*Autorità garante della concorrenza e del mercato* (AGCM) a reconnu par deux fois Facebook responsable de pratiques commerciales déloyales, en violation du code de la consommation italien pour sa gestion de la protection de la vie privée et de la collecte de données. L'AGCM a d'abord considéré que Facebook avait trompé les utilisateurs relativement à la collecte et à l'utilisation de leurs données lors de l'étape d'inscription, estimant que les informations fournies n'étaient ni opportunes, ni claires, ni complètes. En l'espèce, l'AGCM contestait le slogan de Facebook, « C'est gratuit (et ça le restera toujours) », dans la mesure où les consommateurs fournissent leurs données en échange de l'accès à un service. Dans le second cas, elle a considéré les pratiques de partage de données de Facebook comme « agressives », en ce sens que l'entreprise partageait des données des consommateurs avec des applications et des sites internet tiers sans demander au préalable le consentement explicite des consommateurs. L'AGCM a donc infligé une amende de 5 millions EUR pour chaque infraction, pour un montant total de 10 millions EUR.

Facebook a fait appel de la décision auprès du tribunal administratif régional de Lazio, lequel a confirmé en 2020 le jugement de l'AGCM pour le premier chef d'accusation, mais annulé la décision pour le second chef, réduisant par conséquent l'amende totale à 5 millions EUR. Concernant le premier grief, le tribunal a validé l'interprétation de l'AGCM selon laquelle les données à caractère personnel peuvent être considérées comme une ressource négociable pouvant faire l'objet d'une exploitation économique, et donc pouvant constituer une « contrepartie » dans le cadre d'un contrat.

Source : FTC (2012[165]) ; FTC (2019[166]) ; FTC (2019[167]) ; AGCM (2018[168]) ; Monga (2020[169]) ; Asaro et Thiem (2020[170]), Il Tribunale Amministrivo Regionale per il Lazio (2020[171])

5.3. Rôle éventuel de la réglementation économique

188. Indépendamment du recours au droit de la concurrence, de la protection de la vie privée ou de la consommation, certains observateurs estiment que la réglementation économique pourrait éventuellement avoir un rôle à jouer pour lutter contre les défaillances du marché associées aux données des consommateurs et à la protection de la vie privée dans certains marchés reposant sur l'exploitation des données des consommateurs. Dans le cas des données au sens large, Crémer et al. (2019, p. 74[14]) concluent ainsi que :

> *Pour garantir l'accès à des données afin de promouvoir le développement de l'IA de manière générale dans l'optique d'encourager l'innovation (soit par une forme d'accès sans lien avec les activités commerciales du maître du fichier), nous pensons qu'il sera nécessaire d'instaurer un régime de droit commun en dehors du droit de la concurrence.*

189. Colangelo et Maggiolino (2018[98]) estiment également que si le problème du manque de protection des données sur les plateformes en ligne est en réalité un problème de structure du marché (notamment car de nombreuses plateformes en ligne sont présentes sur des marchés multifaces soumis à des effets de réseau, pouvant eux-mêmes entraîner la concentration du marché), une réglementation économique pourrait permettre d'apporter

une réponse plus adéquate que le droit de la concurrence. Par ailleurs, dans la mesure où il existe des externalités importantes liées à la collecte et à l'utilisation des données des consommateurs, une réglementation économique pourrait également constituer un moyen d'action plus adapté, à condition que les avantages restent supérieurs aux coûts. Par exemple, étant donné que les externalités associées à l'exploitation des données peuvent être positives ou négatives suivant la manière dont ces données sont utilisées, Gal et Rubinfeld (2019[26]) suggèrent qu'il pourrait être plus adapté de réglementer justement la manière dont les données sont utilisées (autrement dit, en limitant ou en restreignant les modes d'utilisation des données susceptibles de générer des externalités négatives).

190. La Commission européenne a ainsi adopté des législations sectorielles visant les données dans le secteur de l'automobile, des prestataires de services de paiement, des compteurs intelligents, des réseaux électriques et des systèmes de transports intelligents (Commission européenne, 2020[1]).

191. Différentes juridictions ont également examiné la possibilité de créer des services spécialisés pour déterminer le meilleur moyen de réglementer les plateformes numériques, y compris leur utilisation des données des consommateurs. Au Royaume-Uni par exemple, le rapport Furman de 2019 consacré à la libération de la concurrence sur les marchés du numérique, recommandait l'établissement d'une unité des marchés numériques (*Digital Markets Unit* ou DMU) (Furman et al., 2019[70]). Cette DMU serait intégrée à la CMA ou à l'Ofcom (ou existerait en tant qu'entité indépendante formant une passerelle entre les deux). Elle aurait pour mission d'utiliser divers instruments et cadres pour encourager la concurrence et promouvoir le choix des consommateurs dans les marchés numériques, avec à sa disposition de nouveaux pouvoirs juridiques. L'une de ses premières tâches serait d'élaborer un code de conduite, applicable à toutes les entreprises considérées comme ayant une « position de marché stratégique ». La DMU serait également chargée de permettre une plus grande mobilité des données à caractère personnel et le développement de systèmes basés sur des normes ouvertes, afin d'améliorer la concurrence et le choix du consommateur. De la même manière, aux États-Unis, le rapport Stigler (2019[172]) recommandait la création d'une autorité de régulation unique ayant pour mission de superviser les normes ouvertes et l'accès et la portabilité des données, de surveiller l'utilisation d'interfaces utilisateur trompeuses et les risques de dépendance, et enfin d'appuyer la FTC et le ministère de la Justice des États-Unis pour l'évaluation des fusions dans les marchés numériques. Il convient de noter que l'autorité danoise de concurrence et des consommateurs et l'ACCC ont toutes deux déjà mis en place de telles unités spécialisées dans les plateformes numériques au cours des deux dernières années.

5.4. Le besoin de coopération

192. Dans son rapport sur la « Problématique de la qualité dans les secteurs numériques de l'économie sans contrepartie financière », l'OCDE a mis en avant la nécessité d'une coopération et d'une coordination efficaces entre les différentes autorités lorsqu'une affaire a trait à plusieurs domaines de l'action publique. Elle précisait ainsi que (OCDE, 2018, p. 31[6]) :

> *… une séparation stricte des domaines d'action des autorités de la concurrence, de la protection des consommateurs et de la protection des données n'apporterait certainement pas des résultats optimaux, à la fois en termes de bien-être et de protection des consommateurs. C'est pourquoi il conviendrait sans doute d'appliquer ces trois politiques en parallèle […].*

193. Bien que cette observation s'appliquât au contexte des marchés sans contrepartie financière, elle s'applique tout autant lorsqu'il s'agit de garantir que les niveaux de

protection assurés et la collecte et l'utilisation des données des consommateurs profitent bien à ces consommateurs et encouragent la concurrence dans les marchés. La coopération entre les autorités de la concurrence, de la protection du consommateur et de la protection de la vie privée était également l'un des thèmes centraux de l'avis préliminaire du CEPD intitulé « Vie privée et compétitivité à l'ère de la collecte de données massives » de 2014 et de l'« Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data) » de 2016 (CEPD, 2013[30] ; CEPD, 2016[173]). Ce dernier avis recommandait un dialogue plus étroit entre les autorités de régulation et les experts, quels que soient leurs domaines de compétence, avec comme objectif de renforcer la politique de la concurrence et la protection des consommateurs, et de stimuler le marché des services protecteurs de la vie privée. Kerber (2016[174]) est même allé plus loin en défendant le développement d'une « stratégie commune » réunissant ces trois domaines de l'action publique. Une telle approche pourrait être plus facilement mise en œuvre lorsque les missions de l'autorité de la concurrence concernée sont plus vastes et incluent la protection du consommateur, la protection des données ou la régulation sectorielle, par exemple.

194. La coordination dans la gestion des problèmes de concurrence et de politique à l'égard des consommateurs est bien plus directe dans la trentaine de juridictions où ces responsabilités incombent à une seule et même autorité (Kovacic et Hyman, 2013[175]). Certaines dispositions législatives offrent également une base juridique pour la coopération entre les autorités de la concurrence, de la protection des données et de la protection du consommateur. C'est notamment le cas en Allemagne, suite aux modifications apportées à la loi contre les restrictions de la concurrence (*Gesetz gegen Wettbewerbsbeschränkungen*) entrées en vigueur en juin 2017 (Stauber, 2019[176]). L'article 50c(1) précise ainsi que les autorités fédérales et nationales chargées de la protection des données et de la concurrence ont la possibilité d'échanger des informations, y compris des données à caractère personnel et des secrets d'affaires, dans la mesure où ces informations sont nécessaires au bon exercice de leurs missions respectives, et d'utiliser ces informations dans le cadre de leurs activités. La coopération entre les autorités compétentes dans la procédure engagée par le Bundeskartellamt à l'encontre de Facebook a par exemple été déterminante. En Australie par ailleurs, la coopération a été intégrée au droit applicable aux données des consommateurs, et l'ACCC, l'OAIC et le DSB partagent la responsabilité de son application (voir l'Encadré 4).

195. D'autres méthodes moins formalisées de coopération peuvent également être mises en œuvre. Par exemple, dans son avis de 2016, le CEPD recommandait la création d'une « chambre de compensation numérique » afin de faciliter l'échange d'informations entre les autorités de régulation chargées des marchés en ligne (voir l'Encadré 13).

Encadré 13. La chambre européenne de compensation numérique

En 2016, le CEPD a publié un « Avis sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data) », dans lequel il recommandait la création d'une « chambre de compensation numérique » afin de coordonner l'application du droit dans le secteur numérique européen. Cette chambre de compensation numérique consisterait en un réseau volontaire d'autorités de régulation chargées de l'application du droit dans les marchés numériques, avec comme priorité la protection des consommateurs, des données et de la concurrence. Dans une résolution de 2017, le Parlement européen a avalisé la création et le développement de cette chambre de compensation numérique telle qu'envisagée par le CEPD, indiquant que

celle-ci pourrait « *contribuer à […] approfondir les synergies et à garantir la protection des droits et intérêts des citoyens* ».

Les principaux objectifs de cette chambre de compensation numérique sont (i) de partager des bonnes pratiques et des idées innovantes pour assurer la protection des individus dans les marchés numériques en couvrant l'ensemble des régimes de droit communs applicables ; et (ii) d'encourager la collaboration des différentes parties prenantes impliquées dans ces efforts. Entre 2017 et 2018, pas moins de quatre réunions de la chambre de compensation numérique ont été organisées par le CEPD. Depuis 2019, la chambre de compensation numérique est organisée conjointement avec le Centre de recherche information, droit et société (CRIDS) de l'université de Namur, le *Tilburg Institute for Law, Technology, and Society* (TILT) de l'université de Tilbourg et le *European Policy Centre* (EPC) à Bruxelles. La chambre de compensation numérique est ouverte et accessible à l'ensemble des autorités de régulation de l'espace numérique à travers le monde.

Source : Chambre de compensation numérique (s.d.[177]) ; CEPD (2016[173]) ; Parlement européen (2017[178]) ; CEPD (s.d.[179])

196. Les études de marché présentent également un intérêt potentiel non négligeable pour mieux comprendre les questions plus générales de politique publique dans des marchés spécifiques (OCDE, 2018[6]). Elles peuvent ainsi s'avérer particulièrement utiles pour appréhender les problèmes liés à la demande qui ne relèvent généralement pas de la compétence des autorités de la concurrence. Tel qu'exposé dans la section 4.2.3, les problèmes liés à la demande représentent un enjeu particulier en termes de protection de la vie privée, qu'ils soient liés à l'asymétrie de l'information comme aux biais comportementaux. S'appuyer sur tous les domaines d'action des politiques de la concurrence, de la protection des consommateurs et de la protection de la vie privée pourrait donc être une approche plus efficace pour apporter les améliorations nécessaires, plutôt que d'aborder la situation sous l'angle d'une seule et unique politique.

6. Conclusions

197. Ce document aborde certaines des difficultés associées à l'intégration de la question des données des consommateurs dans la politique de la concurrence et son application. Bien que les données des consommateurs soient utilisées par les entreprises depuis déjà longtemps et qu'on puisse considérer que la protection de la vie privée a toujours été un enjeu important pour les consommateurs, ces problématiques ne vont faire que s'accentuer au regard de la politique de la concurrence et de la mise en œuvre du droit de la concurrence.

198. De plus en plus de voix se font entendre pour défendre l'idée que les autorités de la concurrence devraient considérer la protection des données et de la vie privée comme un aspect concurrentiel de la qualité lors de l'évaluation des affaires de concurrence dans les marchés impliquant les données des consommateurs. En pratique, cela présente néanmoins un certain nombre de difficultés. Alors que les pressions concurrentielles devraient, au moins en théorie, favoriser la concurrence en matière de protection de la vie privée, différents obstacles liés à la demande peuvent en pratique entraver la bonne marche de la concurrence, même dans les marchés où les consommateurs déclarent accorder de l'importance à la protection de la vie privée. En effet, la compréhension qu'ont les consommateurs, d'une part, des questions de protection de la vie privée et, d'autre part, des pratiques de collecte et d'utilisation des données est souvent très limitée. Cette asymétrie de l'information pourrait mener à des problèmes d'« antisélection » dans le cadre de la

protection de la vie privée dans les marchés concernés. Le cas échéant, la réglementation relative à la protection des données et des consommateurs, et les mesures d'application correspondantes pourraient constituer une solution plus efficace que l'application directe du droit de la concurrence, particulièrement si l'objectif est de garantir un niveau minimum de protection des données. Quoi qu'il en soit, il existe des situations où les entreprises se livrent bel et bien concurrence sur la protection de la vie privée, et les autorités de la concurrence devraient prendre cet élément en compte dans leurs évaluations d'impact sur la concurrence. Cela peut notamment être le cas dans les affaires liées à la mise en œuvre de fusions, notamment si l'une des parties est considérée comme un « franc-tireur » au regard de ses pratiques de protection de la vie privée. Dans de tels cas, des enquêtes menées auprès des consommateurs et des entreprises sur l'importance de la protection de la vie privée dans le marché concerné, ainsi qu'une évaluation des réponses du marché (à la fois pour les consommateurs et les entreprises) face aux modifications du niveau de protection de la vie privée proposé, pourraient apporter nombre d'informations utiles.

199. Il existe également des situations dans lesquelles les données des consommateurs peuvent conférer un avantage concurrentiel à certains acteurs du marché. C'est notamment le cas lorsqu'une entreprise dispose d'un accès exclusif à certains types de données des consommateurs. Si une fusion devait par exemple consolider un tel avantage, il est important que cela soit pris en compte dans l'évaluation de cette fusion. Par ailleurs, si une entreprise dominante limite l'accès à ses données, cet aspect doit également être pris en compte au titre du droit de la concurrence. De la même manière, si une entreprise dominante pratique la vente liée ou groupée pour conserver sa position dominante ou en tirer parti relativement à l'accès et à l'utilisation de données des consommateurs, le droit de la concurrence doit être appliqué. L'une des principales difficultés dans ce type d'affaire réside en l'évaluation des obstacles à l'entrée dans les marchés pertinents, puisque les caractéristiques spécifiques de ces marchés devront également être prises en compte. Dans la mesure où l'accès à un ensemble particulier de données des consommateurs s'avère essentiel pour garantir la concurrence, il pourrait être possible d'invoquer la théorie des installations essentielles, dont l'application aux données des consommateurs n'a à ce jour été que très peu testée. De manière plus générale, cette possibilité reste offerte au titre du droit de la concurrence dans les situations où il existe des inquiétudes quant à l'accès aux données des consommateurs suite à une fusion ou dans les affaires d'abus de position dominante. Différentes mesures correctrices peuvent par ailleurs être adoptées par le biais d'autres domaines d'action publique, comme les politiques de protection des données et de la vie privée.

200. Ainsi, les droits relatifs à la portabilité des données peuvent permettre de favoriser la concurrence si, par leur nature et leur application, ils sont susceptibles d'avoir un impact sur les obstacles à l'entrée et les entraves liées à la demande qui menacent l'exercice de ces droits. Les coûts de mise en œuvre de la portabilité des données, mais aussi de mise en conformité, peuvent être particulièrement élevés, et les possibilités d'utilisation pour les consommateurs peuvent être limitées. Aussi, du point de vue de la concurrence, il convient d'étudier de manière plus approfondie la pertinence d'une approche ciblée de la portabilité des données. La promotion de la concurrence a également un rôle à jouer pour garantir que les réglementations relatives à la protection des données et de la vie privée n'ont pas plus largement des effets pervers sur la concurrence, notamment en augmentant les obstacles à l'entrée de manière injustifiée. Il est recommandé que ces réglementations soient évaluées après leur mise en œuvre, de sorte à déterminer leur impact sur la concurrence et sur les marchés de manière plus générale. Certains problèmes, comme l'asymétrie de l'information ou la fourniture d'informations trompeuses, devraient néanmoins être abordés sous l'angle de la politique de protection des consommateurs plutôt que de la politique de la concurrence. Reste toutefois à savoir s'il existe certains marchés dont la

structure est telle qu'une réglementation économique se révélerait plus adaptée qu'une réglementation axée sur la concurrence. Face à ces différents enjeux et arbitrages, il est essentiel que les autorités chargées de la protection des données, des consommateurs et de la concurrence partagent leurs informations et leurs idées, à la fois pour accompagner et encourager l'évolution des politiques, et pour prendre des mesures réellement efficaces.

201. Les autorités de la concurrence ont par conséquent un rôle important à jouer pour promouvoir la protection de la vie privée et garantir que l'accès aux données des consommateurs et leur utilisation offrent de réels avantages pour les consommateurs dans les marchés où ces pratiques constituent un aspect non négligeable de la concurrence. Il s'agit toutefois d'un domaine encore relativement nouveau de la politique de la concurrence, où les théories du préjudice applicables n'ont que très peu été mises à l'épreuve. Par ailleurs, comme pour d'autres évaluations d'impact sur la concurrence prenant en compte l'aspect de qualité, les modèles économiques restent moins développés et acceptés que ceux basés sur les effets de prix. Au cours des prochaines années, les autorités de la concurrence devront continuer leurs efforts pour mieux comprendre les dynamiques concurrentielles dans les marchés impliquant les données des consommateurs. Elles devront également continuer de collaborer et de coopérer avec les organismes chargés de l'application de la loi et de l'élaboration des politiques dont les responsabilités couvrent notamment la protection des données et la politique à l'égard des consommateurs.

Références

ACCC (2019), *Customer Loyalty Schemes: Final Report*, https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF. [40]

ACCC (2019), *Digital Platforms Inquiry: Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf. [58]

ACCC (s.d.), *Consumer data right (CDR)*, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0. [35]

Acquisti, A., C. Taylor et L. Wagman (2016), « The Economics of Privacy », *Journal of Economic Literature*, vol. 54/2, pp. 442-492, http://dx.doi.org/10.1257/jel.54.2.442. [15]

Adams, M. (2014), *The Origins of Personal Data and its Implications for Governance*, The Information Accountability Foundation, http://dx.doi.org/10.2139/ssrn.2510927. [187]

AGCM (2018), *Facebook – condivisione dati con terzi*. [168]

Akerlof, G. (1970), « The Market for ''Lemons'': Quality Uncertainty and the Market Mechanism », *The Quarterly Journal of Economics*, vol. 84/3, pp. 488-500, http://links.jstor.org/sici?sici=0033-5533%28197008%2984%3A3%3C488%3ATMF%22QU%3E2.0.CO%3B2-6 (consulté le 6 juillet 2017). [67]

altexsoft (2018), *Public Transportation Apps' APIs and Platforms: Maps, Scheduling, Trip Planning, and Mobile Ticketing*, https://www.altexsoft.com/blog/engineering/public-transportation-apps-apis-and-platforms-maps-scheduling-trip-planning-and-mobile-ticketing/. [150]

Anderson, K. (2019), « Mass Market Consumer Fraud in the United States: A 2017 Update », *Staff Report of the Bureau of Economics*, Federal Trade Commission. [62]

Arthur, C. (2011), *What's a zettabyte? By 2015, the internet will know, says Cisco*, https://www.theguardian.com/technology/blog/2011/jun/29/zettabyte-data-internet-cisco. [2]

Article 29 Data Protection Working Party (2016), *Guidelines on the right to data portability*. [149]

Asaro, A. et T. Thiem (2020), *Facebook is not free: The regional Administrative Court of Lazio affirms the commercial value of the personal data of the social network users*, https://www.lexology.com/library/detail.aspx?g=7daa5f60-dfe0-41dd-9a15-34aa7e499a2e. [170]

Autorité de la concurrence (2014), *Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité*, https://www.autoritedelaconcurrence.fr/sites/default/files/2019-10/14mc02.pdf. [94]

Auxier, B. et al. (2019), *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. [113]

Bakhoum, M. et al. (dir. pub.) (2018), *The Rise of Big Data and the Loss of Privacy*, Springer, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795992. [101]

Banco Central do Brasil (2019), *The revitalized Positive Credit Report has become fully operational*, https://www.bcb.gov.br/en/pressdetail/2279/nota. [103]

Banque de France (2019), *Open Data Room*, https://www.banque-france.fr/statistiques/acces-aux-donnees-granulaires/open-data-room. [153]

Bartz, D. et D. Lawsky (2008), *Google clout seen aiding Microsoft antitrust OK*, https://www.reuters.com/article/businesspro-microsoft-yahoo-antitrust-dc/google-clout-seen-aiding-microsoft-antitrust-ok-idUSN0144485520080202. [186]

Beales, J. (2019), *Public Goods, Private Information: Providing an Interesting Internet*, p. 14, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/04/AC-April-02.pdf. [185]

Beal, V. (2008), *What are Internet Cookies and What Do They Do?*, Webopedia, https://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp (consulté le 11 janvier 2018). [41]

Berners-Lee, T. (2018), *One Small Step for the Web…*, https://inrupt.com/blog/one-small-step-for-the-web. [160]

Binns, R. et E. Biettib (2019), « Dissolving privacy, one merger at a time: Competition, data and third party tracking », *Computer Law & Security Review*, https://doi.org/10.1016/j.clsr.2019.105369. [50]

Binns, R. et al. (2018), *Third Party Tracking in the Mobile Ecosystem*, http://dx.doi.org/10.1145/3201064.3201089. [47]

Boerman, S., S. Kruikemeier et F. Zuiderveen Borgesius (2017), « Online Behavioral Advertising: A Literature Review and Research Agenda », *Journal of Advertising*, vol. 46/3, pp. 363-376, http://dx.doi.org/10.1080/00913367.2017.1339368. [44]

Bundeskartellamt (2019), *Bundeskartellamt prohibits Facebook from combining user data from different sources*, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html. [96]

Bundeskartellamt (2019), *Decision of the Bundeskartellamt B6-22/16 regarding Facebook*, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5. [95]

Bundeskartellamt et Autorité de la concurrence (2016), *Competition Law and Data*, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html. [69]

CADE (2016), *CADE approves with restrictions joint venture between banks in the sector of credit information services*, http://www.cade.gov.br/cade_english/press-releases/cade-approves-with-restrictions-joint-venture-between-banks-in-the-sector-of-credit-information-services. [104]

Calgigo (2017), *The Clock is Ticking: The Truth About GDPR Compliance*, https://calligo.cloud/resources/ebook/the-truth-about-gdpr-compliance/. [130]

Calo, R. (2013), « Digital Market Manipulation », *The George Washington Law Review*, vol. 82/4, pp. 995-1051, http://www.gwlr.org/wp-content/uploads/2014/10/Calo_82_41.pdf (consulté le 30 janvier 2018). [63]

Calo, R. et A. Rosenblat (2017), « The Taking Economy: Uber, Information, and Power », *Columbia Law Review*, vol. 117, http://dx.doi.org/10.1111/soc4.12493. [64]

Campbell, J., A. Goldfarb et C. Tucker (2015), « Privacy Regulation and Market Structure », *Journal of Economic & Management Strategy*, vol. 24/1, pp. 47-73, http://dx.doi.org/10.1111/jems.12079. [133]

Carrascal, J. (2011), *Your browsing behavior for a Big Mac: Economics of Personal Information*, https://www.researchgate.net/publication/51968495_Your_browsing_behavior_for_a_Big_Mac_Economics_of_Personal_InformationOnline. [184]

CE (2018), *Apple/Shazam*, https://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf. [92]

CE (2016), *Concentrations: la Commission autorise, sous condition, le rachat de LinkedIn par Microsoft*, https://ec.europa.eu/commission/presscorner/detail/fr/ip_16_4284. [90]

CE (2016), *Sanofi / Google / DMI JV*, https://ec.europa.eu/competition/mergers/cases/decisions/m7813_479_2.pdf. [91]

CEPD (2016), *Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (Big Data)*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_fr.pdf. [173]

CEPD (2013), *Compétitivité à l'ère de la collecte de données massives : l'interaction entre le droit à la protection des données, le droit de la concurrence et la protection des consommateurs dans l'économie numérique*, https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_fr. [30]

CEPD (s.d.), *Mégadonnées et « Digital Clearinghouse »*, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_fr. [179]

Chakrovorti,, B. (2020), *Why It's So Hard for Users to Control Their Data*, https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data. [27]

Chiou, L. et C. Tucker (2017), *Search Engines and Data Retention: Implications for Privacy and Antitrust*, https://www.nber.org/papers/w23815. [109]

Chivot, E. et D. Castro (2019), *The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy*, https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/. [138]

Choi, J., D. Jeon et B. Kim (2019), « Privacy and personal data collection with information externalities », *Journal of Public Economics*, vol. 173, https://doi.org/10.1016/j.jpubeco.2019.02.001. [68]

Christensen, L. et al. (2013), *The Impact of the Data Protection Regulation in the E.U.*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf. [132]

Cisco (2019), *Consumer Privacy Report: The growing imperative of getting of getting data privacy right*, https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf. [112]

CMA (2019), *Appendix L: Potential approaches to improving personal data mobility*, https://assets.publishing.service.gov.uk/media/5df9efa2ed915d093f742872/Appendix_L_Potential_approaches_to_improving_personal_data_mobility_FINAL.pdf#page=10. [162]

CMA (2016), *Energy Market Investigation*, https://assets.publishing.service.gov.uk/media/5773de34e5274a0da3000113/final-report-energy-market-investigation.pdf. [93]

CMA (2015), *The commercial use of consumer data*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf. [28]

Cohen, J. (2013), « What Privacy is For », *Havard Law Review*, vol. 126, p. 1904, https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf. [65]

Colangelo, G. et M. Maggiolino (2018), « Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S. », *Stanford Law School and the University of Vienna School of Law TTLF Workin*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125490. [98]

Commission européenne (2020), *Une stratégie européenne pour les données*, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_fr.pdf. [1]

Commission européenne (2017), *Concentrations : la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp*, https://ec.europa.eu/commission/presscorner/detail/fr/ip_17_1369. [83]

Commission européenne (2016), *Cas n° M.8124 – Microsoft/LinkedIn*, https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf. [89]

Commission européenne (2013), *Cas n° COMP/M.7217 - Facebook/WhatsApp*, https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf. [80]

Commission européenne (2012), *Cas n° COMP/M.6314 – Telefónica UK/Vodafone UK/Everything Everywhere/JV*, https://ec.europa.eu/competition/mergers/cases/decisions/m6314_20120904_20682_2898627_EN.pdf. [76]

Commission européenne (2008), *Cas n° COMP/M.4731 - Google/ DoubleClick*, https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_fr.pdf. [72]

Commission, F. (dir. pub.) (2013), *FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition*, https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed. [85]

Condorelli, D. et J. Padilla (2019), *Harnessing Platform Envelopment Through Privacy Policy Tying*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504025. [71]

Cooper, J. (2013), *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, https://www.law.gmu.edu/assets/files/publications/working_papers/1339PrivacyandAntitrust.pdf. [125]

Costa-Cabral, F. et O. Lynskey (2017), « Family ties: the intersection between data protection and competition in EU Law », *Common Market Law Review*, vol. 54/1, pp. 11-50, http://www.kluwerlawonline.com/abstract.php?area=Journals&id=COLA2017002. [105]

Cour de justice de l'Union européenne (2006), *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62005CJ0238&from=EN. [102]

CPI (2019), *Germany: Facebook succeeds in blocking German ban on data collection*, https://www.competitionpolicyinternational.com/germany-cartel-office-to-take-facebook-case-to-high-court/. [97]

Crémer, J., Y. de Montjoye et H. Schweitzer (2019), *Competition policy for the digital era*, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. [14]

Ctrl-Shift (2019), *Personal Data Mobility Sandbox report*, https://www.ctrl-shift.co.uk/news/2019/06/17/release-of-data-mobility-infrastructure-sandbox-report/. [154]

Ctrl-Shift (2018), *Data Mobility: The personal data portability growth opportunity for the UK economy*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/Data_Mobility_report.pdf. [146]

Data Transfer Project (2018), *Data Transfer Project Overview and Fundamentals*, https://datatransferproject.dev/dtp-overview.pdf. [152]

Department for Business, Innovation & Skills (2011), *The midata vision of consumer empowerment*, https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment (consulté le 20 February 2020). [33]

Department of Justice (2010), *Justice Department Requires Ticketmaster Entertainment Inc. to Make Significant Changes to Its Merger with Live Nation Inc.*, https://www.justice.gov/opa/pr/justice-department-requires-ticketmaster-entertainment-inc-make-significant-changes-its. [127]

Digital Clearinghouse (s.d.), *Digital Clearinghouse*, https://www.digitalclearinghouse.org/. [177]

Diker Vanberg, A. et M. Ünver (2017), « The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? », *European Journal of Law and Technology*, vol. 8/1, http://ejlt.org/article/view/546/727. [129]

EC (2008), *TomTom/Tele Atlas*, https://ec.europa.eu/competition/mergers/cases/decisions/m4854_20080514_20682_en.pdf. [75]

Egin, E. (2019), *Charting a Way Forward: Data Portability and Privacy*, Facebook, https://iapp.org/media/pdf/fb_whitepaper_sep_2019.pdf. [147]

Engels, B. (2016), « Data portability among online platforms », *Internet Policy Review*, vol. 5/2, http://dx.doi.org/10.14763/2016.2.408. [61]

Esayas, S. (2018), *Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232701. [122]

Ezrachi, A. et V. Roberston (2019), « Competition, Market Power and Third-Party Tracking », *World Competition*, vol. 42/1, pp. 5-20, https://www.kluwerlawonline.com/abstract.php?area=Journals&id=WOCO2019002. [49]

Farrell, J. (2012), « Can privacy be just another good? », *Journal on Telecommunications and High Technology Law*, vol. 10, pp. 251-265, http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Farrell.PDF. [121]

FCA (2015), *Making current account switching easier: The effectiveness of the Current AccountSwitch Service (CASS) and evidence on account number portability*, https://www.fca.org.uk/publication/research/making-current-account-switching-easier.pdf. [144]

Federal Trade Commission (2007), *Statement of the Federal Trade Commission concerning Google/DoubleClick*, https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf. [73]

fieldfisher (dir. pub.) (2019), *CCPA Blog Series, Part 2: Rethinking access and data portability rights*, https://privacylawblog.fieldfisher.com/2019/ccpa-blog-series-part-2-rethinking-access-and-data-portability-rights. [36]

Forrest, K. (2019), *Big Data and Online Advertising: Emerging Competition Concerns*, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/04/AC-April-02.pdf. [107]

FTC (2019), *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (consulté le 17 February 2020). [167]

FTC (2019), *Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, Inc.*, https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf. [166]

FTC (2017), *Cross-Device Tracking*, https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (consulté le 26 mars 2018). [43]

FTC (2013), *Early Termination Notice: 20140457: Google Inc.; Nest Labs, Inc.*, https://www.ftc.gov/enforcement/premerger-notification-program/early-termination-notices/20140457. [86]

FTC (2012), *FTC Approves Final Settlement With Facebook: Facebook Must Obtain Consumers' Consent Before Sharing Their Information Beyond Established Privacy Settings*, https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook (consulté le 17 February 2020). [165]

FTC (2012), *FTC Closes Its Investigation Into Facebook's Proposed Acquisition of Instagram Photo Sharing Program*, https://www.ftc.gov/news-events/press-releases/2012/08/ftc-closes-its-investigation-facebooks-proposed-acquisition. [79]

Furman, J. et al. (2019), *Unlocking digital competition: Report of the Digital Competition Expert Panel*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [70]

Gal, M. et O. Aviv (2020), « The Competitive Effects of the GDPR », *Journal of Competition Law and Economics*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444. [110]

Gal, M. et D. Rubinfeld (2019), *Data Standardization*, pp. 737-770, https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-GalRubinfeld-1.pdf. [26]

Gilbert, P. et R. Pepper (2015), *Privacy Considerations in European Merger Control: A Square Peg for a Round Hole*, Competition Policy International, https://www.competitionpolicyinternational.com/assets/Uploads/PepperGilbertMay-152.pdf. [52]

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. [77]

Google (2018), *Introducing Data Transfer Project: an open source platform promoting universal data portability*, https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html. [148]

Graef, I., J. Verschakelen et P. Valcke (2013), « Putting the right to data portability into a competition law perspective », *Law: The Journal of the Higher School of Economics, Annual Review.*, https://www.researchgate.net/publication/281092445_Putting_the_right_to_data_portability_into_a_competition_law_perspective. [128]

Greif, B. (2018), *Study: Google Is the Biggest Beneficiary of the GDPR*, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr. [137]

GTFS (s.d.), *GTFS: Making Public Transit Data Universally Accessible*, https://gtfs.org/. [151]

Hall, D. et J. Pesenti (2017), *Growing the Artificial Intelligence Industry in the UK*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf. [155]

Haucap, J. (2019), *Data protection and antitrust: new types of abuse cases? An economist's view in light of the German Facebook decision*, Competition Policy International, pp. 24-29, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [126]

Hemmi, J. (2020), *Japan's 'information banks' to let users cash in on personal data*, https://asia.nikkei.com/Business/Business-trends/Japan-s-information-banks-to-let-users-cash-in-on-personal-data. [161]

Honey, K., P. Chrousos et T. Black (2016), *My Data: Empowering All Americans with Personal Data Access*, https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access (consulté le 20 février 2020). [31]

Hoofnagle, C. et J. Whittington (2014), « Free: Accounting for the Costs of the Internet's Most Popular Price », *UCLA Law Review*, vol. 61, pp. 606-670, https://www.uclalawreview.org/pdf/61-3-2.pdf. [117]

Höppner, T. (2019), *Data Exploiting as an Abuse of Dominance: The German Facebook Decision*, Hausfeld, https://www.hausfeld.com/news-press/data-exploiting-as-an-abuse-of-dominance-the-german-facebook-decision. [100]

Hull, G. (2014), « Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data », *Ethics and Information Technology*, vol. 17/2, pp. 89-101, http://dx.doi.org/10.2139/ssrn.2533057. [116]

IAB (2013), *Cookies on Mobile 101*, https://www.iab.com/wp-content/uploads/2015/07/CookiesOnMobile101Final.pdf (consulté le 26 mars 2018). [42]

Il Tribunale Amministrativo Regionale per il Lazio (2020), *Altroconsumo, National Consumers' Union and Citizen's Defence Movement v. Facebook*, https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=tar_rm&nrg=201815288&nomeFile=202000261_01.html&subDir=Provvedimenti. [171]

ISO/IEC (2018), *Privacy enhancing data de-identification terminology and classification of techniques*, http://www.iso.org/standard/69373.html. [23]

Jones Harbour, P. (2007), *Dissenting Statement of Commissioner Pamela Jones Harbour: In the Matter of Google/DoubleClick*, https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf. [74]

Jones Harbour, P. et T. Koslov (2010), « Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets », *Antitrust Law Journal*, vol. 76/3, pp. 769-797, https://www.jstor.org/stable/40843729?seq=1. [106]

Këllezi, P. (2019), *Data Protection and Competition Law: Non-Compliance as Abuse of Dominant Position*, p. 343, https://ssrn.com/abstract=3503860. [99]

Kemp, K. (2019), « Concealed Data Practices and Competition Law: Why Privacy Matters », *University of New South Wales Law Research Series*, vol. 53/Research Paper No. 19-53, http://dx.doi.org/10.2139/ssrn.3432769. [17]

Kerber, W. (2019), « Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data », *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 9, pp. 310-331, https://www.jipitec.eu/issues/jipitec-9-3-2018/4807/JIPITEC_9_3_2018_310_Kerber. [51]

Kerber, W. (2016), « Digital markets, data, and privacy: competition law, consumer law and data protection », *Journal of Intellectual Property Law & Practice*, p. jpw150, http://dx.doi.org/10.1093/jiplp/jpw150. [174]

Kokolakis, S. (2017), « Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon », *Computers & Security*, vol. 64, pp. 122-134, http://dx.doi.org/10.1016/j.cose.2015.07.002. [119]

Körber, T. (2018), « Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law », *NZKart 2016*, pp. 303-348, https://ssrn.com/abstract=31122. [59]

Kovacic, W. et D. Hyman (2013), « Competition Agencies with Complex Policy Portfolios: Divide or Conquer? », *GW Law Faculty Publications & Other Works*, p. 631, https://scholarship.law.gwu.edu/faculty_publications/631/. [175]

Lambretch, A. et C. Tucker (2017), *Can Big Data Protect a Firm from Competition?*, https://www.competitionpolicyinternational.com/wp-content/uploads/2017/01/CPI-Lambrecht-Tucker.pdf. [60]

Lewis, A. (2017), *A gentle introduction to self-sovereign identity*, https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/. [158]

Libert, T., L. Graves et R. Nielsen (2018), *Changes in Third-Party Content on European News Websites after GDPR*, https://reutersinstitute.politics.ox.ac.uk/our-research/changes-third-party-content-european-news-websites-after-gdpr (consulté le 20 February 2020). [136]

Lynskey, O. (2018), *Non-price Effects of Mergers*, Éditions OCDE, https://one.oecd.org/document/DAF/COMP/WD(2018)70/en/pdf. [82]

Lyons, D. (2018), *GDPR: Privacy as Europe's tariff by other means?*, https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/. [140]

Lyons, S. (2006), *Measuring the Benefits of Mobile Number Portability*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.571.9222&rep=rep1&type=pdf. [143]

Maggiolino, M. et G. Ferrari (2020), *Can Digital Data be Replaced? Data*, Competition Policy International, p. 37, https://www.competitionpolicyinternational.com/wp-content/uploads/2020/02/AC-February-II.pdf. [56]

Manne, G. et R. Sperry (2015), « The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework », *CPI Antitrust Chronicle*, vol. 2, https://www.competitionpolicyinternational.com/assets/Uploads/ManneSperryMay-152.pdf. [111]

Marr, B. (2016), *What Is The Difference Between Artificial Intelligence And Machine Learning?*, https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/. [55]

Marthews, A. et C. Tucker (2019), *Privacy policy and competition*, https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf. [134]

Moazed, A. (2019), *How GDPR is Helping Big Tech and Hurting the Competition*, https://www.applicoinc.com/blog/how-gdpr-is-helping-big-tech-and-hurting-the-competition/. [29]

Monga, G. (2020), *Italian Court says that personal data submitted to Facebook are economic assets*, https://www.mmlex.it/en/magazine/italian-administrative-court-lazio-confirms-personal-data-are-economic-asset. [169]

Nicholas, G. et M. Weinberg (2019), *Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?*, https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition. [141]

Norberg, P., D. Horne et D. Horne (2007), « The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors », *The Journal of Consumer Affairs*, vol. 41/1, pp. 100-126, http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x. [118]

OCDE (2020), *Effets conglomeraux des fusions*, http://www.oecd.org/fr/daf/concurrence/effets-conglomeraux-des-fusions.htm. [10]

OCDE (2020), *Perturbation numérique des marchés financiers*, https://www.oecd.org/fr/daf/concurrence/perturbation-numerique-des-marches-financiers.htm. [8]

OCDE (2020), *Start-ups, killer acquisitions and merger control*, http://www.oecd.org/daf/competition/start-ups-killer-acquisitions-and-merger-control.htm. [9]

OCDE (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Éditions OCDE, http://dx.doi.org/10.1787/276aaca8. [12]

OCDE (2019), *Good practice guide on consumer data*, Éditions OCDE, http://dx.doi.org/10.1787/20716826. [13]

OCDE (2019), *Online Advertising: Trends, benefits and risks for consumers*, http://dx.doi.org/10.1787/20716826. [45]

OCDE (2019), *Recommandation du Conseil sur l'intelligence artificielle*. [53]

OCDE (2018), *IoT measurement and applications*, Éditions OCDE, http://dx.doi.org/10.1787/20716826. [21]

OCDE (2018), *Non-price effects of mergers*, https://www.oecd.org/fr/daf/concurrence/non-price-effects-of-mergers.htm (consulté le 14 February 2020). [5]

OCDE (2018), *Personalised Pricing in the Digital Era*, https://www.oecd.org/daf/competition/personalised-pricing-in-the-digital-era.htm (consulté le 14 February 2020). [7]

OCDE (2018), *Perspectives de l'économie numérique de l'OCDE 2017*, Éditions OCDE, Paris, https://dx.doi.org/10.1787/9789264282483-fr. [20]

OCDE (2018), *Quality considerations in the zero-price economy*, https://www.oecd.org/daf/competition/quality-considerations-in-the-zero-price-economy.htm (consulté le 14 February 2020). [6]

OCDE (2018), *Rethinking Antitrust Tools for Multi-Sided Platforms*, https://www.oecd.org/daf/competition/Rethinking-antitrust-tools-for-multi-sided-platforms-2018.pdf. [108]

OCDE (2016), *Big data: Bringing competition policy to the digital era*, https://www.oecd.org/fr/concurrence/big-data-bringing-competition-policy-to-the-digital-era.htm (consulté le 14 February 2020). [4]

OCDE (2016), *Recommandation du conseil sur la protection du consommateur dans le commerce électronique*, Éditions OCDE, Paris, https://dx.doi.org/10.1787/9789264255272-fr. [163]

OCDE (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OCDE, Paris, https://dx.doi.org/10.1787/9789264229358-en. [3]

OCDE (2015), *Perspectives de l'économie numérique de l'OCDE 2015*, Éditions OCDE, Paris, https://dx.doi.org/10.1787/9789264243767-fr. [19]

OCDE (2013), *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, Éditions OCDE, http://dx.doi.org/10.1787/20716826. [18]

OCDE (2013), *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Éditions OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188. [11]

Ocello, E., C. Sjödin et A. Subočs (2015), *What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case*, Commission européenne, https://ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf. [81]

OFT (2012), *Anticipated acquisition by Facebook Inc of Instagram Inc*, https://webarchive.nationalarchives.gov.uk/20160815232112/https://assets.publishing.service.gov.uk/media/555de2e5ed915d7ae200003b/facebook.pdf. [78]

Ohlhausen, M. (2019), *Privacy and Competition: Friends, Foes, or Frenemies?*, Competition Policy International, pp. 14-18, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [88]

Ohlhausen, M. et A. Okuliar (2015), « Competition, Consumer Protection, and the Right [Approach] to Privacy », *Antitrust Law Journal*, vol. 80/1, pp. 121-156, https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf. [164]

Open Banking (s.d.), *Open Banking*, https://www.openbanking.org.uk/. [34]

Park, M. (2011), « The Economic Impact of Wireless Number Portability », *The Journal of Industrial Economics*, vol. 59/4, pp. 714-745, https://onlinelibrary.wiley.com/doi/full/10.1111/j.1467-6451.2011.00471.x. [142]

Parlement européen (2017), *Rapport sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi*, https://www.europarl.europa.eu/doceo/document/A-8-2017-0044_FR.html. [178]

PCAST (2013), *Big Data and Privacy: A Technological Perspective*. [24]

Pecman, J., P. Johnson et J. Reisler (2020), *Essential facilities fallacy: Big tech, winner-take-all markets, and anticompetitive effects*, Competition Policy International, p. 21, https://www.competitionpolicyinternational.com/wp-content/uploads/2020/02/AC-February-II.pdf. [57]

Petit, N. (2019), *Are « FANGs » Monopolies? A Theory of Competition Under Uncertainty*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3414386. [183]

Picker, R. (2008), « Competition and Privacy in Web 2.0 and the Cloud », *Northwestern University Law Review Colloquy*, vol. 103/1, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1147&context=journal_articles. [135]

Posner, E. et E. Weyl (2019), *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*, Princeton University Press. [157]

Preibusch, S., D. Kübler et A. Beresford (2013), « Price versus privacy: an experiment into the competitive advantage of collecting less personal information », *Electronic Commerce Research*, vol. 13, pp. 423–455, https://link.springer.com/article/10.1007/s10660-013-9130-3. [120]

Productivity Commission (2017), *Data Availability and Use*, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf. [188]

Purra, J. et N. Carlsson (2016), *Third-Party Tracking on the Web: A Swedish Perspective*, http://dx.doi.org/10.1109/LCN.2016.14. [48]

PWC (2017), *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html. [131]

Rich, J. (2013), *Letter to Facebook and WhatsApp*, https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf. [84]

Robertson, V. (2020), « Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data », *Common Market Law Review*, vol. 57, pp. 161–189, https://ssrn.com/abstract=3408971. [16]

RSA (2019), *RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses*, https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf. [114]

Rubinfeld, D. et M. Gal (2017), *Access Barriers to Big Data*, p. 339, https://arizonalawreview.org/pdf/59-2/59arizlrev339.pdf. [37]

Ryte (2019), *Tracking Pixel*, https://en.ryte.com/wiki/Tracking_Pixel#What_is_a_tracking_pixel.3F. [46]

Solove, D. (2013), « Privacy Self-Management and the Consent Dilemma », *Harvard Law Review*, vol. 126, pp. 1880-1903, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018. [182]

Srinivasan, D. (2019), « The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy », *Berkeley Business Law Journal*, vol. 16/1, p. 39, https://lawcat.berkeley.edu/record/1128876?ln=en. [124]

Statistica (2020), *Internet of Things - number of connected devices worldwide 2015-2025*, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [22]

Stauber, P. (2019), *Facebook's Abuse Investigation in Germany and Some Thoughts on Cooperation Between Antitrust and Data Protection Authorities*, Competition Policy International, pp. 36-43, https://www.competitionpolicyinternational.com/wp-content/uploads/2019/02/AC_February_2.pdf. [176]

Stigler Committee (2019), *Stigler Committee on Digital Platforms, Final Report*, https://research.chicagobooth.edu/stigler/media/news/committee-on-digitalplatforms-final-report. [172]

Stucke, M. (2018), *Should We Be Concerned About Data-opolies?*, p. 275, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144045. [66]

Stucke, M. et A. Grunes (2016), *Big Data and Competition Policy*, Oxford University Press. [25]

Swire, P. et Y. Lagos (2013), « Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique », *Maryland Law Review*, vol. 72/3, pp. 335-380, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2159157. [139]

Thompson, W., H. Li et A. Bolen (s.d.), *Artificial intelligence, machine learning, deep learning and beyond: Understanding AI technologies and how they lead to smart applications*, https://www.sas.com/en_us/insights/articles/big-data/artificial-intelligence-machine-learning-deep-learning-and-beyond.html. [54]

Tide (2019), *The Personal Data Economy: Technical Whitepaper*, https://tide.org/Tide_Whitepaper.pdf. [156]

Trustpilot (2018), *Open Banking expected to contribute over £1 Billion annually to UK economy supporting 17,000 new jobs*, http://press.trustpilot.com/news/2018/2/26/open-banking-expected-to-contribute-over-1-billion-annually-to-uk-economy-supporting-17000-new-jobs. [145]

Turow, J. (2017), *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, Yale University Press. [38]

Turow, J. (2003), *Americans Online Privacy: The System Is Broken*, The Annenberg Public Policy Center of the University of Pennsylvania, http://repository.upenn.edu/asc_papers (consulté le 8 août 2017). [181]

Turow, J. et al. (2009), « Americans Reject Tailored Advertising and Three Activities That Enable It », vol. 9, http://dx.doi.org/10.2139/ssrn.1478214. [180]

UIDAI (s.d.), *About UIDAI*, https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html. [159]

United States Department of Energy (s.d.), *Green Button: Open Energy Data*, https://www.energy.gov/data/green-button. [32]

United States v. Bazaarvoice (2014), *Competitive Impact Statement*, https://www.justice.gov/atr/case-document/file/488826/download. [87]

Waehrer, K. (2016), *Online Services and the Analysis of Competitive Merger Effects in Privacy Protections and Other Quality Dimensions*, http://dx.doi.org/10.2139/ssrn.2701927. [123]

Walters, R., B. Zeller et L. Trakman (2018), *Personal Data Law and Competition Law - Where is it Heading?*, pp. 18-73, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275832. [115]

Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs. [39]