



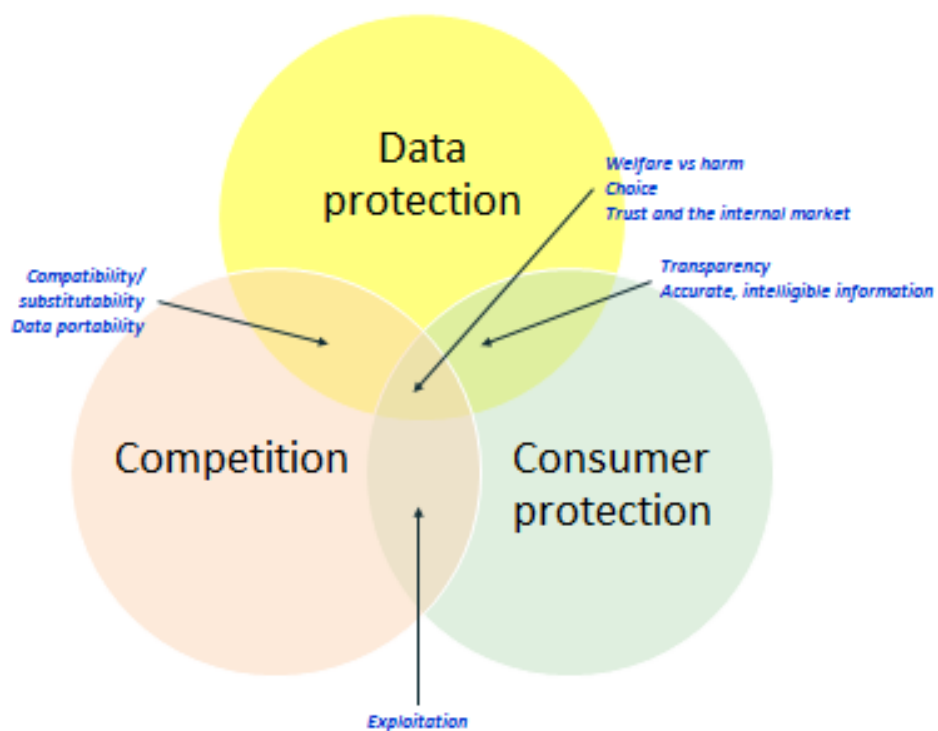
LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Avis préliminaire du Contrôleur européen de la protection des données

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

mars 2014



Data protection	Protection des données
Compatibility/substitutability	Compatibilité / substituabilité
Data portability	Portabilité des données
Competition	Concurrence
Exploitation	Exploitation
Consumer protection	Protection des consommateurs
Transparency	Transparence
Accurate, intelligible information	Informations exactes et intelligibles
Welfare vs harm	Bien-être / atteinte
Choice	Choix
Trust and the internal market	Confiance et marché intérieur

Résumé

Les approches de l'Union européenne en matière de protection des données, de concurrence et de protection des consommateurs ont des objectifs communs, notamment la promotion de la croissance, de l'innovation et du bien-être des consommateurs individuels. En pratique, cependant, la collaboration entre les décideurs politiques dans ces domaines est limitée.

Certains services numériques dirigent la forte croissance vers l'économie numérique. Nombre de ces services sont commercialisés comme étant «gratuits», mais ils requièrent en réalité un paiement sous la forme d'informations personnelles des consommateurs. Une enquête sur les coûts et avantages de ces échanges, tant pour les consommateurs que pour les entreprises, se fait attendre depuis longtemps.

Un dialogue plus étroit entre les législateurs et les experts au-delà des frontières politiques peut non seulement contribuer à la mise en œuvre des règles de concurrence et de protection des consommateurs, mais également stimuler le marché de services qui renforcent la protection de la vie privée.

Table des matières

1. Introduction.....	6
2. Données massives, données à caractère personnel: le carburant de l'économie numérique	8
2.1. Les données massives à caractère personnel, un atout.....	9
2.2. Une monnaie pour l'achat de services «gratuits».....	11
2.3. Des modèles d'entreprise conçus pour s'emparer de la valeur des données massives à caractère personnel.....	11
2.4. Un marché sous-développé de services renforçant la protection de la vie privée.....	12
3. Cadre juridique.....	13
3.1. Protection des données	13
3.1.1. Le droit fondamental à la protection des données à caractère personnel.....	13
3.1.2. Personnes soumises à des obligations en vertu des règles en matière de protection des données	15
3.1.3. Finalités légitimes et compatibles du traitement de données.....	16
3.1.4. Consentement et droit à l'information, droit d'accès aux données et droit à la portabilité des données.....	16
3.1.5. Contrôle, mise en œuvre, sanctions et accès aux voies de recours en cas de violations.....	18
3.2. Concurrence	19
3.2.1. Objectifs des règles européennes de concurrence.....	19
3.2.2. Domaine d'application des règles de concurrence et pouvoir de marché.....	20
3.2.3. Définition du marché pertinent	21
3.2.4. La notion de bien-être du consommateur dans l'application des règles de concurrence	21
3.2.5. Supervision, exécution, sanctions et accès aux voies de recours en cas de violations.....	26
3.3. Protection des consommateurs	27
3.3.1. L'exigence de garantir un niveau élevé de protection des consommateurs.....	27
3.3.2. Obligations d'équité et de fourniture d'informations exactes.....	27
3.3.3. Supervision, exécution, sanctions et accès aux voies de recours en cas de violations.....	29
4. Interfaces entre le droit de la concurrence, la protection des consommateurs et la protection des données.....	30
4.1. Les marchés pertinents et le pouvoir de marché dans l'économie numérique.....	30
4.1.1. Les marchés de services payés au moyen d'informations personnelles	31
4.1.2. Mesurer le pouvoir du marché numérique	32
4.2. Pouvoir du marché numérique et considérations relatives au bien-être des consommateurs	33

4.2.1.	Appréciation de concentrations.....	33
4.2.2.	Accès aux marchés et intrant de concurrents	35
4.2.3.	La protection des données, facteur du bien-être des consommateurs	36
4.2.4.	Voies de recours contre des décisions en matière de concurrence	36
4.3.	Exécution conjointe destinée à faciliter une «course vers le sommet» en matière de normes de sécurité.....	37
4.3.1.	Favoriser la vie privée comme avantage concurrentiel.....	38
4.3.2.	Choix du consommateur, consentement et transparence	39
4.3.3.	Contrôle de leurs propres informations par les individus	42
4.4.	Supervision et mise en œuvre.....	42
5.	Conclusion: poursuivre l'étude et la discussion.....	43

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

1. Introduction

1. L'économie numérique présente de nombreux avantages pour les consommateurs et les citoyens. Les services numériques offrent une occasion inédite de nouer des relations sociales, d'innover et de résoudre efficacement les problèmes. Parallèlement, les utilisateurs de ces services divulguent énormément d'informations les concernant. Le volume et la diversité des données générées ne peuvent être pris en charge par des technologies traditionnelles d'exploration et d'analyse de données, mais il est de plus en plus possible de contrôler ces informations grâce au développement des «données massives»¹. La capacité à extraire de la valeur des données massives est devenue une source importante de pouvoir pour les principaux acteurs des marchés internet. Toutes les données massives n'ont pas de caractère personnel, mais pour de nombreuses offres en ligne qui sont présentées ou perçues comme étant «gratuites», les données à caractère personnel fonctionnent comme une sorte de monnaie indispensable utilisée pour payer ces services. Outre leurs avantages, ces marchés en pleine expansion présentent donc des risques spécifiques pour le bien-être des consommateurs et les droits au respect de la vie privée et à la protection des données.
2. Les principes et les règles de l'Union européenne en matière de protection des données, de concurrence et de protection des consommateurs ont été conçus pour promouvoir un marché intérieur florissant et pour protéger les individus. Une meilleure convergence dans l'application de ces politiques pourrait contribuer à relever les défis que pose l'économie des données massives. Toutefois, jusqu'à présent, les politiques ont eu tendance à se développer parallèlement les unes aux

¹ Les données massives «sont de gigantesques ensembles de données numériques détenus par des sociétés, gouvernements et autres grandes organisations, qui sont ensuite analysés de façon extensive à l'aide d'algorithmes informatiques»; avis du groupe de travail Article 29 n° 03/2013 sur la limitation des finalités, p. 35. Selon une autre définition, les données massives désignent des «ensembles de données dont la taille est supérieure à ce que les logiciels typiques de bases de données peuvent capturer, enregistrer, gérer et analyser»; McKinsey Global Institute, «Big data: The next frontier for innovation, competition, and productivity», juin 2011. Dans le présent avis préliminaire, le terme «données massives» est utilisé pour désigner l'association de la collecte de données massives à caractère personnel et de l'analyse d'ensembles très volumineux de données très variées.

autres, sans beaucoup d'interaction sur des centres d'intérêt communs². En outre, à ce jour, les décideurs politiques et les législateurs européens se sont généralement concentrés sur des marchés de produits et services échangés contre de l'argent. Dans la mesure où les consommateurs et les entreprises s'adaptent aux évolutions technologiques constantes et les font avancer, il est de la responsabilité des décideurs politiques et des législateurs de suivre le rythme, ainsi qu'il ressort du récent engagement politique concernant le «parachèvement» du «marché unique numérique»³.

3. Le CEPD encourage une «culture de la protection des données» dans les institutions et organes communautaires au sein desquels les principes de la protection des données s'expriment dans tous les domaines pertinents de la politique et du droit⁴. En vue de la réalisation de cet objectif, le présent avis préliminaire vise à stimuler un dialogue entre les experts et les praticiens, y compris les institutions communautaires et les autorités réglementaires nationales des secteurs de la concurrence, de la protection des consommateurs et de la protection des données. Le CEPD réfléchira ensuite aux

² Le présent avis préliminaire développe les thèmes mis en avant par le Contrôleur européen de la protection des données (ci-après le «CEPD») lors d'un séminaire à Bruxelles le 13 juin 2013 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-06-13_Speech_CB_Brussels_FR.pdf. Des discussions associées ont eu lieu en 2010 lors de la 32^e Conférence Internationale des commissaires à la protection des données et de la vie privée qui s'est tenue à Jérusalem. En outre, le vice-président de la Commission Joaquin Almunia a prononcé un discours sur la concurrence et la vie privée sur les marchés de données («Competition and privacy in markets of data») en novembre 2012 (http://europa.eu/rapid/press-release_SPEECH-12-860_fr.htm). En février 2013, lors de la 4^e Conférence internationale de la revue Concurrences - New Frontiers of Antitrust, suite à une table ronde sur le thème «Personal data: Will competition law collide with privacy?», le directeur général de la justice de la Commission européenne avait appelé à une meilleure prise en considération de la protection des données et du droit de la concurrence; Françoise Le Bail, «Protection de la vie privée et des données personnel: l'Europe à l'avant-garde», Concurrences Revue des droits de la concurrence: Competition Law Journal: «Demain la concurrence» New Frontiers of Antitrust Colloque I Concurrences, n° 2-2013. Aux États-Unis, un débat similaire a lieu notamment depuis la décision de la Federal Trade Commission sur la fusion Google DoubleClick (voir note de bas de page 76) et l'avis divergent du commissaire de l'époque, Jones Harbour http://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf; pour une mise à jour de l'analyse de M^{me} Harbour, consulter son essai «The Transatlantic Perspective: Data Protection and Competition Law», dans *Data Protection Anno 2014: How to Restore Trust?* éd. Hijmans, H. et Kranenborg, H., 2014, p. 225 à 234.

³ En octobre 2013, le Conseil européen s'est engagé à «parachever le marché unique numérique» d'ici à 2015 en incluant «les conditions-cadres adaptées pour un marché unique des données massives et de l'informatique en nuage», en développant le gouvernement en ligne, la santé en ligne, la facturation en ligne et la passation de marchés publics en ligne, par l'accélération de l'identification électronique et des services de confiance, des services de facturation et de paiement en ligne, et par la portabilité des contenus et des données; http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf. Le CEPD a émis un avis sur le programme politique général de l'Union européenne relatif à la Stratégie numérique pour l'Europe; https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-04-08_Digital_Agenda_EN.pdf

⁴ Stratégie 2013-2014 du CEPD: «Vers un niveau d'excellence en matière de protection des données»; https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/13-01-22_Strategy_FR.pdf. En plus d'avis réguliers émis en réponse à des propositions législatives ou documents politiques adoptés par la Commission ou d'autres institutions ou organes au titre de l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, et en sa qualité de conseiller des institutions et organes communautaires et des personnes concernées sur tous les sujets liés au traitement de données à caractère personnel au titre de l'article 41, paragraphe 2, le CEPD peut décider de publier des avis de sa propre initiative dans le but de contribuer à des débats sur des évolutions juridiques et sociétales susceptibles d'avoir un impact majeur sur la protection des données à caractère personnel. Par exemple, voir avis du CEPD sur la relation entre l'informatique en nuage et le cadre juridique de la protection des données, JO C 253 du 3.9.2013, p. 1. Des avis similaires peuvent être publiés dans d'autres domaines d'intérêt.

positions et idées découlant de cet exercice dans un avis de suivi, dans lequel il formulera des recommandations d'actions.

4. Le chapitre 2 du présent avis commence par passer en revue les tendances de l'économie numérique et le rôle des données à caractère personnel à l'ère de la collecte de données massives. Le chapitre 3 traite des aspects pertinents des règles européennes en matière de protection des données, de concurrence et de protection des consommateurs. Le chapitre 4 présente une analyse des interactions entre les trois domaines politiques:

- la façon dont le contrôle des informations personnelles contribue au pouvoir du marché dans l'économie numérique et les implications pour la protection des données;
- les risques pour les consommateurs résultant de concentrations et de l'abus de la position dominante sur le marché lorsque des entreprises traitent des volumes considérables de données à caractère personnel; et
- la façon dont la croissance d'un marché dynamique de services renforçant la protection de la vie privée⁵ peut être encouragée par le renforcement du choix informé du consommateur.

L'importance d'une réflexion, d'une mise en œuvre et d'une coopération communes entre les autorités de contrôle aux niveaux international, européen et national est également soulignée⁶.

5. En conclusion, le chapitre 5 étudie les réponses politiques possibles et invite la Commission, les autorités nationales de contrôle, les groupes de défense et les praticiens du droit à entamer une discussion plus large et plus approfondie sur le sujet. Au début de chaque partie, des puces et des références croisées guident le lecteur dans les arguments clés et les intersections entre les trois domaines du droit communautaire. Un résumé de ces interfaces est présenté en annexe au présent document.

2. Données massives, données à caractère personnel: le carburant de l'économie numérique

- *Les sociétés de tous les secteurs de l'économie comptent sur des volumes considérables de données à caractère personnel pour développer des services, mais contrairement à d'autres actifs incorporels, il est rarement rendu compte de cette situation.*

⁵ Les technologies qui renforcent la protection de la vie privée ont été définies par la Commission comme «un dispositif cohérent de mesures dans le domaine des technologies de l'information et de la communication, qui protège la vie privée en supprimant ou restreignant les données à caractère personnel, ou encore en évitant les traitements inutiles et/ou non souhaités de ces données, sans pour autant perdre la fonctionnalité du système d'information». «Promouvoir la protection des données par les technologies renforçant la protection de la vie privée», COM(2007) 228 final. Dans ce document, l'expression «services renforçant la protection de la vie privée» est utilisée pour désigner des services clients qui ont été conçus sur la base d'une telle technologie.

⁶ Cela comprend la liaison avec et entre le Global Privacy Enforcement Network, l'International Competition Network, ainsi qu'une collaboration plus approfondie entre les autorités communautaires et la Federal Trade Commission américaine.

- *Les services en ligne «gratuits» sont «payés» par l'utilisation de données à caractère personnel dont la valeur totale a été estimée à plus de 300 milliards d'euros et devrait tripler d'ici 2020.*
- *Malgré les risques pour les données à caractère personnel des individus qui utilisent ces services, le marché des services renforçant la protection de la vie privée reste comparativement faible.*

La concurrence sur les principaux marchés numériques prend souvent une forme assez distinctive. Tout d'abord, la concurrence entre les modèles d'entreprise («business models») ou les plateformes tend à être plus importante que la concurrence au sein d'un modèle d'entreprise du fait que la concurrence de plateforme aboutit souvent à une issue dans laquelle un seul acteur remporte la mise. En d'autres termes, la dominance (voire le monopole) peut être l'issue quasiment inévitable du succès. Ensuite, les marchés numériques sont souvent caractérisés par des effets de réseau importants et des économies d'échelle qui renforcent ce rapport entre concurrence et position dominante. Enfin, de nombreux marchés numériques ont deux facettes, de sorte que plusieurs groupes d'utilisateurs bénéficient de l'utilisation de la plateforme numérique. Les moteurs de recherche, par exemple, sont utilisés à la fois par des personnes pour accéder à des informations sur l'internet et par des publicitaires pour accéder à des clients [...]

OCDE, «The Digital Economy», février 2013

2.1. Les données massives à caractère personnel, un atout

6. L'économie numérique se caractérise par une croissance forte et dynamique, un chiffre d'affaires élevé généré par de nouveaux services, une concentration du marché impliquant quelques acteurs extraordinairement dominants et un déséquilibre encore plus grand entre de grandes entreprises, d'une part, et des PME et utilisateurs individuels, d'autre part⁷. Cette croissance s'est accompagnée, dans tous les secteurs de l'économie, d'une hausse exponentielle de la valeur des données et d'avancées dans l'exploration et l'analyse de données, ainsi que d'une augmentation considérable de la puissance informatique et de la capacité de stockage de données.
7. Selon un récent sondage, 57 % des entreprises analysées considèrent qu'elles «gèrent des données massives» au sens de «très grands ensembles de données», ce qui peut inclure la «transmission en continu de données provenant de machines, de capteurs, d'applications en ligne et de réseaux sociaux»⁸. Dans un processus qui a été qualifié de «mise en données» («*datafication*»), on estime à 2,3 trillions de gigabits le volume des données collectées et regroupées chaque jour, les données elles-mêmes servant de base à des services aussi divers que des outils de contrôle de la bonne condition

⁷ Avis du CEPD sur la communication de la Commission «Exploiter le potentiel de l'informatique en nuage en Europe», 16 novembre 2013.

⁸ L'étude réalisée en 2013 par le Data Warehousing Institute portait sur les «professionnels de la gestion de données» et a reçu 693 réponses provenant d'un éventail de secteurs (notamment services financiers, conseil, logiciels/internet, soins de santé et assurance), dont 48 % étaient basés aux États-Unis et 20 % en Europe; Russom, P., «TDWI Best Practices Report: Managing Big Data», quatrième trimestre 2013.

physique et des outils de cartographie mondiale⁹. Les données massives sont plus que des données à caractère personnel: elles incluent des données agrégées et des données anonymes. Certaines entreprises peuvent considérer que la plupart de leurs données sont des ensembles de données sans caractère personnel mais, en réalité, il est désormais rare que des données générées par l'activité d'utilisateurs soient anonymisées de façon totale et irréversible¹⁰. Des quantités d'informations personnelles sont générées par plus de 369 millions d'internautes dans l'Union européenne¹¹ du fait de leur utilisation de réseaux sociaux, jeux, moteurs de recherche, sites de vente en ligne et autres services. Les informations collectées sur les abonnés à un service en ligne donné comprennent le nom, le sexe, les préférences personnelles, le lieu, les adresses électroniques, les adresses IP et l'historique de navigation. Elles sont utilisées pour investir dans des relations avec la clientèle existante et pour acquérir de nouveaux clients.

8. Tandis que les données étaient auparavant collectées dans le cadre de la prestation d'un service particulier, «la valeur ajoutée des données massives», explique un observateur, «réside dans le potentiel de découverte de nouvelles corrélations pour de nouveaux usages après la collecte des données... [qui] pourraient être sans rapport avec les finalités originales pour lesquelles les données ont été collectées»¹². Les estimations de cette valeur ajoutée varient selon le contexte et la méthodologie: des recettes ou un revenu net par dossier/utilisateur de deux entreprises mondiales dont les modèles reposent sur des données à caractère personnel ont été calculés à 3-5 euros par an¹³; tandis que la valeur numérique que les consommateurs européens accordent à leurs données a été estimée à 315 milliards d'euros en 2011 et devrait atteindre 1 trillion d'euros d'ici à 2020¹⁴.
9. La question de savoir dans quelle mesure les entreprises devraient pouvoir tirer parti des ensembles de données à caractère personnel et les monétiser a fait l'objet de discussions. Quoi qu'il en soit, les informations personnelles sont devenues un actif incorporel important qui est utilisé pour créer de la valeur et qui est comparable au

⁹ Source de l'estimation du volume de données généré quotidiennement: IBM. Voir Mayer-Schönberger, V., et Cukier, K. (2013), «Big Data, A Revolution That Will Transform How We Live, Work and Think», p. 94 à 97.

¹⁰ Avis du groupe de travail Article 29 n° 4/2007 sur le concept de données à caractère personnel, WP 136, adopté le 20 juin 2007.

¹¹ Miniwatts Marketing Group (chiffres basés sur l'Union européenne des 27).

¹² Moerel L., discours d'inauguration à la Tilburg Law School, «Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof», 14 février 2014.

¹³ Organisation de coopération et de développement économiques (OCDE) (2013), «Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value», OECD Digital Economy Papers, n° 220, OECD Publishing. L'acquisition récemment annoncée de WhatsApp par Facebook pour 19 milliards de dollars revient à payer 30 euros pour chacun des 450 millions d'utilisateurs du service de messagerie. La Commission européenne doit encore statuer sur la question de savoir si cette transaction sera soumise à un contrôle de concentration voir <http://www.bloomberg.com/news/2014-02-20/facebook-s-whatsapp-deal-seen-avoiding-u-s-antitrust-challenge.html> (consulté le 10 mars 2014).

¹⁴ Boston Consulting Group, «The Value of our Digital Identity», novembre 2012 (voir <http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>, consulté le 5 mars 2014).

droit d'auteur, aux brevets, au capital intellectuel et au fonds commercial¹⁵. Il s'agit souvent de l'actif le plus précieux d'une entreprise, comme démontré par de récentes offres publiques de vente marquantes sur les bourses mondiales et par des concentrations dans l'économie numérique. Toutefois, contrairement à d'autres actifs incorporels, la valeur des informations personnelles qui sont contrôlées par une entreprise ne semble pas intégrée dans son bilan¹⁶.

2.2. Une monnaie pour l'achat de services «gratuits»

10. Avec de nombreux services numériques, tels que le courriel et les moteurs de recherche, utilisés par la quasi-totalité des internautes, les entreprises entretiennent l'idée qu'ils sont fournis gratuitement. En réalité, tout individu qui souhaite en bénéficier doit remettre des informations personnelles précieuses. Du fait de leurs activités en ligne, les consommateurs fournissent des informations très détaillées sur leurs préférences qui permettent de cibler des individus, et non des groupes, avec une précision bien plus grande qu'auparavant. Pour les consommateurs, les informations personnelles font donc office de monnaie et, parfois, de monnaie unique pour l'échange de services en ligne¹⁷.

2.3. Des modèles d'entreprise conçus pour s'emparer de la valeur des données massives à caractère personnel

11. Une «chaîne de valeur des données à caractère personnel» à quatre étapes a été identifiée¹⁸: elle s'articule autour (1) de la collecte et de l'accès, (2) du stockage et de l'agrégation, (3) de l'analyse et de la distribution, et (4) de l'utilisation d'ensembles de données à caractère personnel. Tout au long de cette chaîne de valeur, il est probable qu'une multiplicité d'individus, d'entreprises, d'institutions publiques et d'organisations à but non lucratif consultent et traitent ces ensembles de données. Parmi eux: les courtiers de données («*data brokers*»), qui servent d'intermédiaires pour l'échange d'informations personnelles entre un responsable du traitement de

¹⁵ Ce constat a été reconnu par la Commission: «Aujourd'hui, les données à caractère personnel constituent un type d'actif pour les entreprises» (discours du vice-président Almunia, «Competition and personal data protection», 26 novembre 2012); «[...] les données massives ne sont pas qu'un nouveau secteur, mais aussi une nouvelle catégorie d'actifs. Une catégorie qui constitue un pilier de notre économie, comme les ressources humaines ou le capital financier» (discours de la vice-présidente Kroes, «Big Data for Europe», 7 novembre 2013). Voir également la publication du Forum économique mondial, «Personal Data: The Emergence of a New Asset Class», 2011. Quant à la définition d'un actif, le cadre des normes internationales d'information financière indique qu'«un actif est une ressource contrôlée par l'entreprise du fait d'événements passés et dont des avantages économiques futurs sont attendus par l'entreprise». Bien que cela ne soit pas le sujet du présent document, des révélations découlant d'activités de surveillance gouvernementale ont démontré une fois encore que la valeur des informations personnelles va bien au-delà des préoccupations commerciales.

¹⁶ OCDE, «Innovation Strategy and sources of growth».

¹⁷ «Les données à caractère personnel sont la monnaie du marché numérique actuel», discours de la vice-présidente de la Commission, Viviane Reding, «The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age – Innovation Conference Digital, Life, Design», Munich, 22 janvier 2012. «Les entreprises qui cherchent à maximiser les profits ne fournissent pas des produits gratuitement, à moins que cela ne les aide à faire de l'argent autre part»; Evans, D., S. (2011), «The Antitrust Economics of Free», University of Chicago Working Paper n° 555, 2011.

¹⁸ OCDE, «Exploring the Economics of Personal Data», 2013.

données et un autre,¹⁹ ainsi que les prestataires d'informatique en nuage (pour des services applicatifs et de stockage).

12. Il arrive souvent que des entreprises comptent sur des données massives et les exploitent par le biais d'**une plateforme ou d'un modèle d'entreprise biface ou multi-face**, des services distincts de financement croisé fournis à plusieurs groupes d'utilisateurs distincts, c'est-à-dire à des utilisateurs de services «gratuits», d'une part, et à d'autres entreprises, en particulier des publicitaires, d'autre part. Par la prestation de services «sans paiement», ces entreprises rivalisent pour obtenir l'attention et la fidélité des individus dont l'utilisation de ces services générera des données à caractère personnel à grande valeur commerciale. Elles peuvent faire une distinction entre les utilisateurs avec des offres allant de services gratuits de base à des services de première qualité ciblant les entreprises qui sont prêtes à en payer le prix²⁰.
13. Plus lucrativement, ces entreprises peuvent vendre les informations collectées à des publicitaires, souvent par l'intermédiaire de courtiers de données, ou acheter un espace pour diffuser leurs publicités à côté de résultats de recherche. Les services de publicité, de conseil et de statistiques dépendent des informations collectées par les entreprises numériques pour créer des profils d'internautes qui, à leur tour, permettront un ciblage comportemental plus efficace²¹. Ce processus est bien différent des anciennes approches marketing qui consistaient, par exemple, à cibler les publicités sur des groupes de téléspectateurs mal segmentés.

2.4. *Un marché sous-développé de services renforçant la protection de la vie privée*

14. Les données massives sont la promesse de recettes faramineuses pour des entreprises de secteurs allant des loisirs aux transports, en passant par la santé et les économies d'énergie; mais quand il s'agit de données à caractère personnel, elles s'accompagnent aussi de risques considérables pour l'individu sur lequel portent les informations²². Malgré ce risque accru, le marché des services renforçant la protection de la vie privée reste faible dans l'économie numérique. Si beaucoup de consommateurs sont de plus en plus technophiles, la plupart semblent ne pas avoir conscience ou ne pas se préoccuper du niveau d'intrusion dans leurs recherches et leurs courriels du fait de la journalisation et de l'analyse d'informations sur leurs

¹⁹ Les courtiers de données ou d'informations collectent des informations personnelles sur les consommateurs et vendent ces informations à d'autres organisations en utilisant une série de sources publiques et privées, tels que les registres de tribunaux, les cookies de sites internet et les programmes de cartes de fidélité, pour créer des profils d'individus à des fins marketing, puis les vendent à des entreprises souhaitant cibler leurs publicités et leurs offres spéciales. Outre les droits généraux d'accès applicables en vertu de la directive relative à la protection des données (voir point 25), aucune législation n'impose explicitement à un courtier de données de dire à ses clients quelles informations il a collectées ou les profils qu'il a développés à l'aide de ces données. Aux États-Unis, ce secteur fait actuellement l'objet d'activités d'exécution, de collecte d'informations et de sensibilisation par la Federal Trade Commission (voir http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf, consulté le 10 mars 2014).

²⁰ Ces services peuvent être mis en contraste avec des offres numériques, telles que Wikipédia, dont l'utilisation est véritablement gratuite et exempte de publicité, bien que les utilisateurs puissent être invités à donner de l'argent en guise de soutien.

²¹ Geradin, D. et Kuschewsky, M. (2013), «Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue», SSRN.

²² Par exemple, Pentland, A., «Social Physics: How Good Ideas Spread—The Lessons from a New Science», (Penguin, 2014), et la discussion sur les avantages et les risques dans Polonetsky, J. et Omer, T., «Privacy and Big Data: Making Ends Meet», 66 Stanford Law Review Online, 25, 3 octobre 2013.

activités en ligne, ainsi que de leur transformation en recettes par des prestataires de services. À ce jour, un nombre relativement faible d'entreprises de l'économie numérique a identifié un avantage financier à renforcer la protection de la vie privée dans leurs offres²³.

3. Cadre juridique

- *Les règles distinctes en matière de protection des données, de concurrence et de protection des consommateurs convergent toutes vers une double finalité: la protection et la promotion du bien-être de l'individu et la facilitation de la création d'un marché unique européen.*
- *La finalité des règles de concurrence est l'efficacité du marché intérieur et le bien-être des consommateurs, et l'appréciation de ces règles doit être placée dans le cadre général des objectifs et valeurs de l'Union européenne.*
- *Les règles de protection des consommateurs visent à interdire les déclarations trompeuses sur des produits et services, en particulier ceux commercialisés comme étant «gratuits».*

15. Les principaux objectifs de l'Union européenne comprennent ses valeurs fondamentales de promotion de la paix et du bien-être de ses peuples, ainsi que sa mission économique, notamment un espace de liberté sans frontières intérieures et un marché intérieur offrant une concurrence libre et non faussée²⁴. Les règles adoptées par l'Union européenne en matière de protection des données, de concurrence et de protection des consommateurs, qui s'appliquent aux opérateurs économiques et aux États membres²⁵, reflètent ces valeurs fondamentales et cette mission économique de diverses façons et sur différentes bases légales dans le traité sur le fonctionnement de l'Union européenne (TFUE). Il existe des autorités de contrôle distinctes aux niveaux national et européen, et le respect d'un ensemble de règles ne signifie pas forcément le respect de l'autre, de même que le non-respect de l'un ne signifie pas la violation de l'autre. Cependant, les finalités des trois domaines convergent et ce point de convergence est le sujet de cette partie.

3.1. Protection des données

3.1.1. Le droit fondamental à la protection des données à caractère personnel

Voir également: parties 3.2.1 (Objectifs des règles européennes de concurrence) et 3.3.1 (Exigence de garantir un niveau élevé de protection des consommateurs)

²³ Point 4.3 ci-dessous. Pour une discussion sur la façon dont le «parti pris pour le statu quo» («*status quo bias*») peut induire une réticence à remettre en question les «paramètres de confidentialité» par défaut, voir Moerel (précité à la note de bas de page 12).

²⁴ Article 3 du traité sur l'Union européenne.

²⁵ Les organes publics des États membres, lorsqu'ils traitent des données à caractère personnel, sont soumis aux obligations découlant de la directive relative à la protection des données, sauf dans le cadre d'une activité ne relevant pas du champ d'application du droit communautaire ou lorsque le traitement a pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal; article 3 de la directive relative à la protection des données. Les règles relatives aux aides d'État des articles 107, 108 et 109 du TFUE visent à contrôler les actions par les États membres eux-mêmes, plutôt que par des entreprises susceptibles de fausser la concurrence ou le commerce entre des États membres.

16. Le droit au respect de la vie privée et familiale, du domicile et des communications, tel qu'il est prévu à l'article 7 de la Charte des droits fondamentaux (ci-après la «Charte»), protège principalement l'individu contre toute atteinte par l'État. L'article 8 énonce la protection des données à caractère personnel comme un droit distinct, qui va au-delà de la simple protection contre toute atteinte par l'État. Il s'agit d'un droit proactif au titre duquel un individu peut s'attendre à ce que ses informations soient uniquement traitées, par *quiconque* et pas uniquement par l'État, si certaines conditions essentielles énoncées à l'article 8, paragraphes 2 et 3, sont satisfaites. Cela requiert que le traitement soit loyal, licite et réalisé dans un but précis, qu'il soit transparent pour l'individu qui a le droit d'accéder à ses informations et de les rectifier, et que les droits soient soumis au contrôle d'une autorité indépendante²⁶.
17. L'article 16 du TFUE requiert que des règles soient adoptées concernant la protection des données et la libre circulation de ces données dans le marché intérieur. La **directive 95/46/CE** (ci-après la «directive relative à la protection des données»), bien qu'adoptée sur une autre base juridique, reste aujourd'hui l'acte législatif central en vertu de cet article. Elle impose un équilibre entre le contrôle des informations à caractère personnel d'un individu et la libre circulation des données dans le marché intérieur. Le Parlement européen et le Conseil étudient actuellement les propositions de nouveau cadre juridique formulées par la Commission en janvier 2012²⁷. Dans ce cadre, la **directive 2002/28/CE** contient des règles spécifiques concernant la vie privée en lien avec les technologies numériques et les services de communication électroniques, notant en particulier que «le succès du développement transfrontalier de ces services dépend en partie de la confiance qu'auront les utilisateurs que ces services ne porteront pas atteinte à leur vie privée» (considérant 5)²⁸.
18. Les données à caractère personnel telles que définies à l'article 2, point a), de la directive 95/46/CE désignent «toute information concernant une personne physique identifiée ou identifiable». Cela comprend toute information se rapportant à l'identité, aux caractéristiques ou au comportement d'un individu ou qui est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée²⁹. Des identités peuvent être dissimulées par diverses techniques, telles que des données codées par une clé, mais il est généralement possible de remonter des informations «pseudonymisées» jusqu'à l'individu concerné, de sorte que les législations relatives à la protection des données continueront à s'appliquer³⁰. Tous les individus, en tant que personnes concernées, bénéficient de cette protection juridique, peu importe qu'ils soient présumés être des consommateurs d'un service particulier. Dans certains cas, des personnes morales peuvent aussi bénéficier de la protection, par exemple lorsque

²⁶ Kokott, J. et Sobotta, C., «The Distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», *International Data Privacy Law*, 2013, vol. 3, n° 4, p. 222 à 228.

²⁷ Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final.

²⁸ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37.

²⁹ Document du groupe de travail WP 105, «Working document on data protection issues related to RFID technology», 19 janvier 2005, p. 8.

³⁰ Avis du groupe de travail Article 29 n° 4/2007 sur le concept de données à caractère personnel, WP 136, adopté le 20 juin 2007, p. 18 à 21.

le titre officiel de la personne morale ou toute autre information identifie une ou plusieurs personnes physiques³¹.

19. Le droit à la protection des données à caractère personnel n'est pas un droit absolu mais «doit être considéré au regard de sa fonction dans la société»³². Conformément à l'article 52, paragraphe 1, de la Charte des droits fondamentaux, des limitations peuvent être apportées à l'exercice de ces droits et d'autres droits pour autant que ces limitations sont prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et libertés et que, dans le respect du principe de proportionnalité, elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui.

3.1.2. Personnes soumises à des obligations en vertu des règles en matière de protection des données

Voir également: partie 3.2.2 Champ d'application des règles de concurrence

20. Dans l'intérêt de garantir des conditions équitables, le droit européen en matière de protection des données s'applique de la même façon à tous les responsables du traitement de données établis dans l'Union européenne ou recourant à des moyens situés dans l'Union européenne³³. Conformément à la proposition de règlement général sur la protection des données de la Commission, le champ territorial des règles communautaires devrait être étendu à tout responsable du traitement de données «offrant des biens ou des services» et «observant [le] comportement de personnes concernées résidant dans l'Union européenne»³⁴. Cette précision semble appropriée compte tenu de la dimension mondiale des échanges d'informations qui caractérisent l'économie numérique. Une comparaison est possible avec les règles européennes de concurrence, qui s'appliquent à chaque fois que le comportement d'une entreprise pourrait affecter le marché intérieur, peu importe son lieu d'établissement (voir point 32).

21. Toutes les entreprises qui sont des responsables du traitement sont soumises aux obligations de protéger les données à caractère personnel, peu importe leur taille, voire leur position dominante sur un marché. Cependant, comme l'a récemment relevé la Cour européenne des droits de l'homme, «plus le volume et la sensibilité des données conservées et divulguées sont importants, plus le contenu des garanties devant être appliquées aux divers stades critiques du traitement ultérieur des données

³¹ Arrêt du 9 novembre 2010, Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, Rec. p. I-11063), point 53. La directive relative à la protection des données (article 2, point a)) prévoit la protection des données à caractère personnel de toutes les personnes physiques identifiées ou identifiables. Ceci est maintenu dans la proposition de règlement général sur la protection des données de la Commission (12e considérant et article 4, paragraphe 1). Certaines juridictions nationales (Autriche, Danemark, Italie et Luxembourg) étendent la protection à des personnes morales; Korff, D. (pour le compte de la Commission européenne), «Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons», 1998 (voir http://ec.europa.eu/justice/policies/privacy/docs/studies/legal_en.pdf).

La directive 2002/58/CE prévoit expressément (article 1, paragraphe 2) la protection des intérêts légitimes des abonnés à des services de communication électronique qui sont des personnes morales.

³² *Schecke*, point 48.

³³ Article 4, paragraphe 1, de la directive 95/46/CE.

³⁴ Article 3, paragraphes 1 et 2. Il est intéressant de noter que le Parlement européen a cherché à préciser que le champ d'application devrait englober l'offre de biens ou de services, «qu'un paiement soit exigé ou non» [texte ajouté au considérant 20] afin de lever tout doute quant au fait que des services en ligne «gratuits», tels qu'une recherche ou un réseau social, relèvent avec certitude du champ d'application du règlement.

est essentiel». De nombreuses dispositions relatives à la protection des données peuvent donc être considérées comme adaptables au volume, à la complexité et à la nature intrusive des traitements de données à caractère personnel d'une entreprise et, par conséquent, comme particulièrement pertinentes pour des entreprises puissantes gérant des données massives³⁵. Cela est analogue au concept de la «responsabilité particulière» d'entreprises dominantes visant à éviter des distorsions de concurrence dans le marché intérieur, comme évoqué ci-après (voir point 33)³⁶.

3.1.3. Finalités légitimes et compatibles du traitement de données

Voir également: partie 3.2.3 Définition du marché pertinent

22. L'article 6, paragraphe 1, point b), de la directive relative à la protection des données dispose que les données à caractère personnel doivent être «collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités». Ce principe de limitation des finalités est nécessaire pour garantir la confiance, la prévisibilité, la sécurité juridique et l'utilisation transparente des données à caractère personnel par des responsables du traitement³⁷. Un traitement ultérieur pour une finalité secondaire n'est pas interdit, mais cette finalité secondaire ne doit pas être «incompatible» avec les finalités pour lesquelles les données ont été collectées. Distinguer un traitement compatible et un traitement incompatible de données à caractère personnel est souvent un exercice complexe et délicat dans le droit en matière de protection des données. Si la directive n'interdit pas forcément le traitement pour des finalités différentes, le groupe de travail Article 29 a recommandé d'en vérifier la compatibilité au regard du contexte dans lequel les données ont été collectées, des attentes raisonnables des personnes concernées, de la nature des données à caractère personnel en question, de l'impact du traitement ultérieur et des garanties protégeant la personne concernée.
23. Le concept de la compatibilité peut être comparé à celui de la substituabilité, qui est utilisé dans l'application des règles de concurrence pour déterminer quels produits peuvent être considérés comme concurrents sur le même marché. Dans le contexte de l'économie numérique, il est concevable qu'une entreprise puisse collecter des données dans le but de fournir un certain service sur un marché, puis traiter ces données pour rivaliser dans le cadre de la prestation d'un autre service sur un marché distinct (voir point 58).

3.1.4. Consentement et droit à l'information, droit d'accès aux données et droit à la portabilité des données

Voir également: parties 3.2.4 (Bien-être des consommateurs conformément aux règles de concurrence) et 3.3.2 (Obligation de fournir des informations précises aux consommateurs)

³⁵ Cour européenne des droits de l'homme, affaire 24029/07, M.M. c. Royaume-Uni, 13 novembre 2012, point 200.

³⁶ Dans sa proposition de règlement général sur la protection des données, la Commission envisage un nombre moins important d'obligations administratives pour les petites et moyennes entreprises; voir considérant 11 de la proposition de la Commission. Selon le projet de résolution législative du Parlement européen sur la proposition, des obligations réduites s'appliqueraient aux responsables dont le traitement de données vise moins de 5 000 personnes au cours d'une année donnée.

³⁷ Cette partie utilise l'analyse figurant dans l'avis du groupe de travail Article 29 n° 03/2013 sur la limitation des finalités, WP 203, adopté le 2 avril 2013.

24. Le traitement de données à caractère personnel requiert une base juridique. C'est sur cette base que la personne concernée peut donner son consentement libre, indubitable et informé au traitement en question³⁸. Un simple silence ou une simple inaction, comme pour les paramètres de confidentialité de réseaux sociaux en ligne ou de navigateurs internet, n'est pas valable. Le consentement doit être demandé avant le traitement des données et uniquement après que les traitements ont été notifiés de façon claire et compréhensible à la personne concernée par le responsable du traitement. Il peut être retiré, auquel cas toutes données à caractère personnel relatives à la personne concernée doivent être effacées, à moins qu'une autre base juridique ne justifie leur conservation³⁹.
25. Les individus ont le droit d'être informés du traitement de leurs données à caractère personnel, y compris de l'identité du responsable du traitement, des finalités du traitement, des destinataires des données, ainsi que de leurs droits en tant que personnes concernées⁴⁰. Conformément à l'article 12 de la directive relative à la protection des données, ils ont le droit d'accéder aux données les concernant et d'en obtenir la rectification, l'effacement ou le verrouillage si elles sont incomplètes ou inexacts. La réforme proposée envisage (article 18) d'étendre ce droit pour permettre à la personne concernée d'obtenir une copie des données traitées dans un format électronique, tels que les profils de réseaux sociaux ou les historiques d'achats et de recherches, et de les transmettre à un autre système de traitement automatisé.
26. Ce droit à la portabilité des données permettrait aux utilisateurs de passer d'un service en ligne à un autre de la même façon que les utilisateurs de services téléphoniques peuvent changer de prestataire de services tout en conservant leurs numéros de téléphone⁴¹. En outre, la portabilité des données permettrait aux utilisateurs de remettre leurs données à des tiers proposant différents services à valeur ajoutée. À titre d'illustration, la portabilité appliquée au comptage électrique intelligent permettrait aux consommateurs de télécharger les données relatives à leur consommation énergétique auprès de leur compagnie d'électricité actuelle, pour ensuite engager un tiers capable de les conseiller sur un autre fournisseur proposant un meilleur prix sur la base de leurs modèles de consommation électrique. Une telle transparence permet aux individus d'exercer leurs autres droits à la protection des données et pourrait être vue comme reflétant les objectifs des règles relatives à l'obligation de remettre des informations claires et précises au consommateur (voir partie 3.3.2).

³⁸ Article 2, point h), de la directive relative à la protection des données. Avis du groupe de travail Article 29 n° 15/2011 sur la définition du consentement, WP 187, adopté le 13 juillet 2011.

³⁹ Ceci est dit implicitement dans la directive relative à la protection des données et explicitement à l'article 6, paragraphe 3, et l'article 9, paragraphe 1, de la directive vie privée et communications électroniques concernant le traitement de données relatives au trafic et de données de localisation par des services de communications électroniques accessibles au public.

⁴⁰ Article 10 de la directive 95/46/CE.

⁴¹ La «portabilité du numéro» est prévue par l'article 30 de la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive «service universel»).

3.1.5. Contrôle, mise en œuvre, sanctions et accès aux voies de recours en cas de violations

Voir parties 3.2.5 et 3.3.3 sur la supervision, etc.

27. L'article 8, paragraphe 3, de la Charte des droits fondamentaux dispose que les règles énoncées «[sont] soumis[es] au contrôle d'une autorité indépendante». L'article 16, paragraphe 2, du TFUE prévoit l'adoption de règles relatives à la protection des données dont la conformité doit être «soumise au contrôle d'autorités indépendantes». L'article 28, paragraphe 1, de la directive relative à la protection des données impose dûment aux États membres de l'Union européenne de prévoir qu'une ou plusieurs autorités publiques soient chargées de surveiller, en toute indépendance, l'application de la directive⁴². Les missions des autorités chargées de la protection des données comprennent le traitement des plaintes et la réalisation d'enquêtes. Elles peuvent ordonner le verrouillage, l'effacement ou la destruction de données, et prononcer des interdictions temporaires ou définitives de traitement.
28. Toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par la directive (article 22), ainsi que du droit d'obtenir réparation du préjudice subi du fait d'un traitement illicite de données (article 23). Les montants des possibles sanctions en cas de manquement varient considérablement entre les États membres: le seuil est de 10 000 HRK (1 131 EUR) en Croatie, tandis que l'autorité britannique impose des pénalités pouvant aller jusqu'à 500 000 GBP (597 000 EUR). En pratique, les victimes d'un traitement illicite sont dans l'impossibilité d'obtenir réparation en raison de la longueur et du coût de la procédure, ainsi que de la méconnaissance des règles et droits en matière de protection des données, bien qu'il y ait eu des évolutions encourageantes⁴³. Dans sa proposition de règlement, la Commission envisage également des sanctions administratives proportionnelles au chiffre d'affaires annuel de l'entreprise qui pourraient s'appliquer en cas de non-respect d'obligations en matière de protection des données, par exemple en cas de divulgation illicite à une autre organisation⁴⁴. Cela semble suivre l'approche en matière de sanctions applicable aux accords anticoncurrentiels (voir point 45 ci-dessous).
29. Contrairement aux concentrations selon les règles de concurrence (voir point 52 ci-dessous), lorsqu'un problème de protection des données affecte des individus dans plusieurs États membres, l'entreprise concernée peut actuellement faire l'objet d'enquêtes de plusieurs autorités nationales, dont les résultats sont souvent divergents. Les autorités nationales se réunissent sous la forme d'organe consultatif indépendant appelé groupe de travail «Article 29» sur la protection des données, dont les missions englobent la promotion d'une application uniforme des principes généraux de la

⁴² Article 28 de la directive 95/46/CE. La Cour de justice de l'Union européenne (ci-après la «Cour de justice») a donné une interprétation large de l'exigence de totale indépendance des autorités chargées de la protection des données dans les arrêts C-518/07 (Commission/Allemagne) et C-614/10 (Commission/Autriche). Voir également article 47 de la proposition de règlement général sur la protection des données, COM(2012) 11 final.

⁴³ Agence des droits fondamentaux, «Access to data protection remedies in EU Member States», 2013. En février 2014, le gouvernement fédéral allemand a annoncé son intention de permettre à des associations de défense des consommateurs de poursuivre directement des entreprises pour des manquements aux règles nationales relatives à la protection des données (voir <http://www.spiegel.de/netzwelt/netzpolitik/verbraucherschutzminister-maas-kuendigt-verbandsklagerecht-an-a-952767.html>).

⁴⁴ Articles 31 et 32, COM(2012) 11 final.

directive relative à la protection des données, mais qui ne joue pas de rôle formel dans son exécution. La proposition de règlement général sur la protection des données envisage donc des mesures garantissant la cohérence⁴⁵ selon lesquelles une seule autorité serait chargée de prendre des décisions juridiquement contraignantes contre une entreprise, les autorités seraient tenues de coopérer et un nouveau comité européen de la protection des données statuerait sur les affaires ayant un impact dans toute l'Union européenne.

3.2. Concurrence

3.2.1. Objectifs des règles européennes de concurrence

Voir parties 3.1.1 (Droit fondamental à la protection des données) et 3.3.1 (Exigence de garantir la protection des consommateurs)

30. Le droit de la concurrence porte sur le comportement des entreprises et l'abus de pouvoir de marché. Il a longtemps été essentiel pour l'Union européenne et a connu plusieurs phases: il était à l'origine un moyen de prévenir les obstacles publics au commerce interétatique et il vise désormais à garantir les contrôles nécessaires des concentrations d'entreprises et la libéralisation des secteurs de l'économie publique⁴⁶. Ses principaux objectifs sont d'améliorer l'efficacité du marché intérieur, ainsi que le bien-être et les choix offerts aux consommateurs⁴⁷. Selon certains, la finalité ultime du droit de la concurrence serait même de garantir que le marché intérieur réponde à tous les souhaits raisonnables des consommateurs en matière de concurrence, non seulement au souhait de prix compétitifs, mais aussi à ceux de diversité, d'innovation, de qualité et d'autres avantages non tarifaires, notamment la protection de la vie privée⁴⁸.
31. À cette fin, les articles 101 à 106 du TFUE interdisent les accords entre des entreprises susceptibles d'empêcher ou de fausser la concurrence, visent à écarter les abus de position dominante et imposent à la Commission d'enquêter sur les cas de violation suspectée des principes de la concurrence. Les articles 107, 108 et 109 du TFUE visent également à garantir des conditions équitables au sein du marché intérieur en empêchant tout traitement de faveur d'États membres envers certaines entreprises. L'Union européenne peut adopter des règlements ou directives appropriés en application de ces principes et règles (articles 103, 106 et 109), dont les plus significatifs sont le **règlement (CE) n° 1/2003 du Conseil (ci-après le «règlement de modernisation»)**, qui a décentralisé aux autorités nationales l'application des règles de concurrence, ainsi que le **règlement (CE) n° 139/2004 du Conseil (ci-après**

⁴⁵ Articles 58 à 63, COM(2012) 11 final.

⁴⁶ Wesseling, R. (2000), «The Modernisation of EC Antitrust Law», p. 48-9.

⁴⁷ La Cour de justice a défini les préoccupations du droit de la concurrence comme étant le bien-être des consommateurs, les intérêts des concurrents et la structure du marché [arrêt du 6 octobre 2009, GlaxoSmithKline Services e.a./Commission e.a. (C-501/06 P, C-513/06 P, C-515/06 P et C-519/06 P, Rec. p. I-9291), point 6].

⁴⁸ «Premièrement, les atteintes à la vie privée réduisent le bien-être des consommateurs, qui constitue un objectif majeur de toute analyse concurrentielle moderne. Deuxièmement, les atteintes à la vie privée entraînent une baisse de la qualité des produits ou services, qui constitue un type classique d'atteinte résultant du pouvoir de marché», Swire, P., «Protecting Consumers: Privacy matters in antitrust analysis», CCTr. for Am. Progress, 19 octobre 2007. Voir également Lande, R., «The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern», FTC: Watch, n° 714, 2008, University of Baltimore School of Law Legal Studies Research Paper n° 2008-06; et Averitt, N., Lande, R. et Nihoul, P., «'Consumer choice' is where we are all going – so let's go together», Foreword, Concurrences n° 2-2011.

le «**règlement sur les concentrations**») et le règlement d'exécution (UE) n° 1269/2013 qui contiennent les principales règles et procédures pour l'appréciation des concentrations⁴⁹.

3.2.2. Domaine d'application des règles de concurrence et pouvoir de marché

Voir également: partie 3.1.2 Personnes soumises à des obligations de protection des données

32. Les règles européennes de concurrence s'appliquent à chaque fois qu'une «activité économique» peut «affecter le commerce entre des États membres»; leur domaine d'application n'est pas déterminé par le lieu d'établissement d'une entreprise donnée⁵⁰. L'exécution de ces règles implique souvent d'apprécier le pouvoir de marché d'une entreprise donnée et de déterminer si l'entreprise occupe une position dominante. La Commission évalue le pouvoir de marché et la structure de marché en appréciant la part de marché, c'est-à-dire l'importance relative des différentes entreprises actives sur le marché⁵¹. Le déterminant habituel dans l'appréciation de la part de marché est le chiffre d'affaires de l'entreprise, ou le volume ou la valeur totale des ventes du produit pertinent dans le domaine concerné. La part de marché est ensuite interprétée à la lumière des conditions régnant sur le marché en cause⁵²: afin de mesurer la part de marché dans un secteur spécifique pertinent pour l'économie numérique, les lignes directrices de la Commission recommandent de sélectionner les critères qui sont les plus appropriés au regard des caractéristiques du marché⁵³.

33. Une position dominante sur le marché devient probable, quoique pas inévitable, dès lors que la part de marché d'une entreprise est supérieure ou égale à 40 %⁵⁴. La Commission envisage aussi des barrières à l'expansion ou à l'entrée sur le marché intérieur, énumérant à titre d'exemple les économies d'échelle, un accès privilégié à

⁴⁹ Règlement (CE) n° 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité, JO L 1 du 4.1.2003, p. 1 à 25; règlement (CE) n° 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises («le règlement CE sur les concentrations»), JO L 24 du 29.1.2004 (ci-après «le règlement sur les concentrations»); règlement d'exécution (UE) n° 1269/2013 de la Commission du 5 décembre 2013 modifiant le règlement (CE) n° 802/2004 concernant la mise en œuvre du règlement (CE) n° 139/2004 du Conseil relatif au contrôle des concentrations entre entreprises, JO L 336 du 14.12.2013, p. 1 à 36.

⁵⁰ Communication de la Commission, Lignes directrices relatives à la notion d'affectation du commerce figurant aux articles 81 et 82 du traité, JO C 101 du 27.4.2004.

⁵¹ Communication de la Commission, Orientations sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes, JO C 45 du 24.2.2009.

⁵² Point 13 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

⁵³ «Les critères à utiliser pour mesurer la part de marché des entreprises concernées dépendront des caractéristiques du marché en cause. Il revient à l'ARN de décider des critères les plus appropriés pour mesurer la présence sur le marché. À titre d'exemple, les recettes tirées des lignes louées, la capacité louée ou le nombre de points de terminaison de lignes louées sont autant de critères dont il est possible de se servir pour déterminer la force relative d'une entreprise sur les marchés des lignes louées»; Lignes directrices de la Commission sur l'analyse du marché et l'évaluation de la puissance sur le marché en application du cadre réglementaire communautaire pour les réseaux et les services de communications électroniques, JO C 165 du 11.7.2002. La publication de ces lignes directrices était une exigence de la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques.

⁵⁴ Point 14 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes. La Cour de justice a considéré d'autres facteurs dans l'appréciation de la position dominante ou autre d'entreprises; voir arrêts du 25 octobre 1977, Metro/Commission (26/76, Rec. p. 1875) et du 13 février 1979, Hoffmann-La Roche/Commission (85/76, Rec. p. 461).

des intrants essentiels, des coûts et d'autres entraves lorsque des clients veulent changer de fournisseur⁵⁵. La jurisprudence a établi qu'une position dominante faisait peser sur une entreprise la «responsabilité particulière» de ne pas porter atteinte à la concurrence par son comportement⁵⁶: elle peut chercher à préserver ses propres intérêts en cas d'attaque de concurrents, mais pas à renforcer sa position dominante.

3.2.3. Définition du marché pertinent

Voir partie 3.1.3 Finalités légitimes et compatibles du traitement de données

34. La définition du marché pertinent est la première étape de l'analyse juridique d'affaires impliquant des accords anticoncurrentiels, des concentrations et des abus de position dominante sur le marché. Elle permet aux autorités de contrôle de la concurrence d'identifier les opérateurs du marché, c'est-à-dire les fournisseurs, clients et consommateurs, et de calculer la taille totale du marché et la part de marché de chaque fournisseur en référence au produit ou service pertinent dans le domaine concerné. Cet exercice tient généralement compte de trois variables:

- a. le marché de produits, y compris les produits et services que les consommateurs considèrent comme interchangeables ou substituables; cet élément comprend la substituabilité du côté du fournisseur, c'est-à-dire la possibilité d'opérer un changement du côté de la production;
- b. le marché géographique, c'est-à-dire le territoire sur lequel les conditions de concurrence sont généralement homogènes et différent de celles de zones voisines; et
- c. un calendrier reflétant les changements dans les habitudes des consommateurs et les évolutions technologiques⁵⁷.

35. La Commission dispose d'une certaine flexibilité quand elle détermine la substituabilité. Elle tient non seulement compte des caractéristiques et de la destination du produit, mais aussi d'autres facteurs tels que les points de vue des clients et des concurrents, les témoignages sur les préférences des consommateurs et l'existence de différentes catégories de clients pour le produit⁵⁸.

3.2.4. La notion de bien-être du consommateur dans l'application des règles de concurrence

Voir parties 3.1.4 (Consentement et droit à l'information, etc.) et 3.3.2 (Obligations d'informations justes et exactes)

⁵⁵ Points 16, 17 et 18 des Orientations de la Commission, JO C 45 du 24.2.2009.

⁵⁶ Point 9 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

⁵⁷ Communication de la Commission sur la définition du marché en cause aux fins du droit communautaire de la concurrence, JO C 372 du 9.12.1997. Décision de la Commission du 24 juillet 1991 relative à une procédure d'application de l'article 86 du traité CEE (IV/31043 - Tetra Pak II) 92/163/CEE, JO L 072 du 18.3.1992.

⁵⁸ Points 36 à 43 de la Communication de la Commission sur la définition du marché en cause aux fins du droit communautaire de la concurrence.

36. Le droit communautaire ne définit pas le bien-être des consommateurs, et son lien avec l'efficacité du marché n'est pas généralement compris⁵⁹. En outre, la Cour de justice a rarement mentionné le bien-être du consommateur dans ses arrêts relatifs à des affaires de concurrence⁶⁰. Cela étant dit, comme la Commission le reconnaît dans ses lignes directrices relatives à l'application des règles en matière d'abus de position dominante⁶¹, le bien-être est déterminé non seulement par le prix, mais aussi par d'autres facteurs, tels que la qualité et le choix du consommateur, ce dernier étant également une préoccupation pertinente pour la protection des données. En outre, l'importance des intérêts des consommateurs revient, au moins au niveau conceptuel, dans chaque branche majeure du droit de la concurrence, à savoir:

- a. l'interdiction des accords anticoncurrentiels;
- b. la lutte contre les abus de position dominante sur le marché, par un comportement d'éviction (tel que le refus de fournir un produit ou service qui est nécessaire pour faire jouer la concurrence) ou par l'exploitation;
- c. le contrôle des concentrations; et
- d. le contrôle de l'aide d'État.

a) *Accords anticoncurrentiels*

37. L'article 101 du TFUE interdit les accords entre entreprises qui affectent le commerce entre États membres et qui ont pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence. Certains accords sont autorisés s'ils contribuent «à améliorer la production ou la distribution des produits ou à promouvoir le progrès technique ou économique, tout en réservant aux utilisateurs une partie équitable du profit qui en résulte», conformément aux dispositions de l'article 101, paragraphe 3, du TFUE.

b) *Abus de position dominante sur le marché: comportement d'éviction, refus de fourniture, installations essentielles et exploitation*

38. La dominance concurrentielle implique la capacité à déterminer des prix et à contrôler la production sur un marché donné. La dominance sur un marché donné ne constitue

⁵⁹ Les économistes comprennent généralement le bien-être des consommateurs comme l'évaluation par un individu de sa propre satisfaction quant aux avantages qu'il tire de la consommation de produits et services par rapport aux prix et aux revenus. Une mesure exacte du bien-être des consommateurs nécessite donc des informations sur les préférences individuelles; voir par exemple OCDE, «Glossary of Industrial Organisation Economics and Competition Law». Voir également Skourtis, A. (2012), «Is consumer welfare the (only) way forward? A re-appreciation of competition law objectives ante portas in both US and EU», University of Reading, Centre for Commercial Law and Financial Regulation, août 2012. Selon certains arguments, la politique de la concurrence devrait tenir compte d'objectifs sociaux et politiques plus larges; par exemple, Stucke, M. E., «Reconsidering Antitrust's Goals», Boston College Law Review, vol. 53 2012, p. 551 à 629; Stucke, M. E., «Reconsidering Competition», Mississippi Law Journal, vol. 81, 2011, p. 107 à 188.

⁶⁰ Akman, P. (2008), «'Consumer welfare' and Article 82EC: Practice and rhetoric», CCP Working Paper 08-25, juillet 2008.

⁶¹ Article 19 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

pas en soi une violation des règles de concurrence⁶². Cependant, l'abus de position dominante sur le marché qui affecte le commerce entre États membres est interdit par l'article 102 du TFUE. Un tel abus a tendance à être compris⁶³ comme prenant l'une des deux formes suivantes⁶⁴:

- i. un *comportement d'éviction*, dans lequel une entreprise dominante exclut des concurrents réels ou potentiels par d'autres moyens que la concurrence sur le fond des produits ou services qu'ils fournissent; et
- ii. l'*exploitation*, ou l'action qui porte «directement» atteinte à des consommateurs, par exemple en appliquant un prix excessivement élevé.

La Commission a publié des orientations concernant l'application au regard d'un comportement d'éviction⁶⁵ par des entreprises dominantes.

39. Le **comportement d'éviction** est abusif dès lors qu'il entraîne une «[éviction des] concurrents [de l'entreprise dominante] par des pratiques anticoncurrentielles» et donc des dommages potentiels à la structure de marché concurrentielle⁶⁶. Les orientations de la Commission identifient des formes spécifiques de comportement d'éviction, à savoir les accords exclusifs, les **ventes liées** et **groupées**, la prédation et le refus de fourniture ainsi que la compression des marges⁶⁷. Il peut s'agir, par exemple, de vente à des clients à un prix tellement bas que d'autres entreprises ne

⁶² Par conséquent, si la constatation de l'existence d'une position dominante n'implique en soi aucun reproche à l'égard de l'entreprise concernée, il lui incombe, indépendamment des causes d'une telle position, une responsabilité particulière de ne pas porter atteinte par son comportement à une concurrence effective et non faussée dans le marché commun [arrêt du 30 septembre 2003, Michelin/Commission (T-203/01, Rec. p. II-4071), point 57]. De même, si l'existence d'une position dominante ne prive pas une entreprise placée dans cette position du droit de préserver ses propres intérêts commerciaux, lorsque ceux-ci sont menacés, et si cette entreprise a la faculté, dans une mesure raisonnable, d'accomplir les actes qu'elle juge appropriés en vue de protéger ses intérêts, on ne peut cependant admettre de tels comportements lorsqu'ils ont pour objet de renforcer cette position dominante et d'en abuser [arrêts Metro/Commission, précité, point 189; du 1^{er} avril 1993, BPB Industries et British Gypsum/Commission (T-65/89, Rec. p. II-389), point 69; du 8 octobre 1996, Compagnie maritime belge transports e.a./Commission (T-24/93, T-25/93, T-26/93 et T-28/93., Rec. p. II-1201), point 107, et du 7 octobre 1999, Irish Sugar/Commission (T-228/97, Rec. p. II-2969), point 112].

⁶³ Whish, R. (2012), *Competition Law*, 7e éd., 2012, p. 201.

⁶⁴ Points 6 et 7 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

⁶⁵ L'objectif des mesures d'application prises par la Commission à l'égard des pratiques d'éviction est de faire en sorte que les entreprises dominantes n'entravent pas le libre jeu de la concurrence en évinçant leurs concurrents par des pratiques anticoncurrentielles, en ayant de ce fait un effet défavorable sur le bien-être des consommateurs, que ce soit sous l'effet de prix plus élevés que ceux qui auraient autrement été appliqués ou d'une autre manière, telle que la limitation de la qualité ou la réduction du choix pour les consommateurs. Dans le présent document, l'expression «éviction anticoncurrentielle» décrit une situation dans laquelle un accès effectif des concurrents réels ou potentiels aux sources d'approvisionnement ou aux marchés est entravé ou supprimé sous l'effet du comportement de l'entreprise dominante, ce qui va probablement permettre à cette dernière d'augmenter rentablement les prix au détriment des consommateurs. L'existence d'un préjudice probable pour les consommateurs peut être déterminé sur la base de preuves qualitatives et, lorsque cela est possible et approprié, de preuves quantitatives. La Commission examinera en outre cette éviction anticoncurrentielle à la fois au niveau intermédiaire et/ou à celui du consommateur final»; point 19 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

⁶⁶ Points 5 et 19 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

⁶⁷ Points 75 à 90 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes.

pourront pas pénétrer le marché (ventes groupées) ou du fait d'obliger les clients d'un service populaire à acheter un autre service du vendeur que le client n'a pas demandé (ventes liées). De telles actions sont réputées être «les plus préjudiciables aux consommateurs» et avoir «un effet défavorable sur le bien-être des consommateurs», même si on ne sait pas comment ni pourquoi elles peuvent se produire.

40. Une forme de comportement d'éviction, le **refus de fourniture**, englobe le concept d'«**installations essentielles**»⁶⁸. Une installation essentielle est «un produit ou un service qui est objectivement nécessaire pour pouvoir exercer une concurrence efficace» et pour lequel il n'existe pas de produit ou service alternatif et dont le développement d'une solution alternative est rendu impossible ou excessivement difficile par des obstacles techniques, juridiques ou économiques⁶⁹. Le refus de fourniture est susceptible de conduire à l'élimination d'une concurrence effective» ou de léser le consommateur. Le consommateur sera probablement lésé «par exemple[...] lorsque les concurrents évincés par l'entreprise dominante sont, du fait de ce refus, dans l'impossibilité de mettre sur le marché des produits ou des services innovants et/ou lorsque l'innovation subséquente est susceptible d'être freinée», en particulier si le concurrent «a l'intention d'offrir des produits ou des services pour lesquels il existe une demande potentielle ou qui sont susceptibles de contribuer au développement technique»⁷⁰.
41. L'**exploitation** abusive, qui serait la plus à même de léser le consommateur, telle que l'application de prix excessifs ou une discrimination injuste, n'a pas été traitée dans des orientations de la Commission. Elle a rarement été prise en compte par les autorités de la concurrence et, dans la plupart des cas, les «victimes» d'exploitation ont été des entreprises, et non des consommateurs finals⁷¹. La jurisprudence a toutefois établi que la pratique d'un prix excessif consisterait à appliquer un prix sans rapport raisonnable avec la valeur économique du produit fourni⁷². La Cour de justice a également élaboré un test en deux étapes selon lequel la Commission doit déterminer:

⁶⁸ La doctrine des installations essentielles vient de la jurisprudence américaine et elle dispose que les propriétaires d'installations essentielles sont tenus de faire affaire avec des concurrents («obligation de fourniture»). Elle n'a pas été expressément citée par la Cour de justice, mais dans l'arrêt du 26 novembre 1998, *Bronner* (C-7/97, Rec. p. I-7791), la Cour de justice a restreint l'obligation de fourniture à des situations dans lesquelles le propriétaire d'une installation essentielle détenait plus qu'une position dominante. La Cour de justice a également introduit un test d'avant-garde sur la question de savoir si le refus de fourniture entraînerait une monopolisation d'un marché en aval; voir Evvard, S. J. (2004), «Essential facilities in the European Union: *Bronner and beyond*», *Columbia Journal of European Law* 491, 2004.

⁶⁹ Voir *Bronner* et l'arrêt du 29 avril 2004, *IMS Health*. (C-418/01, Rec. p. I-5039), selon lesquels une «installation essentielle» peut être comprise comme les unités d'informations ou «modules» concernant des pharmacies et des docteurs utilisées par une entreprise dominante pour analyser, par zone géographique, les ventes de médicaments pour lesquels elle détient un droit d'auteur en vertu de la législation d'un État membre. En théorie, toute entreprise concurrente peut construire sa propre «structure modulaire», mais il a été retenu que l'entreprise dominante avait acquis cette structure modulaire en question au moyen d'effets de réseau et d'une participation économique élevée des utilisateurs de la structure modulaire (point 30).

⁷⁰ Point 87 des Orientations de la Commission sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes. L'arrêt majeur de la Cour de justice dans ce domaine reste l'arrêt du 17 septembre 2007, *Microsoft/Commission* (T-201/04, Rec. p. II-3601).

⁷¹ Hubert, P., et Combet, L., «Exploitative abuse: The end of the Paradox?», *Doctrines I Concurrences* n° 1-2011, p. 44 à 51.

⁷² Arrêt du 14 février 1978, *United Brands/Commission* (27/76, Rec. p. 207), point 250.

(a) si le montant de la marge bénéficiaire est excessif en comparant le prix contesté et les coûts de production et, si oui,

(b) si le prix est (i) injuste en lui-même ou (ii) injuste par rapport aux produits concurrents.

c) *Contrôle des concentrations*

42. Le règlement (CE) n° 139/2004 du Conseil (ci-après le «règlement sur les concentrations»)⁷³ s'applique aux **concentrations** à «dimension communautaire» qui apportent des «modifications structurelles importantes dont l'effet sur le marché s'étend au-delà des frontières nationales d'un État membre». Une concentration à dimension communautaire relève du champ d'application du règlement et, par conséquent, est examinée par la Commission si le chiffre d'affaires combiné des entreprises est supérieur à des seuils spécifiques⁷⁴. Le système communautaire de contrôle des concentrations vise à contrôler les concentrations d'entreprises (généralement qualifiées de «fusions» ou «fusions-acquisitions») et leur effet sur la concurrence, tout en tenant compte d'autres facteurs tels que les «intérêts des consommateurs intermédiaires et finals»⁷⁵. Dans l'affaire Google/DoubleClick, la Commission avait affirmé s'être «exclusivement» référée au risque que la concentration entrave la concurrence effective dans le marché commun, tout en précisant que sa décision était sans préjudice des obligations de l'entité issue de la fusion au titre de la directive relative à la protection des données⁷⁶.

d) *Exceptions à l'aide d'État*

43. Conformément à l'article 107 du TFUE, l'**aide d'État** est définie comme tout transfert des ressources d'un État membre qui crée un avantage sélectif pour une ou plusieurs entreprises commerciales, a la possibilité de fausser le commerce sur le marché commercial concerné et affecte le commerce entre États membres. Une telle pratique est illégale, mais un certain nombre d'exceptions s'appliquent, par exemple dans le cas de la protection environnementale, où il est possible que les entreprises ne soient pas incitées à réduire leur pollution en raison du coût associé⁷⁷. Il serait concevable de plaider pour que l'aide d'État incite les industries naissantes à adopter des technologies et services renforçant la protection de la vie privée dans l'Union européenne⁷⁸.

⁷³ Voir note de bas de page 49.

⁷⁴ Article 1 du règlement sur les concentrations. La Commission est tenue de rendre compte de l'exploitation de ces seuils et peut en proposer la révision.

⁷⁵ Article 2, paragraphe 1, point b), du règlement sur les concentrations.

⁷⁶ Affaire COMP/M.4731 Google/DoubleClick. DoubleClick était un prestataire de technologie publicitaire, à savoir de logiciels utilisés pour garantir que des publicités correctement ciblées s'affichent sur la page Web que visite un utilisateur donné.

⁷⁷ Considérant 45, règlement (CE) n° 800/2008 de la Commission du 6 août 2008 déclarant certaines catégories d'aide compatibles avec le marché commun en application des articles 87 et 88 du traité (règlement général d'exemption par catégorie).

⁷⁸ En 2014, la Commission a l'intention de compléter son programme de modernisation des aides d'État dans des secteurs clés; annexes au programme de travail de la Commission pour l'année 2014, COM(2013) 739 final, 22 octobre 2013, p. 6.

3.2.5. Supervision, exécution, sanctions et accès aux voies de recours en cas de violations

Voir parties 3.1.5 et 3.3.3 sur la supervision, etc.

44. Les règles de concurrence sont appliquées par les autorités nationales de la concurrence ou par la Commission. Pour les concentrations, tout dépend de l'existence d'une dimension communautaire. Pour les accords anticoncurrentiels ou les cas d'abus, l'autorité qui est «bien placée» traitera l'affaire en question⁷⁹. Les autorités de concurrence peuvent tenir compte de considérations politiques plus larges⁸⁰. À cet égard, la Commission est tenue par les traités [article 2 du traité sur l'Union européenne (ci-après le «TUE») et article 2 du TFUE] de «placer son appréciation dans le cadre général» des objectifs et valeurs de l'Union européenne, qui englobent évidemment les droits à la vie privée et à la protection des données. Les autorités de concurrence se sont montrées favorables à une interprétation restrictive centrée sur les efficacités économiques objectives dans un marché intérieur compétitif, bien que des considérations relatives au bien-être des consommateurs puissent être «en pleine ascension»⁸¹.
45. Les règles sont encadrées par un solide système de sanctions. Par exemple, une entreprise reconnue comme ayant enfreint des règles relatives aux accords anticoncurrentiels peut être redevable d'une amende maximale correspondant à 10 % de son chiffre d'affaires total de groupe de l'année précédente⁸². Toutefois, il n'existe aujourd'hui aucune harmonisation des droits qui permettent aux consommateurs, collectivement ou individuellement, de solliciter en justice l'arrêt d'une violation de règles de concurrence ou une réparation suite à une telle violation, bien que de telles réclamations puissent être présentées devant des juridictions nationales⁸³.
46. Le réseau européen de la concurrence agit comme un forum de discussion et de coopération entre les autorités réglementaires dans des affaires impliquant l'application des articles 101 et 102 du TFUE⁸⁴. Il vise à garantir une division efficace du travail et une application effective et cohérente des règles de concurrence de l'Union européenne. Le réseau comprend des groupes d'experts dans certains secteurs spécifiques, tels que l'informatique, l'information et la communication.

⁷⁹ Les affaires sont attribuées par l'intermédiaire du réseau européen de la concurrence (voir note de bas de page 84).

⁸⁰ Voir <http://www.utrechtlawreview.org/index.php/ulr/article/view/URN%3ANBN%3ANL%3AUI%3A10-1-101035/16>; http://cadmus.eui.eu/bitstream/handle/1814/22688/2012_guidi_authorversion.pdf?sequence=1

⁸¹ Whish (2012), p. 19. Aux États-Unis, où la tendance est à une approche sectorielle de la législation relative à la vie privée et où il n'existe pas une seule mesure de protection des données comparables à la directive de l'Union européenne relative à la protection des données, la réglementation de la concurrence est aussi allée vers une approche puriste: «Non seulement la Commission n'a pas l'autorité légale pour imposer des conditions à cette concentration sans rapport avec la lutte antitrust, mais réglementer les exigences en matière de vie privée d'une seule et unique entreprise pourrait, en soi, porter une atteinte sérieuse à la concurrence dans cette vaste industrie qui connaît une rapide évolution», déclaration de la Federal Trade Commission concernant Google/DoubleClick, FTC dossier n° 071-0170.

⁸² Article 23, paragraphe 2, du règlement (CE) n° 1/2003.

⁸³ Arrêt du 13 juillet 2006, Manfredi (C-295/04 à C-298/04, Rec. p. I-6619). La Commission enquête sur l'exécution privée et a proposé un projet de directive en la matière; Proposition de directive du Parlement européen et du Conseil relative à certaines règles régissant les actions en dommages et intérêts en droit interne pour les infractions aux dispositions du droit de la concurrence des États membres et de l'Union européenne, COM(2013) 404 final.

⁸⁴ Établi par la communication de la Commission relative à la coopération au sein du réseau des autorités de concurrence, 2004/C 101/3, JO C 101 du 27.4.2004.

3.3. *Protection des consommateurs*

3.3.1. **L'exigence de garantir un niveau élevé de protection des consommateurs**

Voir parties 3.1.1 (Droit fondamental à la protection des données) et 3.2.1 (Objectifs des règles de concurrence de l'Union européenne)

47. Le droit communautaire en matière de protection des consommateurs vise à supprimer les barrières au marché intérieur en établissant la confiance envers les produits et services dans l'ensemble du marché intérieur, sur la base de la transparence et de la bonne foi⁸⁵. L'article 38 de la Charte impose aux politiques européennes de garantir un niveau élevé de protection des consommateurs. L'article 12 du TFUE impose de prendre en considération les exigences de la protection des consommateurs dans la définition et la mise en œuvre des politiques et actions de l'Union européenne en général. L'article 169 du TFUE dispose que l'Union européenne doit contribuer à la protection de la santé, de la sécurité et des intérêts économiques des consommateurs ainsi qu'à la promotion de leur droit à l'information, à l'éducation et à s'organiser afin de préserver leurs intérêts.
48. L'Union européenne a dûment adopté diverses mesures pour la protection des utilisateurs de produits et services quel que soit l'endroit du marché intérieur où ils sont fournis ou consommés. Chaque mesure a été justifiée par le fait que la diversité des normes et des niveaux de confiance des consommateurs a un effet néfaste sur le bon fonctionnement du marché intérieur et fausse la concurrence, tandis que des normes communes, un choix et une équité sont bénéfiques. Le dernier programme d'action pluriannuel souligne la nécessité de disposer d'informations exactes et d'établir une transparence du marché, de promouvoir le bien-être des consommateurs en matière de prix, de choix, de qualité, de diversité, d'accessibilité financière et de sécurité, ainsi que de protéger les consommateurs contre les risques potentiels⁸⁶.

3.3.2. **Obligations d'équité et de fourniture d'informations exactes**

Voir parties 3.1.4 (Consentement et droit à l'information, etc.) et 3.2.4 (Bien-être des consommateurs dans les règles de concurrence)

49. Dans les contrats conclus avec les consommateurs, les fournisseurs ont l'avantage dans la définition des modalités qui ne sont pas négociées avec des consommateurs individuels. La **directive «clauses abusives»**⁸⁷ a donc introduit la notion de «bonne foi» et imposé que les clauses contractuelles soient rédigées en des termes clairs et intelligibles, tout d'abord quant à la signification d'un terme devant être interprété en faveur du consommateur. Selon la **directive sur l'indication des prix**⁸⁸, les professionnels doivent indiquer le prix de vente de façon aisément identifiable et

⁸⁵ Voir partie 3.3.2. Le terme «consommateur», selon la législation secondaire de l'Union européenne, désigne «toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale».

⁸⁶ Décision n° 1926/2006/CE du Parlement européen et du Conseil du 18 décembre 2006 établissant un programme d'action communautaire dans le domaine de la politique des consommateurs (2007-2013).

⁸⁷ Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.

⁸⁸ Directive 98/6/CE du Parlement européen et du Conseil du 16 février 1998 relative à la protection des consommateurs en matière d'indication des prix des produits offerts aux consommateurs.

clairement lisible. La **directive relative aux droits des consommateurs**⁸⁹ va plus loin en visant à éliminer les charges et coûts cachés lors de transactions «hors établissement», en particulier sur l'internet, notamment lorsque des personnes sont trompées et amenées à payer pour des services présentés comme «gratuits». Cette dernière impose aux professionnels d'informer les consommateurs sous «une forme claire et compréhensible» sur le «prix total des biens ou services [...] ou lorsque le prix ne peut être raisonnablement calculé à l'avance du fait de la nature du bien ou du service [...]» [article 6, point e)]. Plus précisément, les professionnels sont tenus de fournir des informations sur le contenu des services numériques⁹⁰, telles que leur compatibilité avec du matériel et des logiciels.

50. La **directive sur les pratiques commerciales déloyales**⁹¹ définit les pratiques commerciales trompeuses comme celles qui omettent une information (notamment le prix) dont le consommateur moyen a besoin pour prendre une décision commerciale en connaissance de cause et, par conséquent, l'amène ou est susceptible de l'amener à prendre une décision commerciale qu'il n'aurait pas prise autrement. Une telle omission trompeuse inclurait des cas dans lesquels un professionnel «dissimule une information substantielle [...] ou la fournit de façon peu claire, inintelligible, ambiguë ou à contretemps, ou lorsqu'il n'indique pas sa véritable intention commerciale dès lors que celle-ci ne ressort pas déjà du contexte» (article 7). Par exemple, il est trompeur de décrire un produit comme étant «gratuit» ou «sans frais» si le consommateur doit payer autre chose que les coûts inévitables liés au fait de répondre à la pratique commerciale et de prendre possession ou de régler la livraison de l'article, ou de donner l'impression fautive que le professionnel n'agit pas à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale (annexe I). Cela est complété par la **directive sur la publicité trompeuse et comparative**⁹², qui impose aux États membres de prendre des mesures pour lutter contre la publicité trompeuse et qui autorise la publicité comparative à condition qu'elle soit objective et ne soit pas source de confusion parmi les professionnels et les concurrents.

51. Enfin, l'Union européenne a mis en place des garanties générales et spécifiques à certains secteurs contre les risques pour la santé et la sécurité des consommateurs. La **directive relative à la sécurité générale des produits**⁹³ définit comme «sûr» tout produit qui «dans des conditions d'utilisation normales ou raisonnablement prévisibles [...] ne présente aucun risque ou seulement des risques réduits à un niveau

⁸⁹ Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil.

⁹⁰ Le contenu numérique est défini comme «les données qui sont produites et fournies sous une forme numérique, comme les programmes informatiques, les applications, les jeux, la musique, les vidéos ou les textes, que l'accès à ces données ait lieu au moyen du téléchargement ou du streaming, depuis un support matériel ou par tout autre moyen», considérant 19 de la directive 2011/83/UE.

⁹¹ Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (JO L 304 du 22.11.2011).

⁹² Directive 2006/114/CE du Parlement européen et du Conseil du 12 décembre 2006 en matière de publicité trompeuse et de publicité comparative.

⁹³ Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits (JO L 011 du 15.01.2002).

bas compatibles avec l'utilisation du produit et considérés comme acceptables dans le respect d'un niveau élevé de protection de la santé et de la sécurité des personnes, compte tenu, en particulier: i) des caractéristiques du produit [...] iii) de la présentation du produit [...] iv) des catégories de consommateurs se trouvant dans des conditions de risque au regard de l'utilisation du produit, en particulier des enfants et des personnes âgées».

52. La fourniture d'informations claires sur le coût et la valeur d'un service au consommateur est donc constamment mise en avant dans les différents actes, ce qui reflète le droit de l'individu, en vertu de la directive relative à la protection des données, d'obtenir des informations sur le traitement de données «sous une forme intelligible». La préoccupation concernant la sécurité des produits, parallèlement, complète à la fois le concept de l'exploitation en droit de la concurrence et l'accent mis, dans la proposition de règlement général sur la protection des données, sur l'analyse d'impact⁹⁴, ainsi que les discussions ultérieures sur une approche progressive basée sur les risques et sur le principe de la responsabilité⁹⁵.

3.3.3. Supervision, exécution, sanctions et accès aux voies de recours en cas de violations

Voir parties 3.1.5 et 3.2.5 sur la supervision, etc.

53. Les autorités nationales sont responsables de l'exécution des règles relatives à la protection des consommateurs au sein de l'Union européenne. Peu d'autorités ont le pouvoir d'obtenir une réparation pécuniaire pour des consommateurs⁹⁶.

54. Il n'existe pas d'approche communautaire commune concernant les enquêtes sur des violations du droit de la concurrence, sauf s'il s'agit d'«infractions intracommunautaires», c'est-à-dire tout acte ou toute omission qui «porte ou est susceptible de porter atteinte aux intérêts collectifs des consommateurs résidant dans un ou plusieurs États membres autres que celui où l'acte ou l'omission en question a son origine ou a eu lieu»⁹⁷. À cette fin, les États membres sont tenus de désigner des autorités compétentes chargées de coopérer les unes avec les autres pour garantir le respect de ces règles, le bon fonctionnement du marché intérieur et la protection des intérêts économiques des consommateurs. Ces autorités ont le droit d'enquêter sur des suspicions d'infractions intracommunautaires, de demander que le vendeur ou le fournisseur concerné mette fin à l'infraction et d'imposer un «paiement» de la «partie perdante» en cas de non-exécution d'une décision de justice.

⁹⁴ Article 33, COM(2012) 11 final.

⁹⁵ «Observations complémentaires du CEPD sur le paquet de mesures pour une réforme de la protection des données», 15 mars 2014.

⁹⁶ OCDE, «Consumer Dispute Resolution and Redress in the Global Marketplace», 2006.

⁹⁷ Règlement (CE) n° 2006/2004 du Parlement européen et du Conseil du 27 octobre 2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs («règlement relatif à la coopération en matière de protection des consommateurs»).

55. Les autorités nationales au sein de l'Espace économique européen forment le réseau Concurrence Protection Coopération (ou «CPC») ⁹⁸ qui identifie chaque année des priorités communes d'exécution et met en œuvre des activités d'exécution concertées, notamment des contrôles simultanés de la conformité aux règles relatives aux consommateurs et des projets conjoints dans des secteurs spécifiques. Ce cadre de coopération est actuellement en cours d'examen.

4. Interfaces entre le droit de la concurrence, la protection des consommateurs et la protection des données

- *Le marché des services gratuits dans un nombre croissant de secteurs de l'économie numérique n'a pas encore été analysé, mais il est évident que le contrôle de volumes considérables de données au sujet des utilisateurs des services confère un certain pouvoir*
- *L'étendue de l'abus de position dominante sur le marché et du préjudice subi par les consommateurs par le refus d'accès à des informations personnelles et du fait de politiques de confidentialité opaques ou trompeuses peuvent justifier un nouveau concept d'atteinte aux consommateurs pour l'exécution de la concurrence dans l'économie numérique*
- *L'application de règles de concurrence aux marchés numériques devrait permettre de promouvoir des services renforçant la protection de la vie privée et un meilleur contrôle de leurs propres données par les consommateurs*

56. La partie précédente a mis en évidence les principales caractéristiques des règles en matière de protection des données, de concurrence et de protection des consommateurs en cas de préoccupations communes. Cette partie aborde plus en détail *quatre aspects de cette convergence politique* dans le contexte de ces marchés de services fondés sur des informations personnelles. L'argument est que, dans ces domaines, la vie privée et la protection des données à caractère personnel devraient être considérées non comme des préoccupations annexes, mais plutôt comme des facteurs centraux dans l'évaluation des activités des entreprises et de leur impact sur la compétitivité, l'efficacité du marché et le bien-être des consommateurs.

4.1. Les marchés pertinents et le pouvoir de marché dans l'économie numérique

Voir parties 3.1.3 (Finalités légitimes et compatibles du traitement de données) et 3.2.3 (Définition du marché pertinent)

⁹⁸ Communication de la Commission présentée conformément à l'article 5, paragraphe 2, du règlement (CE) n° 2006/2004 du Parlement européen et du Conseil relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, concernant les autorités compétentes et les bureaux de liaison uniques, JO C 185 du 23.6.2012.

Les jeux «freemium» en ligne sont disponibles gratuitement dès lors que les utilisateurs s'enregistrent et communiquent des informations personnelles. Ces jeux contrôlent l'activité en ligne pour déterminer comment convertir des bénéficiaires sans contrepartie en clients payants ou pour proposer des formes ciblées et plus lucratives de publicité. Une petite minorité d'utilisateurs paie des fonctionnalités supplémentaires, mais une part de recettes encore assez importante est générée par des «bénéficiaires sans contrepartie» ou des joueurs «non payants». Dans l'Union européenne, 46 % des utilisateurs des réseaux sociaux ou sites de partage se sentent insuffisamment informés des possibles conséquences de la divulgation d'informations personnelles. L'Office for Fair Trading du Royaume-Uni a également enquêté sur les paiements d'applications intrajeu et identifié de possibles manquements au droit de la consommation, non des moindres dans le cadre de pratiques pouvant s'apparenter à un chantage affectif, afin d'établir une approche commune pour relever les normes industrielles au niveau international.

Sources: EU Kids Online, «Zero to Eight: Young Children and their Internet Use», août 2013; Hoofnagle et Whittington, «Free: Accounting for the Costs of the Internet's Most Popular Price»; Eurobaromètre 359; site web de l'OFT.

4.1.1. Les marchés de services payés au moyen d'informations personnelles

57. Aucune analyse complète du marché pour chaque service numérique «gratuit» n'a encore été réalisée⁹⁹. Dans son analyse de la fusion Google/DoubleClick, la Commission a considéré que seuls les services payants, c'est-à-dire la vente directe d'espace publicitaire en ligne, les services intermédiaires de publicité en ligne et la fourniture de technologie de diffusion d'affichages publicitaire, étaient pertinents¹⁰⁰. Depuis la clôture de cette affaire, l'évolution de l'économie numérique a été marquée par une explosion de la collecte de données. Aujourd'hui, une analyse de marché pertinente équivalente étudierait les nouveaux modèles d'entreprise et évaluerait la valeur des informations personnelles comme actif incorporel. Une telle analyse pourrait révéler la nécessité pour les entreprises de collecter des volumes considérables de données afin de pouvoir monétiser le service proposé, principalement par le biais de la publicité, tout en faisant concurrence à d'autres prestataires de services rémunérés.

58. Une analyse de la concurrence pourrait aussi tenir compte de la substituabilité des produits et services, eu égard aux avis des consommateurs et des concurrents et des preuves des préférences des consommateurs, conformément aux lignes directrices existantes de la Commission. De puissants fournisseurs de divers services numériques peuvent initialement collecter des données à caractère personnel à grande échelle sur un marché pour fournir un certain service sur ce marché. L'un de ces fournisseurs pourrait ensuite traiter ces données, ce qui pourrait être défini comme un intrant en termes de concurrence, afin de fournir un autre service et/ou de vendre les données en vue de leur traitement par une autre entreprise fournissant des services sur un autre marché distinct. Si, selon l'analyse, le «second» type de service utilisant les données comme intrant relève d'un marché distinct, ce service serait présumé non substituable au service pour lequel les données ont été initialement collectées. Par conséquent,

⁹⁹ Discours du vice-président Almunia (voir note de bas de page 2).

¹⁰⁰ Voir note de bas de page 76.

l'analyse de la concurrence pourrait étayer la conclusion selon laquelle, du point de vue de la protection des données, les données sont traitées à des fins distinctes et éventuellement incompatibles à l'insu des personnes qui les ont fournies. Une telle conclusion serait encore plus évidente dans les cas où les deux types de services sont perçus par les consommateurs comme étant très différents. L'application de règles de concurrence pourrait donc aider à identifier des cas de manquement au droit de la protection des données.

59. L'analyse devrait tenir compte de la rapidité d'évolution sur les marchés technologiques. L'expansion d'une entreprise et l'élargissement de sa gamme de services peuvent brouiller les frontières entre les marchés. La convergence technologique a transformé des produits jusque-là complémentaires en substituts: par exemple, des dispositifs mobiles font désormais directement concurrence à des ordinateurs portables et ordinateurs de bureau, ce qui n'était pas le cas il y a dix ans. En outre, les marchés géographiques dans l'économie numérique peuvent être évasifs puisque certains services, tels que la recherche, le courriel et le partage de fichiers, ne sont pas confinés à une zone ou un état donné, mais sont disponibles de façon homogène dans l'ensemble de l'environnement mondial en ligne¹⁰¹.

4.1.2. Mesurer le pouvoir du marché numérique

60. Une fois définis les marchés pertinents pour ces services, l'étape suivante consisterait à évaluer le pouvoir du marché. Le pouvoir dans l'économie numérique est en partie déterminé par le niveau auquel une entreprise donnée peut réellement, potentiellement ou hypothétiquement collecter et diffuser des informations personnelles. Mesurer le contrôle des informations personnelles serait un exercice difficile. Une part de marché pertinente détenue par le prestataire d'un service en ligne gratuit ne peut pas être calculée facilement à l'aide de données sur les ventes traditionnelles ou le volume. Ces difficultés pourraient être surmontées si les autorités de concurrence, de protection des consommateurs et de protection des données collaboraient pour identifier des scénarios et définir une norme de mesure du pouvoir du marché dans ce domaine. Cette norme pourrait ensuite être utilisée pour apprécier des suspicions d'infractions dans les trois domaines.

61. Quant à savoir si des manquements aux règles de concurrence et de protection des données devraient être établis, une connaissance plus approfondie de ces marchés et des finalités pour lesquelles des informations personnelles sont traitées serait bénéfique à l'exécution. Des législateurs mieux informés seraient plus à même de détecter les acteurs dominants du marché dont les pratiques sont anticoncurrentielles ou déloyales ou qui ne fournissent pas d'informations précises aux consommateurs. Les implications pour le bien-être des consommateurs deviendraient donc plus claires. Si les législateurs ne reconnaissent pas l'importance croissante des informations personnelles comme actif incorporel, de plus en plus de services fondés sur le traitement de données massives à caractère personnel pourraient effectivement être «cantonnés» en dehors du champ d'application des règles de concurrence et de protection des consommateurs.

¹⁰¹ Il a été retenu, en revanche, que le marché publicitaire en ligne était divisé selon des frontières nationales et linguistiques; Brockhoff, J. et al., «Google/Double Click: The first test for the Commission's non-horizontal merger guidelines», Competition Policy Newsletter n° 2, 2008.

4.2. *Pouvoir du marché numérique et considérations relatives au bien-être des consommateurs*

Une entreprise dominante sur le marché des services de messagerie électronique lance une nouvelle plateforme de partage de photos. Le produit est proposé gratuitement dans une offre groupée avec le service de messagerie. Les utilisateurs du service de messagerie sont incités à télécharger et utiliser la plateforme sans étude sérieuse. Les opportunités pour l'entreprise en termes d'observation et d'élaboration de profil de comportement de l'utilisateur en sont accrues. Les consommateurs deviennent de plus en plus dépendants du service de partage de photos à mesure qu'ils téléchargent des photos et postent des liens vers l'une de leurs photos sur leurs profils de réseaux sociaux, de sorte que, un peu plus tard, l'entreprise commence à demander un paiement pour une mise à niveau vers une version «premium» du service et affaiblit les contrôles de la protection des données en imposant une politique de confidentialité revue pour la version «gratuite». Les consommateurs sont bel et bien enfermés dans le service en raison du temps et de l'effort nécessaires pour récupérer et recréer les données requises afin de rejoindre un autre fournisseur. Parallèlement, les incitations de concurrents potentiels à pénétrer le marché sont diminuées puisqu'ils ne sont pas en mesure d'attirer un volume critique d'utilisateurs pour faire concurrence. Cela pourrait soulever des questions de comportement d'éviction par la vente groupée, voire d'exploitation, si le «prix» payé du fait de la remise d'informations personnelles était jugé excessif par rapport à la valeur du service consommé et si les informations transmises étaient insuffisamment précises.

4.2.1. **Appréciation de concentrations**

Voir partie 3.2.4, point c) (Contrôle des concentrations)

62. Conformément au règlement sur les concentrations¹⁰², les autorités vérifient si la concentration déclencherait une dynamique susceptible d'«entraver de manière significative une concurrence effective». Si, dans l'économie numérique, le pouvoir du marché peut être mesuré en fonction du contrôle d'informations personnelles commercialisables (voir point 4.1.3 ci-dessus), les décisions de concentration pourraient tenir compte des effets d'association de ces capacités sur le marché.
63. À ce jour, la décision la plus significative de la Commission concernant une concentration entre entreprises de l'économie numérique est celle concernant Google et DoubleClick¹⁰³. La Commission, appliquant les critères de calcul du seuil, avait déterminé que la concentration ne présentait pas de dimension communautaire. L'affaire avait néanmoins été examinée par la Commission après une saisie par les parties à la concentration, celle-ci pouvant être examinée en vertu des législations nationales de plusieurs États membres¹⁰⁴. À l'époque, Google était signalée comme

¹⁰² Voir note de bas de page 73.

¹⁰³ Voir partie 3.2.4, point c).

¹⁰⁴ Article 4, paragraphe 5, du règlement sur les concentrations.

étant à la tête d'un quasi-monopole de la recherche en Europe¹⁰⁵ et décrivait la nature de son activité comme la prestation d'un service de recherche en ligne, ainsi que de publicité¹⁰⁶. La Commission n'avait cependant pas tenu compte du marché de la recherche et avait plutôt considéré le marché de produits de Google comme ayant «pour principale activité la fourniture d'espaces publicitaires en ligne». Analysant dans quelle mesure l'association des bases de données sur les recherches de clients et le comportement de navigation des deux entreprises affecterait la concurrence sur le marché pertinent, la Commission avait conclu que l'association ne créerait pas «d'avantage compétitif dans le secteur publicitaire qui ne puisse être reproduit par d'autres acteurs ayant accès à des données similaires concernant un usage en ligne».

64. Avec cette approche purement économique de l'affaire, la Commission n'avait pas cherché à savoir comment la concentration aurait pu affecter les utilisateurs dont les données seraient traitées ultérieurement par la fusion des ensembles de données des deux sociétés, probablement pour fournir des services, peut-être sous forme d'offre groupée ou conjointement à chaque simple service de recherche, qui n'étaient pas envisagés au moment où les données avaient été initialement soumises. La décision ne mentionnait ni le bien-être des consommateurs, ni les utilisateurs des moteurs de recherche de Google, alors même que chaque internaute dans l'Union européenne était potentiellement concerné. Elle n'avait donc 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.
65. La Commission avait certes analysé l'effet sur les consommateurs, mais dans deux décisions ultérieures concernant des entreprises de l'économie numérique. Examinant le projet d'acquisition de Tele Atlas (fournisseur de bases de données de cartes numériques) par TomTom (fabricant d'appareils de navigation portables et fournisseur de logiciels GPS), la Commission avait examiné une théorie d'atteinte concurrentielle et de protection de la «confidentialité» de la clientèle, concluant que l'entité fusionnée serait probablement incitée à atténuer toutes préoccupations pouvant aboutir à la perte de clients en faveur de concurrents¹⁰⁷. Dans l'affaire de l'achat envisagé par Microsoft des activités de recherche en ligne et de publicité de Yahoo!, la Commission avait étudié la capacité accrue de Microsoft, après l'acquisition, à utiliser son pouvoir de marché pour influencer sur des négociations d'accords de distribution, par exemple par l'offre groupée de produits¹⁰⁸. Elle avait

¹⁰⁵ Rapport de la conférence Search Engine Strategies, 13 au 15 février 2007. Londres, <http://searchenginewatch.com/article/2066064/Stats-Show-Google-Dominates-the-International-Search-Landscape> et comparaison avec la tendance constante depuis ces dates http://gs.statcounter.com/#search_engine-eu-monthly-200807-201402 (consultés le 25 février 2014).

¹⁰⁶ Rapport annuel Google Inc. pour 2008 (voir http://investor.google.com/pdf/2008_google_annual_report.pdf). L'enquête de marché de la Commission n'avait toutefois pas conclu que d'autres marchés pertinents présentaient une dimension correspondant à l'EEE. Brockhoff et al. Selon l'eurobaromètre 299, seuls 7,4 % des achats en lignes sont transfrontaliers.

¹⁰⁷ Le raisonnement de la Commission dans cette affaire était que la perte de confidentialité pourrait être considérée comme similaire à une dégradation de produit pouvant aboutir à la perte de clients en faveur d'un rival qui ne serait pas compensée par des gains en aval; décision de la Commission du 14 mai 2008 déclarant une concentration compatible avec le marché commun et le fonctionnement de l'accord EEE, affaire n° COMP/M.4854 – TOMTOM/TELE ATLAS, C(2008)1859, points 272 à 275.

¹⁰⁸ Décision de la Commission du 18 février 2010 [affaire n° COMP/M.5727 – MICROSOFT/YAHOO! SEARCH BUSINESS, C(2010), 1077].

conclu que la possibilité d'une atteinte significative pour les utilisateurs des services de recherche en ligne de Yahoo! était peu probable.

4.2.2. Accès aux marchés et intrant de concurrents

Voir parties 3.1.3 (Finalités légitimes et compatibles du traitement de données), 3.1.4 (Consentement et droits à l'information, etc.), 3.2.4 point b) (Abus de position dominante sur le marché) et 4.1.3 (Mesurer le pouvoir de marché)

66. Dans des marchés numériques bifaces, tels que la prestation de multiples services «gratuits» en vue de collecter des données, couplée à la fourniture d'espaces publicitaires comportementaux en ligne, les coûts marginaux de la prestation de services en ligne sur un nouveau marché sont faibles et il existe une tendance nette au groupement de services (voir point 39). Des entreprises puissantes ou dominantes sont en mesure d'exploiter des «économies d'agrégation»¹⁰⁹ et de créer des barrières à l'entrée du fait de leur contrôle d'ensembles volumineux de données à caractère personnel associés à des logiciels propriétaires qui organisent les données. En théorie, l'information pourrait être considérée comme une installation essentielle sur un marché numérique particulier (point 40): l'entreprise dominante a le contrôle exclusif de l'information, tandis que les concurrents n'ont pas les moyens techniques de recréer la structure ou le système sur lequel repose le service. Cela empêche effectivement l'entrée sur le marché et limite le choix des consommateurs concernant les services «gratuits» en question. Simultanément, les coûts du marché publicitaire augmentent du fait de l'absence d'offres concurrentes.
67. L'accès à des informations personnelles pourrait légalement être accordé à des concurrents sur la base d'un consentement ou d'autres motifs légitimes, mais cela constitue un obstacle considérable au regard du droit en matière de protection des données (voir partie 3.1.4). Une entreprise dominante pourrait ainsi chercher à justifier son refus de fournir des ensembles de données à des concurrents, y compris dans le cadre d'accords d'exclusivité, en affirmant qu'elle se conforme aux règles en matière de protection des données.
68. Un tel refus de fourniture a été reconnu comme pouvant avoir un effet anticoncurrentiel¹¹⁰: s'il existe des limites à la divulgation d'ensembles de données à des concurrents, l'entreprise dominante pourrait empêcher le développement de produits concurrents par des concurrents. L'entreprise pourrait donc essayer de se «protéger» contre des voies de recours potentiellement imposées par des autorités de concurrence en invoquant la conformité aux règles en matière de protection des données. Toutefois, l'entreprise dominante pourrait encore enfreindre les règles en matière de protection des données, de façon opportuniste, en utilisant l'ensemble contenant des données à caractère personnel à une fin incompatible avec celle pour laquelle les données ont initialement été collectées, ce dans le but de proposer d'autres services que des concurrents ne pourraient jamais développer. Dans ce contexte, il existe manifestement une marge de coopération entre les autorités de concurrence et de protection des données afin de garantir l'exécution effective des règles respectives.

¹⁰⁹ Ce terme est étudié dans Bakos, Y. et Brynjolfsson, E., «Bundling and Competition on the Internet, Marketing Science», vol. 19, n° 1, Winter 2000, p. 63 à 82. Voir également OCDE, «Hearings on the Digital Economy», 2012 (voir <http://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf>).

¹¹⁰ Picker, R. C., «Competition and privacy in Web 2.0 and the Cloud», Chicago John M. Olin Law & Economics Working Paper n° 414, juin 2008, p. 13 et 14.

4.2.3. La protection des données, facteur du bien-être des consommateurs

Voir parties 3.2.4 (*Bien-être des consommateurs dans le droit de la concurrence*) et 3.3.2 (*Obligations d'informations justes et exactes*)

69. Il ressort d'une récente étude¹¹¹ que les consommateurs de l'économie numérique subissent une discrimination en partie du fait du manque d'attention dans l'application du droit de la concurrence. Selon l'étude, cette négligence consiste en l'absence de mesures uniformes de signalement de pratiques discriminatoires et en l'absence d'approche harmonisée en matière de recours collectif. S'il est possible pour des organisations de défense des consommateurs de déposer plainte devant des autorités de concurrence, ces plaintes sont rares en raison du montant des frais de justice et de la méconnaissance des droits des consommateurs¹¹².
70. Il convient de garder à l'esprit que les consommateurs sont également des personnes concernées dont le bien-être peut être mis en danger dès lors que la liberté de choix et le contrôle de leurs propres informations personnelles sont restreints par une entreprise dominante dans des cas similaires à ceux présentés ci-dessus. Des recherches psychologiques et sur l'économie du comportement ont révélé que la présentation d'offres comme «gratuites» à des consommateurs était trompeuse, aveuglait les consommateurs quant aux coûts réels qu'ils subiraient «en aval» et faussait la prise de décision, portant ainsi atteinte à la fois aux consommateurs et à la concurrence¹¹³.
71. Compte tenu de la portée et de la croissance dynamique des services en ligne, il pourrait s'avérer nécessaire de développer une notion d'atteinte aux consommateurs, en particulier par la violation de droits à la protection des données, en vue de l'application de la concurrence dans les secteurs numériques de l'économie.

4.2.4. Voies de recours contre des décisions en matière de concurrence

Voir parties 3.1.5, 3.2.5 et 3.1.3 (*Supervision, etc.*)

72. Les décisions concernant des affaires individuelles antitrust et de concentration imposent généralement des voies de recours. Une décision, notamment, a imposé à une entreprise de vendre une copie d'une base de données comprenant des informations personnelles à un ou plusieurs de ses rivaux¹¹⁴. D'autres voies de recours de cette nature devraient être soumises à des conditions et garanties strictes,

¹¹¹ «Discrimination of Consumers in the Digital Single Market», étude menée par l'université d'Osnabrück pour le compte du département des politiques économiques et scientifiques de la direction générale des politiques internes du Parlement européen, 2013.

¹¹² «Panel on class actions», Competition Summit, Bruxelles, décembre 2013; en France, l'autorité de la concurrence a prononcé des amendes lourdes (27,6 millions d'euros et 70 millions d'euros respectivement) à l'encontre de deux monopoles étatiques pour des infractions impliquant une utilisation déloyale de données clients. Décision n° 09-D-24 du 28 juillet 2009 relative à des pratiques mises en œuvre par France Télécom sur différents marchés de services de communications électroniques fixes dans les DOM. Décision n° 12-D-25 du 18 décembre 2012 relative à des pratiques mises en œuvre dans le secteur du transport ferroviaire de marchandises.

¹¹³ Friedman, D.A., «Free Offers: A New Look», 38 N.M. L. REV. 49, 68–69 (2008); Hoofnagle, C.J. et Whittington, J., «Free: Accounting for the Costs of the Internet's Most Popular Price», 61 UCLA L. Rev. 606 (2014).

¹¹⁴ Décision de la Commission du 19 février 2008 déclarant une concentration compatible avec le marché commun et le fonctionnement de l'accord EEE, Bruxelles, 19 février 2008, C (2008) 654 final (affaire n° COMP/M.4726 – Thomson Corporation/Reuters Group).

conformément au principe de la minimisation des données (selon lequel seules les informations personnelles strictement nécessaires pour exécuter la fonctionnalité souhaitée doivent être collectées)¹¹⁵. Dans les affaires de concurrence impliquant des entreprises de l'économie numérique, d'autres voies de recours pourraient aussi être envisagées, notamment en réponse à une atteinte à la vie privée. Les options pourraient comprendre:

- offrir à des utilisateurs un service payant minimisant la collecte et la conservation d'informations personnelles;
- appliquer une limite proportionnée à la conservation des données clients¹¹⁶, par exemple selon la méthode «comparer et oublier» («*compare and forget*») recommandée par l'autorité néerlandaise chargée de la protection des données¹¹⁷;
- mettre en place la portabilité des données en permettant à l'utilisateur de retirer ses informations personnelles et de les transférer vers un autre prestataire de services (voir partie 4.3.3), ce qui donnerait un certain pouvoir aux individus, tout en faisant la promotion de structures de marché concurrentielles; et
- imposer des contrôles stricts sur le traitement des informations dans différentes parties de l'activité à des fins incompatibles.

4.3. Exécution conjointe destinée à faciliter une «course vers le sommet» en matière de normes de sécurité

Voir parties 3.1.4 (Consentement et droit à l'information, etc.), 3.2.4 (Bien-être des consommateurs et droit de la concurrence) et 3.3.2 (Obligations d'informations justes et exactes)

¹¹⁵ Le principe de la minimisation des données découle de l'article 6, paragraphe 1, points b) et c), de la directive 95/46/CE.

¹¹⁶ Cette solution a été proposée par Bruno Lasserrre, président de l'autorité française de la concurrence, 2013, Colloque New Frontiers of Antitrust, 22 février 2013.

¹¹⁷ Cette recommandation avait été faite dans le cadre de l'enquête sur l'application de communication mobile WhatsApp. Le prestataire de service avait bénéficié d'un accès en lecture temporaire à l'ensemble du carnet d'adresses d'un utilisateur de WhatsApp pour aider l'utilisateur à identifier ses contacts qui étaient déjà des utilisateurs de WhatsApp. WhatsApp devait ensuite immédiatement supprimer les informations; autorité néerlandaise chargée de la protection des données, «Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc.: Report on the definitive findings», janvier 2013.

L'application du droit de la concurrence et de la protection des consommateurs peut être utilisée comme un outil favorisant l'efficacité dynamique sur les marchés numériques et encourageant l'innovation. La reconnaissance, par les autorités européennes, de la valeur des informations personnelles dans des lignes directrices et des décisions clés pourrait favoriser des services renforçant la protection de la vie privée, qui sont dans l'intérêt des consommateurs.

Si des entreprises sont contraintes à la transparence quant à la véritable valeur des informations personnelles qu'elles collectent et si les analyses de marché tiennent compte de cette valeur dans des décisions concurrentielles, les entreprises pourraient commencer à rechercher des avantages concurrentiels en réduisant les périodes pendant lesquelles les informations sont conservées ou en proposant un bouton «effacer mes données».

Les entreprises concurrentes qui collaborent à l'adoption d'un système de certification garantissant un niveau élevé de protection de la vie privée pourraient être exonérées de l'interdiction d'accords anticoncurrentiels si elles satisfont aux exigences de l'article 101, paragraphe 3, du TFUE.

4.3.1. Favoriser la vie privée comme avantage concurrentiel

73. Sur certains marchés, les consommateurs peuvent considérer qu'un service plus favorable à la vie privée est de meilleure qualité qu'un service dont la politique de confidentialité est peu claire ou opaque. Dans la prestation de services juridiques et médicaux, de banque privée, de sécurité et de sites de vacances exclusifs de luxe, les entreprises se font généralement concurrence autour de la protection de la vie privée. On peut raisonnablement supposer que, sur des marchés aussi concurrentiels, le non-respect de la protection des données par une entreprise aurait pour effet de nuire à son pouvoir de marché¹¹⁸. Dans une mesure bien plus limitée, certains services de recherche en ligne visent à se différencier en matière de confidentialité.

74. Les consommateurs qui sont habitués à profiter de services en ligne gratuits, cependant, pourraient accepter de fournir des informations personnelles en échange d'un service gratuit, rapide et facile, qu'ils soient conscients ou non des risques associés. Pour de tels marchés, des clauses plus favorables au respect de la vie privée pourraient ne pas générer automatiquement une perception de qualité supérieure chez les consommateurs¹¹⁹. Une recherche récente suggère que les consommateurs pourraient être prêts à payer une majoration pour une protection renforcée de leur vie privée¹²⁰. Les entreprises exerçant dans l'économie numérique ne considèrent pas

¹¹⁸ Avis du CEPD soulignant qu'il est souhaitable d'encourager le respect des principes relatifs à la protection des données dans le secteur privé par la concurrence autour de produits et de services respectant la vie privée, de manière à étendre une position sur le marché en répondant mieux aux attentes des consommateurs soucieux du respect de leur vie privée (voir https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_FR.pdf).

¹¹⁹ Selon les résultats (non concluants) de recherches récentes, «lorsque des consommateurs doivent faire un choix entre acheter auprès d'une entreprise respectant la vie privée ou une entreprise moins chère, cette dernière attire la très grande majorité d'entre eux». Preibusch, S., Kuebler, D. et Beresford, A., R., «Price versus privacy: an experiment into the competitive advantage of collecting less personal information», publié en ligne le 7 août 2013.

¹²⁰ Tsai, J. Y., Egelman, S., Cranor, L. et Acquisti, A., «The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study», Information Systems Research, vol. 22 (2), juin 2011, p. 254 à 268.

encore la vie privée comme une opportunité d'avantage concurrentiel. Au contraire, il existe un risque de «course vers le sommet» en matière de protection de la vie privée, auquel cas le non-respect des règles en matière de protection des données et l'acquisition de données par des moyens anticoncurrentiels pourraient devenir symptomatiques du pouvoir du marché, les coûts externes étant supportés par les utilisateurs¹²¹.

75. Une comparaison utile peut être faite avec la diffusion, dans les années 1960 et 1970, de la notion de responsabilité d'entreprise sociale et environnementale. Les entreprises avaient commencé à réaliser l'importance de l'impact socioéconomique de leurs activités et de la façon dont il était perçu par leurs consommateurs. Elles ont désormais l'habitude de comparer leurs propres politiques à celles de leurs concurrents et il existe un réel marché pour la sécurité des produits et les technologies vertes. Une approche plus conjointe de la protection des données et de la concurrence pourrait contribuer à stimuler un niveau similaire de concurrence en matière de services en ligne.

4.3.2. Choix du consommateur, consentement et transparence

76. Le choix dépend de la disponibilité de services concurrents et de la capacité des consommateurs à comprendre les informations fournies sur ces services¹²². Face aux entreprises multiservices de l'économie numérique, il existe plusieurs obstacles significatifs à un véritable choix. Si des informations personnelles sont collectées comme condition de l'utilisation d'un service particulier, puis traitées par la même entreprise aux fins d'un autre service, il est déjà difficile pour les utilisateurs de prédire ce qu'il va advenir de leurs données¹²³.

77. Cette difficulté est aggravée par des «politiques de confidentialité» longues: une étude a calculé qu'il faudrait en moyenne 244 heures par an à chaque internaute pour lire la politique de confidentialité de chaque site web qu'il consulte, soit 50 % du temps qu'un utilisateur moyen passe sur l'internet¹²⁴. Ces politiques contiennent généralement des déclarations sur l'utilisation future des données qui sont dissimulées

¹²¹ Par exemple, Grunes, A.P., «Another look at privacy», *Geo.Mason L. Rev* vol. 20:4, p. 1112; Jones Harbour, P., J., et Koslov, T., I., «Section 2 in a Web 2.0 world: An expanded vision of relevant product markets», *Antitrust Law Journal*, vol. 76 (2010), p. 769 à 797.

¹²² L'article 11 de la proposition de règlement général sur la protection des données prévoit des politiques en matière de protection des données qui soient «transparentes et facilement accessibles».

¹²³ Courrier du groupe de travail Article 29 à Google Inc. (voir http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf, consulté le 10 mars 2014).

¹²⁴ McDonald, A. M. et Cranor, L. F., «The Cost of Reading Privacy Policies», *A Journal of Law and Policy for the Information Society* 2008, *Privacy Year in Review*, p. 17.

dans des petits caractères ou qui doivent être décodées du fait de termes vagues et élastiques, tels que: «améliorer l'expérience du client»¹²⁵.

78. En outre, si les utilisateurs moyens de smartphones téléchargent 37 applications pour des utilisations allant du jeu à des actions bancaires, seules 61 % des applications populaires disposent d'une politique de confidentialité¹²⁶. Cela crée une asymétrie de connaissances qui nécessite d'imposer aux professionnels de fournir des informations claires et indubitables en vertu du droit communautaire en matière de protection des données et remet en question le fait que les personnes concernées disposent de suffisamment d'informations pour donner un consentement informé au traitement de leurs données¹²⁷. La situation peut être aggravée par la croissance de l'«internet des objets», qui englobera de nombreux services techniques ou intégrés collectant des données à caractère personnel, avec pour conséquence que leurs utilisateurs ne pourront pas consulter la politique de confidentialité sur l'appareil lui-même, mais devront se procurer la documentation papier ou, plus probablement, consulter les sites web correspondants depuis un autre appareil.

¹²⁵ Le terme «politique de confidentialité» peut être trompeur en soi, comme révélé par une étude approfondie menée aux États-Unis. Il ressort d'une étude réalisée auprès d'internautes américains que moins de la moitié des personnes interrogées jugent les politiques de confidentialité faciles à comprendre, tandis que deux-tiers d'entre elles pensent (à tort) que les sites disposant d'une politique de confidentialité ne partagent pas les données; Turow, J., «Americans and Online Privacy: The System is Broken», juin 2003. Une grande majorité des politiques de confidentialité évoquées dans l'étude Fortune 500 sont considérées comme ayant été rédigées à un niveau supérieur à la capacité de lecture de l'adulte américain moyen; Shannon Wheatman et Michelle Ghiselli «Privacy Policies: How to Effectively Communicate with Consumers and Avoid Judicial and Regulatory Scrutiny». La FTC a découvert que la plupart des politiques de confidentialité d'entreprises étaient «incompréhensibles» et que les «politiques de confidentialité ne permettaient pas d'informer les consommateurs sur les pratiques des entreprises en matière de données ou de présenter les modifications apportées à leurs pratiques»; «Preliminary Staff Report: Protecting Consumer Privacy in an Era of Rapid Change», mars 2012. En mars 2014, un groupe de consommateurs français a engagé des poursuites contre trois des plus grands réseaux sociaux pour non-respect des règles relatives à la protection des consommateurs et des données, ayant préalablement reproché aux prestataires de services d'utiliser des clauses contractuelles elliptiques et pléthoriques (voir <http://www.quechoisir.org/telecom-multimedia/internet/editorial-donnees-personnelles-main-basse-sur-la-vie-privee>, consulté le 25 mars 2014).

¹²⁶ Avis du groupe de travail Article 29 n° 02/2013 sur les applications destinées aux dispositifs intelligents, WP 202, adopté le 27 février 2013.

¹²⁷ Dans une ordonnance faisant suite à la requête du défendeur de rejeter une action collective alléguant que la numérisation de courriels d'utilisateurs constituait un manquement à la législation américaine sur les écoutes, un tribunal de première instance américain avait retenu qu'«un utilisateur raisonnable de Gmail qui lit les politiques de confidentialité ne comprendra pas forcément que ses courriels sont interceptés pour créer des profils d'utilisateur ou pour fournir des publicités ciblées», et que «les utilisateurs de Gmail qui ne font pas l'objet des politiques de confidentialité ou conditions d'utilisation de Google n'ont pas implicitement consenti à l'interception de leurs courriels à des utilisateurs de Gmail par Google»; United States District Court Northern District of California San Jose Division, affaire n°: 13-MD-02430-LHK, Order Granting in Part and Denying in Part Defendant's Motion to Dismiss, 11 juillet 2013, p. 26, 27 et 28.

79. Les prestataires en ligne populaires persuadent de plus en plus de consommateurs de leur fournir de plus en plus d'informations personnelles, ce qui augmente la valeur des services pour les publicitaires, générant ainsi des «effets de réseau» qui rendent le service encore plus attractif pour les clients¹²⁸. Dans le cas de services en ligne «gratuits», il est possible qu'aucune alternative à l'offre d'un prestataire n'utilisant pas d'informations personnelles à des fins de marketing ne soit proposée aux clients. Les consommateurs n'ont qu'une marge de manœuvre limitée, si tant est qu'ils en aient une, pour négocier les modalités et conditions d'utilisation, ce qui constitue un «déséquilibre significatif» entre le prestataire et l'utilisateur, qui pourrait aussi déclencher une enquête sur la légalité du traitement de données. Cela remet en question l'existence d'un véritable choix au sens de l'article 7, point a), de la directive relative à la protection des données et, parallèlement, de la validité du consentement au traitement des informations personnelles. Lorsqu'il existe un nombre limité d'opérateurs ou lorsqu'un opérateur est dominant, le concept du consentement devient de plus en plus illusoire¹²⁹.
80. Il y a donc eu des appels à la responsabilité concernant la protection des informations personnelles afin de passer plus visiblement de l'utilisateur au prestataire de services, comme pour les règles en matière de protection des consommateurs (voir partie 3.3.2)¹³⁰. Une réponse à ces défis pourrait être d'envisager des normes relatives à la transparence et à l'intelligibilité des clauses contractuelles de services en ligne. Il pourrait être demandé aux organisations d'en dire plus sur leur processus décisionnel en matière de traitement de données¹³¹. Une approche économique basée sur le coût de la transaction a également été recommandée et devrait prendre en considération des facteurs contextuels dans l'évaluation de la valeur de biens et services présentés comme étant gratuits, mais impliquant «une myriade de coûts cachés non pécuniaires», afin que toutes les parties aient un niveau plus égalitaire de compréhension de la valeur des informations personnelles qui sont collectées et traitées¹³².
81. L'application des règles de concurrence nécessite de déterminer si les consommateurs considèrent que différents services sont substituables. Il s'ensuit que cette analyse devrait accorder de l'attention à la transparence et au coût final de politiques de confidentialité pour les consommateurs, ainsi qu'à la question de savoir si le choix est réel et si le consentement au traitement de l'information est valable.

¹²⁸ Les effets de réseau surviennent lorsque l'utilité d'un service augmente proportionnellement à son nombre croissant d'utilisateurs, ce qui signifie que les entrants doivent disposer d'une «masse critique» d'utilisateurs pour pouvoir faire concurrence, tandis que les utilisateurs peuvent utiliser uniquement le service concurrent (par ex. un système d'exploitation informatique) s'il a été adopté de manière générale. Grunes, A. P. (2013), «Another Look at Privacy» (August 13, 2013), *George Mason Law Review*, vol. 20, n° 4, 2013, p. 1120.

¹²⁹ Coates (2011).

¹³⁰ «Dans le contexte de la confidentialité en ligne, ceci implique de mettre moins l'accent sur la notification et le choix et plus sur la mise en œuvre de décisions politiques concernant l'utilité de certaines pratiques commerciales et la conformité de l'organisation aux principes relatifs aux pratiques loyales en matière d'information ("*fair information principles*", FIP). En d'autres termes, le point central de la confidentialité devrait passer des utilisateurs (a) aux décideurs politiques ou aux responsables de l'autoréglementation pour déterminer les contours de pratiques acceptées; et (b) aux entreprises pour le traitement juste et responsable des informations». Dans ce contexte, voir également l'avis du groupe de travail Article 29 sur la notion d'intérêts légitimes poursuivis par le responsable du traitement de données au titre de l'article 7 de la directive 95/46/CE (avril 2014) et sur l'accent renforcé sur le principe de la responsabilité pour les responsables du traitement.

¹³¹ Tene, O. et Polonetsky, J. (2013), «Big Data for All: Privacy and User Control in the Age of Analytics», *11 Nw. J. Tech. & Intell. Prop.* 2.239 (2013).

¹³² Hoofnagle et Whittington (2014).

4.3.3. Contrôle de leurs propres informations par les individus

82. Des consommateurs mieux informés devraient être plus à même de faire un choix entre des services en ligne concurrents. Ils devraient pouvoir retirer et transférer des données enregistrant leurs activités et sauvegardées dans le nuage, que ce soit dans le contexte de réseaux sociaux, de moteurs de recherche, de banques en ligne, de consommation énergétique, d'applications médicales ou de contrôles de la bonne condition physique. Comme l'a relevé un expert en concurrence de la Commission, «plus il est difficile pour un individu de déplacer ses données, plus forte est la position du prestataire qui contrôle les données, et plus il sera difficile pour de nouveaux entrants de réussir»¹³³.
83. La portabilité des données (point 26) pourrait créer des synergies entre le droit de la concurrence et le droit de la protection des données, au moins de deux façons¹³⁴. Premièrement, elle pourrait empêcher l'abus de position dominante, que ce soit par exclusion ou exploitation, et le fait que des consommateurs se retrouvent enfermés dans certains services du fait de la limitation de la production, des marchés ou du développement technique au préjudice des consommateurs¹³⁵. Elle reproduirait les avantages de la portabilité du numéro prévue par le droit des télécommunications¹³⁶. Deuxièmement, la portabilité des données pourrait donner aux consommateurs le pouvoir de profiter de services à valeur ajoutée de tiers, tout en facilitant un meilleur accès au marché par des concurrents, par exemple par l'utilisation de sites comparateurs de produits ou d'entreprises proposant des conseils énergétiques sur la base de données de compteurs intelligents¹³⁷.

4.4. Supervision et mise en œuvre

Voir parties 3.1.5, 3.2.5 et 3.1.3 (*Supervision, etc.*)

84. Des accords de cohérence distincts au sein de l'Union européenne existent déjà pour la réglementation de la concurrence, la protection des consommateurs et la protection des données par l'intermédiaire, respectivement, du réseau européen de la concurrence, du réseau de coopération en matière de protection des consommateurs (CPC) et du groupe de travail Article 29. Il convient de continuer à respecter pleinement le caractère distinct et l'indépendance de ces autorités. Toutefois, compte

¹³³ Coates, K., «Competition Law and Regulation of Technology Markets», 2011.

¹³⁴ Article 18 de la proposition de règlement général sur la protection des données, COM(2012) 11 final. Il existe déjà des initiatives public/privé dans plusieurs États membres qui permettent aux individus d'accéder directement à leurs propres données qui sont détenues par des entreprises et de choisir de les transférer à des prestataires concurrents. Voir, par exemple, au Royaume-Uni <http://www.midatalab.org.uk/> et en France <http://mesinfos.fing.org/>.

¹³⁵ Article 102, paragraphe 2, point b), du TFUE. Voir également Mantelero, A., «Competitive value of data protection: the impact of data protection regulation on online behaviour», *International Data Privacy Law*, 2013, vol. 3, n° 4, p. 229 à 238.

¹³⁶ Article 30, directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive «service universel») (JO L 108 du 24.4.2002).

¹³⁷ «Permettre à des personnes concernées/consommateurs d'accéder directement à leurs données sous un format portable, convivial et assimilable par machine pourrait aider à leur donner un pouvoir et corriger le déséquilibre économique entre les grandes entreprises, d'une part, et les personnes concernées/consommateurs, d'autre part. Cela permettrait aussi aux individus de "partager la richesse" créée par les données massives et inciterait les développeurs à proposer des fonctionnalités et applications supplémentaires à leurs utilisateurs»; avis du groupe de travail Article 29 n° 03/2013 sur la limitation des finalités.

tenu des défis présentés dans ce document, il pourrait être judicieux pour la Commission et le CEPD, au niveau européen conjointement avec les autorités nationales de la concurrence, de protection des consommateurs et de protection des données, de s'accorder sur une approche plus globale de la mise en œuvre. Cela serait particulièrement opportun compte tenu de l'examen de la coopération en matière de protection des consommateurs et des négociations en cours concernant le règlement sur la protection des données, qui contient des dispositions sur un mécanisme de cohérence. Le dialogue entre les autorités à ces deux niveaux (européen et national) pourrait devenir plus systématique chaque fois que survient une affaire dans laquelle le bien-être des consommateurs et la protection des données semblent être mis en danger.

5. Conclusion: poursuivre l'étude et la discussion

Le ou les marchés en ligne qui connaissent une croissance rapide [...] touchent de plus en plus tous les aspects du commerce. Garantir que la concurrence fonctionne de façon efficace sur ces marchés va devenir une priorité essentielle [...] la collecte, le traitement et l'utilisation croissants de données relatives aux transactions de consommateurs à des fins commerciales [...] se révèlent être une source d'avantage concurrentiel de plus en plus importante [qui pourrait être] une source croissante de désavantage pour le consommateur.

De Beesley Lectures, discours de David Currie, président de la UK Competition and Markets Authority, 7 novembre 2013.

85. Le présent avis préliminaire a examiné et étudié les possibles convergences et tensions entre les trois domaines du droit communautaire dans le contexte de l'évolution rapide des données massives. Bien que la vie privée et la protection des données à caractère personnel soient des intérêts publics et des droits fondamentaux reconnus par les traités, l'absence d'interaction dans l'élaboration de politiques sur la concurrence, la protection des consommateurs et la protection des données a peut-être eu pour effet de réduire à la fois l'efficacité de l'application des règles de concurrence et l'incitation à développer des services renforçant le respect de la vie privée et minimisant les risques d'atteintes pour les consommateurs. Dans l'économie numérique, les informations personnelles représentent un actif incorporel significatif dans la création de valeur et une monnaie d'échange de services en ligne. Cela peut avoir de vastes implications pour l'interprétation de concepts clés, dont la transparence, la position dominante sur le marché, ainsi que le bien-être des consommateurs et les atteintes à ceux-ci.

86. Une réponse exhaustive à ces défis demande une étude, une réflexion et une discussion plus longues, mais pourrait inclure tout ou partie des éléments suivants:

- une **meilleure sensibilisation** des consommateurs, prestataires de services et législateurs aux développements technologiques actuels et futurs sur les marchés pertinents dans l'économie numérique et les implications pour la compétitivité, le bien-être des consommateurs ainsi que le choix et l'innovation autour de services renforçant la protection de la vie privée;

- des **conseils efficaces** sur l'application des règles en matière de vie privée, de concurrence et de protection des consommateurs pour les services en ligne, en particulier ceux présentés comme des services «gratuits», qui tiennent compte de la position des consommateurs et des concurrents et mettent en évidence les préférences et préoccupations des consommateurs;
- une **coopération** entre les autorités en matière d'enquête et d'exécution, par exemple par l'identification de scénarios et de normes possibles pour la mesure du pouvoir du marché dans l'économie numérique, ainsi que la consultation sur des enquêtes dans des affaires individuelles; et
- un **examen de la législation sur la concurrence** pour les marchés numériques du 21^e siècle, notamment ses interfaces avec d'autres domaines du droit et les possibilités d'interaction productive avec d'autres autorités pertinentes.

87. Les informations personnelles ont initié et entretenu une croissance dans l'économie numérique. Chaque consommateur devrait pouvoir profiter de sa part des produits de cette croissance. Les autorités de la concurrence et de la protection des données reconnaissent de plus en plus cette situation comme un défi essentiel dans l'établissement de la confiance et de la responsabilité dans l'ensemble de l'économie numérique. La protection des données constitue une opportunité unique de donner aux individus les outils pour se protéger et pour rendre plus efficace l'application des règles de concurrence et de protection des consommateurs.

88. La prochaine étape consistera à explorer l'étendue d'une coordination plus étroite entre les législateurs pour atteindre ces objectifs. Cette coordination ne devrait pas se limiter à l'Europe, mais refléter la dimension mondiale des entreprises de l'économie numérique. Le CEPD se réjouit à la perspective de faciliter cette discussion.

Fait à Bruxelles, le 26 mars 2014

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données

Annexe: Protection des données, concurrence et protection des consommateurs dans l'Union européenne: vue comparative

	<i>Protection des données</i>	<i>Droit de la concurrence</i>	<i>Protection des consommateurs</i>	<i>Interfaces dans l'économie numérique</i>
Cadre juridique	<ul style="list-style-type: none"> ➤ Art. 7 et 8 CDF ➤ 16 TFUE 	<ul style="list-style-type: none"> ➤ 101-106 TFUE 	<ul style="list-style-type: none"> ➤ 38 CDF ➤ Art. 12 et 169 TFUE 	<ul style="list-style-type: none"> ➤ Valeurs communautaires fondamentales et mission économique.
Législation secondaire pertinente	<ul style="list-style-type: none"> ➤ Directive 95/46/CE ➤ Règlement (CE) n° 45/2001 ➤ Directive 2002/58/CE ➤ Règlement général sur la protection des données (en cours de négociation) 	<ul style="list-style-type: none"> ➤ Règlement n° 1/2003 (paquet modernisation) ➤ Règlement n° 139/2004 (concentrations) 	<ul style="list-style-type: none"> ➤ Directive 93/13/CEE (clauses abusives dans les contrats) ➤ Directive 98/6/CE (indication des prix) ➤ Directive 2005/29/CE du Conseil (pratiques commerciales déloyales) ➤ Directive 2006/114/CE (publicité trompeuse) ➤ Règlement n° 2006/2004 (coopération entre les autorités) ➤ Directive 2011/83/UE (droits des consommateurs) 	<ul style="list-style-type: none"> ➤ Règles de promotion du bon fonctionnement du marché intérieur. ➤ Règles garantissant la protection des consommateurs individuels.
Champ d'application	<ul style="list-style-type: none"> ➤ Tous les responsables du traitement des données établis dans l'Union européenne ou recourant à des moyens situés dans l'Union européenne. Dispositions modulables en fonction de la nature et du volume des données traitées. 	<ul style="list-style-type: none"> ➤ Toute activité économique pouvant «affecter le commerce entre États membres». ➤ Les entreprises dominantes ont la «responsabilité 	<ul style="list-style-type: none"> ➤ Tous les biens et services fournis ou consommés sur le marché intérieur. 	<ul style="list-style-type: none"> ➤ Impact sur les individus dans l'Union européenne de l'activité économique qui concerne le marché intérieur.

	<i>Protection des données</i>	<i>Droit de la concurrence</i>	<i>Protection des consommateurs</i>	<i>Interfaces dans l'économie numérique</i>
	<ul style="list-style-type: none"> ➤ (À étendre dans la proposition de règlement général sur la protection des données pour couvrir tout responsable du traitement de données offrant des biens ou des services à des personnes concernées résidant dans l'Union européenne ou observant leur comportement.) 	<ul style="list-style-type: none"> particulière» d'éviter de fausser la concurrence. 		
Contrôle des données et marchés pertinents	<ul style="list-style-type: none"> ➤ Finalités compatibles du traitement de données. 	<ul style="list-style-type: none"> ➤ Définition du marché pertinent et substituabilité de biens et services. 		<ul style="list-style-type: none"> ➤ Définition des marchés pertinents alimentés par des données à caractère personnel. ➤ Mesurer le pouvoir du marché numérique.
Transparence et choix	<ul style="list-style-type: none"> ➤ Droit à l'information et droit d'accéder aux données sous une forme intelligible. ➤ Consentement libre, spécifique, informé et indubitable. ➤ Droit à la portabilité des données. 	<ul style="list-style-type: none"> ➤ Vente liée et groupée de services. ➤ Entrave à la concurrence par le refus de fournir une installation essentielle. 	<ul style="list-style-type: none"> ➤ Information claire et compréhensible sur les prix et les produits. 	<ul style="list-style-type: none"> ➤ Compréhension commune de la valeur des données à caractère personnel. ➤ Détection par un individu de ses propres données par l'exercice de la portabilité des données.
Prévention de toute atteinte	<ul style="list-style-type: none"> ➤ Minimisation des données. ➤ Confidentialité et sécurité des traitements. 	<ul style="list-style-type: none"> ➤ Notion de bien-être du consommateur. ➤ Tarification de services constituant une exploitation. ➤ Théorie de l'atteinte aux consommateurs lors de concentrations. ➤ Exceptions aux règles relatives à l'aide d'État. 	<ul style="list-style-type: none"> ➤ Notion de «bonne foi» dans les contrats. ➤ Interdiction de déclarations trompeuses concernant des biens et services. 	<ul style="list-style-type: none"> ➤ La protection des données, facteur du bien-être des consommateurs. ➤ Utilisation de voies de recours en faveur de la vie privée dans des décisions concurrentielles. ➤ Possibilité offerte aux concurrents de collaborer pour développer des services renforçant la protection de la vie privée.

	<i>Protection des données</i>	<i>Droit de la concurrence</i>	<i>Protection des consommateurs</i>	<i>Interfaces dans l'économie numérique</i>
<i>Supervision, exécution, sanctions, recours</i>	<ul style="list-style-type: none"> ➤ <i>Autorités nationales indépendantes.</i> ➤ <i>Coopération européenne par le biais du groupe de travail Article 29 et mécanisme de cohérence (en cours de négociation).</i> ➤ <i>Droit à un recours juridictionnel en cas de violation de droits.</i> ➤ <i>Droit de recevoir réparation.</i> ➤ <i>Sanctions administratives proportionnelles au chiffre d'affaires annuel d'une entreprise (en cours de négociation).</i> 	<ul style="list-style-type: none"> ➤ <i>Exécution par des autorités nationales de la concurrence et par la Commission pour l'Union européenne.</i> ➤ <i>Coopération des autorités par le biais du réseau européen de la concurrence.</i> ➤ <i>Sanctions en cas de manquement à des accords anticoncurrentiels pouvant aller jusqu'à 10 % du chiffre d'affaires global.</i> ➤ <i>Pas d'harmonisation des droits à un recours juridictionnel pour les consommateurs.</i> 	<ul style="list-style-type: none"> ➤ <i>Autorités nationales uniquement.</i> ➤ <i>Le réseau CPC identifie des priorités communes d'exécution chaque année avec des contrôles de conformité coordonnés et des projets spécifiques à certains secteurs.</i> ➤ <i>Pas d'approche communautaire commune en matière d'enquête sur des violations du droit de la consommation, sauf pour les «infractions intracommunautaires».</i> ➤ <i>Rares réparations obtenues par des autorités pour des violations du droit de la consommation.</i> 	<ul style="list-style-type: none"> ➤ <i>Dialogue et coopération sur des affaires dans lesquelles concurrence, bien-être des consommateurs et protection des données se recoupent.</i>

Abréviations:

CDF: *Charte des droits fondamentaux de l'Union européenne*

TFUE: *Traité sur le fonctionnement de l'Union européenne*