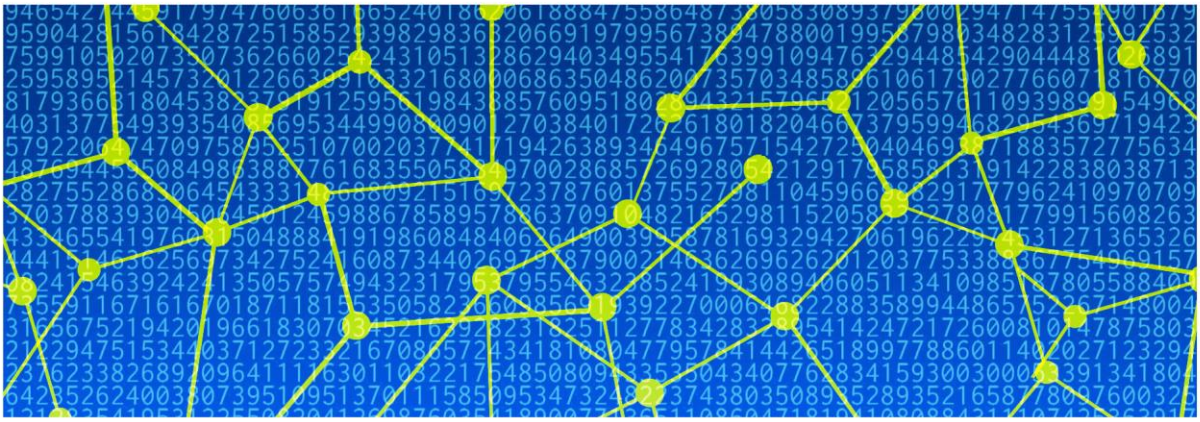

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 8/2016

Avis du CEPD sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*)

EDPS

23 septembre 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée, en vertu de l'article 41, paragraphe 2, du règlement (CE) nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires» et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001, la Commission a l'obligation, «lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel», de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseil des institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques».

Résumé

Le traitement de données à caractère personnel est indispensable aux services en ligne. La stratégie de l'UE en faveur d'un marché unique numérique reconnaît le potentiel des technologies et des services fondés sur les données en tant que catalyseur de la croissance économique. Les services en ligne sont devenus dépendants d'un suivi souvent clandestin des personnes, qui n'ont généralement pas conscience de la nature et de l'étendue de ce suivi. Les entreprises qui dominent ces marchés sont capables d'empêcher les nouveaux venus de leur faire concurrence sur des facteurs qui pourraient être bénéfiques pour les droits et les intérêts des personnes physiques, et peuvent imposer des conditions déloyales qui tirent abusivement profit des consommateurs. Un déséquilibre croissant apparent entre les prestataires de services en ligne et les consommateurs peut réduire le choix, l'innovation et la qualité de la protection de la vie privée. Ce déséquilibre peut aussi entraîner une augmentation du prix effectif - en termes de divulgation de données à caractère personnel - bien supérieure à ce l'on pourrait escompter sur des marchés totalement concurrentiels.

En 2014, le CEPD a publié un avis préliminaire intitulé «Vie privée et compétitivité à l'ère de la collecte de données massives». En dépit des synergies évidentes, comme la transparence, la responsabilité, le choix et le bien-être général, nous avions observé une tendance à appliquer en vase clos les règles européennes en matière de protection des données, de protection des consommateurs, de législation antitrust et de contrôle des concentrations. Nous avions donc lancé un débat sur la manière dont les objectifs et les normes de l'UE pourraient être appliqués de façon plus holistique. Ce nouvel avis explique que la stratégie en faveur d'un marché unique numérique est l'occasion d'adopter une approche cohérente et actualise l'avis préliminaire de 2014, en formulant quelques recommandations pratiques à l'adresse des institutions de l'UE pour remédier à la situation. Il répond à la préoccupation croissante selon laquelle la concentration des marchés numériques pourrait porter préjudice aux intérêts des particuliers en tant que personnes concernées et consommateurs.

Les institutions et organes de l'UE, ainsi que les autorités nationales lorsqu'elles mettent en œuvre le droit de l'UE, sont tenus de respecter les droits et libertés consacrés par la Charte des droits fondamentaux de l'UE. Plusieurs de ces dispositions, notamment le droit au respect de la vie privée et à la protection des données à caractère personnel, la liberté d'expression et la non-discrimination, sont menacées par le comportement normatif et les normes qui prévalent actuellement dans le cyberespace. L'UE dispose déjà d'outils suffisants pour remédier aux distorsions de marché contraires à l'intérêt de l'individu et de la société en général. Diverses pratiques courantes sur les marchés numériques peuvent enfreindre deux ou plusieurs cadres juridiques en vigueur, dont chacun est sous-tendu par la notion d'«équité». À l'instar de plusieurs études publiées ces derniers mois, nous appelons à renforcer le dialogue, à tirer davantage d'enseignements, voire à renforcer la collaboration entre les autorités qui réglementent le comportement dans l'environnement numérique. Nous insistons également sur le fait que l'UE doit créer des conditions, en ligne et hors ligne, dans lesquelles les droits et libertés consacrés par la Charte pourront prospérer.

Le présent avis recommande donc de créer une chambre de compensation numérique pour l'application de la législation dans le secteur numérique européen, à savoir un réseau bénévole d'organes réglementaires en vue de partager des informations, de façon volontaire et dans les limites de leurs compétences respectives, sur d'éventuels abus dans l'écosystème numérique et sur la manière la plus efficace d'y mettre un terme. Ceci devrait être complété par des orientations sur la façon dont les autorités réglementaires pourraient appliquer de manière cohérente les règles protégeant l'individu. Nous recommandons également que les institutions

de l'UE et des experts extérieurs étudient la possibilité de créer un espace commun sur la Toile, à l'intérieur duquel, conformément à la Charte, les personnes peuvent interagir sans être suivies. Enfin, nous recommandons d'actualiser les modalités d'application des contrôles de concentration par les autorités afin de protéger la vie privée en ligne, les informations personnelles et la liberté d'expression.

TABLE DES MATIÈRES

ÉLARGIR LE DÉBAT

1. Contexte et structure de l'avis

Notre avis préliminaire «Vie privée et compétitivité à l'ère des données massives» (ci-après «l'avis préliminaire») comparait les cadres juridiques de l'UE en matière de protection des données, de concurrence et de protection des consommateurs et concluait qu'il existe plusieurs synergies évidentes en ce qui concerne les marchés numériques[1]. Nous avions formulé quelques propositions de recommandations à l'intention des institutions de l'UE, qui ont été affinées à la suite d'un atelier organisé par le CEPD en juin 2014[2], notamment:

1. mieux comprendre **la «valeur» des données à caractère personnel sur le marché numérique** et revoir les approches de l'analyse de marché, notamment pour les services en ligne présentés comme «gratuits», avec une analyse rétrospective ou a posteriori de l'impact des décisions exécutoires;

2. examiner comment **promouvoir les technologies qui protègent la vie privée en tant qu'avantage concurrentiel**;

3. réviser la **législation de l'UE et sa pertinence pour les marchés numériques du XXI^e siècle**;

4. envisager les étapes pratiques de la **coopération entre les autorités**, notamment un dialogue rapproché et des enquêtes conjointes.

2. De l'analyse à l'action

Le présent avis assure le suivi de ces questions, mais répond également à un débat qui est passé, depuis 2014, d'arguments juridiques abstraits à des préoccupations plus urgentes. La concentration et le pouvoir monopolistique, en particulier sur les marchés numériques, posent des problèmes non seulement de compétitivité, mais également de respect de la vie privée et de la liberté d'expression. La stratégie pour un marché unique numérique, adoptée par la Commission en mai 2015, affirmait son intention d'atteindre un certain degré d'harmonisation des règles dans l'écosystème numérique et de permettre à l'Europe d'occuper une position de premier plan dans l'économie numérique mondiale[3]. La stratégie décrivait l'économie des données comme un facteur crucial pour le renforcement de la compétitivité de l'UE, tandis que les données étaient définies comme «un catalyseur de croissance économique». Le présent avis est le résultat le plus récent de l'engagement permanent du CEPD en faveur de cette stratégie ambitieuse[4]. Il entend dépasser les commentaires juridiques en épinglant des mesures pratiques destinées à relever de manière cohérente les défis liés à l'application de la législation[5].

3. Importance stratégique de cette problématique pour les autorités chargées de la protection des données

L'interface entre la concurrence et le respect de la vie privée devrait être une préoccupation majeure, stratégique et à long terme de toutes les autorités indépendantes chargées de la protection des données. Les données à caractère personnel ont joué un rôle capital dans l'évolution des marchés numériques, dont certains peuvent aujourd'hui être considérés comme des services essentiels. Ainsi que nous l'avions déclaré précédemment[6], le développement rapide de technologies fondées sur des données à caractère personnel et des traitements de données que permettent ces technologies, comme les données massives et l'Internet des objets, fait peser une pression sans précédent sur le droit à la protection des données et plusieurs autres droits fondamentaux. Certains droits fondamentaux classiques consacrés par la Charte - le droit au respect de la vie privée (article 7), la liberté d'expression (article 11) et la non-discrimination

(article 21) - ont été conçus à l'origine comme des protections contre l'ingérence de l'État. Or, il apparaît désormais clairement qu'à l'ère numérique, des mesures de protection sont également requises contre l'ingérence potentielle d'entités non étatiques et de personnes physiques, qui conduisent notamment au droit à la protection des données énoncé à l'article 8 de la Charte. Plus récemment, le rapporteur spécial des Nations unies pour la liberté d'expression a appelé le secteur des technologies de l'information et de la communication à respecter les droits de l'homme[7].

La Commission a constaté que les effets de réseau sont une caractéristique des marchés numériques[8]. Les coûts sociaux et professionnels liés au renoncement à de nombreux services en ligne ont augmenté et vont de pair avec un manque d'interopérabilité et des choix offrant souvent une faible protection de la vie privée. Le choix est un paramètre de concurrence, mais il est aujourd'hui virtuellement impossible de choisir de ne pas être suivi tout en consommant des services numériques[9]. Le morcellement apparent de la Toile selon les frontières d'un État et la division de l'expérience en ligne d'un particulier en un nombre restreint de «jardins clos» menacent la vie privée, les informations personnelles, la liberté d'expression et la liberté d'innover au milieu de la concentration des profits et du pouvoir sur le marché.

Par ailleurs, une discrimination déloyale par les prix - en exploitant les différences entre la sensibilité identifiable des consommateurs aux prix - pourrait conduire à soutirer clandestinement des informations aux consommateurs et à accroître les bénéfices[10]. Des études récentes ont mis en évidence le potentiel futur des algorithmes de «machine-learning» pour parvenir à une discrimination parfaite par les prix de premier degré, les entreprises segmentant le marché en consommateurs individuels et leur appliquant un prix en fonction de leur volonté de payer. Dans un avenir proche, la technologie pourrait potentiellement permettre une collusion tacite entre les entreprises actives sur les marchés numériques en vue de fixer les prix par le biais de données et d'algorithmes d'autoapprentissage[11]. Cette tendance pourrait conduire, en termes économiques, à maximiser les revenus mais pas le bien-être des consommateurs et aurait des conséquences négatives évidentes pour les droits fondamentaux. Les autorités chargées de la protection des données et d'autres autorités compétentes devront se montrer vigilantes.

4. La «valeur» des données à caractère personnel sur les marchés numériques

Depuis 2014, des débats nourris se sont concentrés sur la «valeur» des données massives et la mesure dans laquelle elles peuvent être assimilées à des données à caractère personnel. Si de nombreuses applications de données massives portent sur des données factuelles, comme la météo ou les processus machine, les entreprises et les gouvernements utilisent de plus en plus des volumes considérables d'informations personnelles pour comprendre, prédire et façonner le comportement humain[12]. Les principaux fournisseurs de services en ligne, qui comptent quelques-unes des dix plus grandes entreprises du monde, doivent leur succès à la quantité et à la qualité des données à caractère personnel dont ils disposent ainsi qu'à la propriété intellectuelle nécessaire pour analyser et extraire une valeur de ces données[13]. Les informations personnelles sont devenues un facteur de concurrence pour les entreprises; elles sont décrites comme de la «matière première pour les modèles économiques numériques» et sont utilisées pour améliorer les produits et la publicité ciblée[14].

Il est courant aujourd'hui de comparer les informations personnelles à une monnaie utilisée pour accéder à des services en ligne et la proposition de la Commission sur les contrats numériques va jusqu'à reconnaître que les données à caractère personnel peuvent servir de

moyen de paiement[15]. Les données peuvent être un produit négocié directement ou peuvent avoir une fonction auxiliaire d'intrant pour la création de profils d'utilisateurs individuels[16]. Les plateformes numériques «à multiples facettes», qui sont des médiateurs typiques pour l'expérience en ligne de la plupart des gens, traitent les personnes physiques et les organisations comme des fournisseurs d'idées et de produits à mettre en correspondance les uns avec les autres. Des plateformes fondées sur les données et à multiples facettes ont connu le succès et se sont développées en proposant du contenu et/ou des services «gratuits» afin de rassembler des masses d'informations personnelles, révélant les habitudes et préférences passées, présentes, voire futures, des particuliers. Les plateformes attirent des clients payants – généralement des publicitaires –, d'un côté, en recueillant et en analysant les informations personnelles provenant de clients non payants, de l'autre côté. La distinction traditionnelle entre consommateur et producteur s'en trouve ainsi estompée[17].

Le contrôle commercial de données pourrait être le chaînon manquant qui explique l'inflation remarquable de la valeur de marché des entreprises prospères dans le secteur numérique[18]. Notre avis préliminaire citait la déclaration du vice-président de la Commission européenne de l'époque, M. Alumnia, selon lequel il fallait encore procéder à une analyse sectorielle complète des services numériques gratuits[19]. Les autorités compétentes, lorsqu'elles définissent les marchés en cause et déterminent le pouvoir de marché dans des cas spécifiques, ont eu tendance à se concentrer sur le côté «payant», lequel, jusqu'à présent, équivalait généralement aux entités en quête de possibilités publicitaires. Dans l'intervalle, le côté «non payant» n'a pas été approfondi au motif qu'il est difficile de le quantifier et qu'il relève d'autres domaines du droit. L'efficacité de ces marchés a été remise en cause en raison de l'asymétrie des informations entre les deux côtés du marché[20]. Compte tenu de cette incertitude, nous nous félicitons de la volonté de la commissaire européenne chargée de la concurrence d'examiner le rôle des données et pas uniquement le chiffre d'affaires des entreprises dans les affaires de contrôle de concentrations[21].

Dans l'Union européenne, les informations personnelles ne peuvent pas être considérées comme un simple bien économique[22]; selon la jurisprudence de la Cour européenne des droits de l'homme, le traitement de données à caractère personnel requiert une protection afin de garantir l'exercice par une personne du droit au respect de la vie privée, de la liberté d'expression et de la liberté d'association[23]. Par ailleurs, l'article 8 de la Charte de l'UE et l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE) consacrent spécifiquement le droit à la protection des données à caractère personnel. Il s'ensuit que le règlement général de 2016 sur la protection des données contient des mesures de protection spécifiques qui pourraient contribuer à remédier aux déséquilibres du marché dans le secteur numérique. Les autorités chargées de la protection des données doivent faire respecter la minimisation des données, qui impose que les informations personnelles ne soient traitées que lorsqu'il s'agit de données «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées»[24], ainsi que le droit des personnes à recevoir des informations sur la logique suivie pour la prise de décisions automatisées et le profilage[25]. Les autorités chargées de la protection des données et de l'application de la protection des consommateurs devraient également être prêtes à informer et à conseiller les autorités de la concurrence – et en être capables – dans les affaires de concentration entre entreprises dans le secteur numérique, lorsqu'il existe des raisons de croire que la concentration pourrait porter préjudice à des particuliers.

POUVOIR ET RESPONSABILITÉ

1. Obligations légales évolutives

Les législations relatives à la protection des données, au respect de la vie privée (confidentialité des communications) et à la protection des consommateurs ont été récemment révisées ou sont en cours de révision afin de protéger plus efficacement les droits des personnes dans la nouvelle réalité numérique[26]. L'une des principales nouveautés du récent règlement général sur la protection des données est l'intégration du principe de responsabilité, qui est bien établi dans le droit de la concurrence, mais est relativement nouveau dans la législation sur la protection des données. En vertu de ce principe, les organisations soumises à des obligations de protection des données doivent être capables de démontrer que les mesures nécessaires ont été prises pour garantir le respect des règles, les autorités chargées de la protection des données n'intervenant qu'à des fins de contrôle, notamment lorsqu'il y a un signe d'infraction. Dans chacun de ces domaines, les obligations sont évolutives: ainsi, lorsqu'une entreprise jouit d'une puissance supérieure sur le marché (une préoccupation pour les autorités chargées de la concurrence), occupe une position contractuelle plus forte (protection des consommateurs) ou est chargée de traitements de données plus risqués (protection des données), elle est tenue de faire preuve d'une plus grande diligence dans les mesures qu'elle prend pour se conformer aux règles.

Or, comme nous l'avons affirmé dans des avis récents, quoique nécessaires, des législations efficaces ne suffisent pas à créer une culture de la responsabilité, notamment sur des marchés où un comportement peut léser des particuliers et la société dans son ensemble et où la concentration de la puissance de marché ne cesse de s'accroître. La réglementation est généralement en retard sur la technologie et les marchés; des services innovants et dynamiques émergent et perturbent des industries bien établies, en satisfaisant plus efficacement les demandes des consommateurs. L'application des règles à ces services novateurs est souvent contestée et requiert des clarifications des cours et tribunaux[27].

2. Concentration du marché et pouvoir d'information

Lors de l'atelier organisé par le CEPD en 2014, il a été dit que des «économies de gamme» et la concentration sur les marchés liés aux «données massives» pourraient aboutir à des situations dans lesquelles le gagnant emporte tout et à des quasi-monopoles bénéficiant d'un accroissement des rendements d'échelles en raison de la «permanence» absolue de leurs actifs numériques[28]. Ces dernières années, les concentrations sur les marchés numériques ont réduit la concurrence pour de nombreux services, les plus grandes entreprises ayant établi leur domination depuis plus d'une décennie, démentant ainsi le caractère réputé transitoire de ces marchés. Les approches traditionnelles sont considérées comme ne permettant pas de maintenir les profits à des niveaux normaux, ce qui entraîne des prix excessifs pour les consommateurs[29]. En effet, selon les quelques contrôles de concentrations ex post qui ont été menés, la plupart des concentrations tendent à entraîner des hausses de prix[30]. Bien que les entreprises dominantes sur les marchés numériques doivent leur succès à la qualité de leurs produits, en règle générale, il semble probable qu'avec le temps, les concentrations entraînent une hausse des prix et des bénéfices et une baisse de la qualité des services et de l'innovation.

Les principales entreprises du secteur numérique exercent un pouvoir considérable sur les communications et un contrôle important sur les passerelles d'accès à l'Internet, même si les autorités ne disposent d'aucun moyen pour déterminer leur «pouvoir de marché» au sens traditionnel de l'expression[31]. La plupart des gens ont désormais accès aux actualités sur les médias sociaux et les algorithmes des services en ligne déterminent le contenu à présenter aux internautes individuels en fonction de leur profil, ce qui fait de plus en plus craindre que l'expérience en ligne puisse être filtrée et se transformer en une série de caisses de résonance[32].

De la même façon, il est peu probable que les concentrations entre entreprises sur les marchés numériques renforcent le principe de minimisation des données énoncé par le droit de l'UE, ce qui pourrait être considéré comme une sorte d'efficacité en termes de volume des données à caractère personnel traitées. À l'inverse, les concentrations ont abouti au regroupement et à la combinaison de plus de données à caractère personnel, sans amélioration visible de la transparence des politiques relatives à l'utilisation de ces données.

Les préoccupations concernant le pouvoir monopolistique et le pouvoir d'information convergent donc d'une manière analogue à ce qui s'est passé à la fin du XIX^{e} siècle, lorsque la législation antitrust et les droits de l'homme sont devenus des préoccupations publiques majeures en Europe et aux États-Unis. Des organisations puissantes sont en mesure de réduire la qualité de la vie privée et de la liberté des consommateurs de services numériques ou d'agir comme des censeurs réels du contenu en ligne, même si elles n'exercent pas encore pleinement ce pouvoir[33]. Depuis la publication de notre avis préliminaire, les responsables politiques accordent une attention croissante à la nature des transactions numériques qui ne nécessitent pas un paiement monétaire, mais bien la divulgation d'informations personnelles, en particulier lorsque le traitement de données à caractère personnel n'est pas techniquement nécessaire à la fourniture du service[34].

SYNERGIES PRÊTES À ÊTRE EXPLOITÉES

1. Objectifs communs mais coopération limitée

Les législations de l'UE en matière de protection des données, de concurrence et de protection des consommateurs ont toutes pour but, comme nous l'avons fait observer, de protéger et promouvoir le bien-être et de contribuer à la création d'un marché unique européen[35]. Le dialogue en cours depuis deux ans a notamment mis en évidence la notion d'équité prégnante dans chacun de ces domaines et mentionnée dans les articles correspondants de la Charte de l'UE et du TFUE:

- l'équité est peut-être le critère le plus fondamental pour des pratiques commerciales licites dans la législation relative à la protection des consommateurs;
- le caractère loyal du traitement de données à caractère personnel est un principe de base avec la licéité et la transparence;
- le droit de la concurrence fait des concessions aux accords anticoncurrentiels «en permettant aux consommateurs d'avoir une part équitable» du bénéfice et inclut dans sa définition d'un abus de position dominante le fait «d'imposer des prix d'achat ou de vente déloyaux»[36].

En dépit de cela, la coopération entre les autorités reste limitée au niveau européen[37]. Dans notre avis préliminaire, nous avons discuté de la préoccupation commune pour le consommateur. La notion de «bien-être du consommateur» n'a toutefois jamais été clairement définie dans le droit de la concurrence et elle a tendance à être utilisée pour parler de la structure du marché et de l'efficacité économique et ne traite qu'indirectement des préoccupations des consommateurs individuels, comme le respect de la vie privée[38]. L'article 102 du TFUE interdit l'abus de position dominante consistant dans le fait d'«imposer des prix d'achat ou de vente ou d'autres conditions de transaction non équitables». Les autorités chargées de la concurrence ont pourtant tendance à laisser les services de protection des consommateurs poursuivre ces comportements abusifs, tandis que les services de protection des consommateurs laissent

parfois les autorités de la protection des données s'occuper des affaires de pratiques déloyales pour les consommateurs[39].

Les interactions entre autorités nationales ont donné des résultats. En voici quelques exemples:

- selon une décision provisoire de l'autorité française de la concurrence de septembre 2014, GDF Suez a abusé de sa position dominante en utilisant des données à caractère personnel collectées alors que la société était un monopole d'État pour promouvoir une offre combinée pour le gaz et l'électricité sur un marché ouvert non réglementé. L'autorité a ordonné à GDF de divulguer une partie de sa base de données clients à des concurrents après avoir donné aux personnes physiques la possibilité de renoncer à la divulgation;

- en août 2015, l'autorité britannique chargée de la protection des données a formulé un avis à l'intention de l'autorité britannique de la concurrence sur sa proposition d'inviter des ménages qui n'avaient pas changé de fournisseur d'électricité pendant trois ans ou plus à renoncer au partage de leurs coordonnées avec des fournisseurs concurrents;

- en septembre 2015, l'autorité belge de la concurrence a infligé une amende de 1,9 million d'euros à la Loterie nationale belge pour avoir utilisé des données à caractère personnel, collectées en sa qualité de monopole public, pour la finalité incompatible de commercialiser «Scooore!», un service commercial de pari, sur le marché voisin des paris sportifs. L'autorité a jugé que l'utilisation d'informations que ses concurrents ne pouvaient pas répliquer constituait un abus de position dominante;

- en 2016, le *Bundeskartellamt* a lancé une enquête sur les politiques de respect de la vie privée appliquées par l'entreprise de réseau social supposément dominante Facebook, qui avait eu des contacts étroits avec les autorités de protection des données, des associations de protection des consommateurs et d'autres autorités nationales de la concurrence[40].

Néanmoins, dans l'ensemble, le tableau de l'application des règles de l'UE est assez fragmenté, les autorités compétentes ne communiquant pas nécessairement entre elles lorsqu'elles traitent des affaires caractérisées dont le fond est très similaire. À titre d'exemple, des réunions conjointes entre le groupe de travail «Article 29», le réseau européen de la concurrence et le réseau de coopération en matière de protection des consommateurs, qui sont les instances de coordination européennes respectives, seraient utiles.

2. Compétences distinctes mais liées

Les autorités réglementaires subissent souvent des pressions énormes pour répondre aux attentes du public, avec des ressources limitées et une charge de travail croissante et il est normal, dans ces circonstances, qu'elles se concentrent sur leurs propres compétences. Les limites des pouvoirs et compétences respectifs des autorités doivent être respectées: il est manifeste que les autorités ne devraient pas– et ne peuvent probablement pas – faire appliquer la législation dans d'autres domaines du droit[41]. Aucun domaine du droit n'est la panacée à tous les problèmes et il serait inapproprié qu'un domaine de la réglementation se penche sur un autre pour compenser ses propres faiblesses. Les autorités de chaque domaine disposent d'instruments limités. Ainsi, les autorités de la concurrence ne peuvent s'occuper que d'abus de positions dominantes, d'ententes et de concentrations entre entreprises qui sont contraires aux intérêts des consommateurs; des conditions de service abusives ne relèvent pas nécessairement de la législation antitrust.

Un important dossier de concentration postérieur à notre avis préliminaire est celui du rachat de WhatsApp - une application populaire de messagerie qui scanne tous les carnets d'adresses, mais ne commercialise pas les informations sur les utilisateurs - par Facebook, dont l'approche en matière d'utilisation des données est très différente. La Federal Trade Commission américaine a exigé des parties qu'elles informent les clients et leur donnent le choix de ne pas accepter les conditions. Agissant en tant qu'autorité européenne de la concurrence, la Commission européenne a considéré que le règlement sur les concentrations ne contenait aucune disposition obligeant l'entité acheteuse à se conformer à l'accord de confidentialité signé par les clients de WhatsApp[42]. Chacune de ces deux approches impliquait, toutefois, que les utilisateurs des services de messagerie soient invités à accepter les nouvelles conditions ou soient empêchés d'utiliser les services. Récemment, un changement des clauses de confidentialité du service de messagerie WhatsApp a conduit la commissaire chargée de la concurrence à poser des questions à l'entité issue de la fusion[43]. Pour les futures concentrations similaires, les personnes physiques pourraient bénéficier d'une réponse plus cohérente des autorités de la concurrence, de la protection des consommateurs et de la protection des données. Les autorités de contrôle doivent être parfaitement équipées pour anticiper et prévenir tant les comportements que les concentrations susceptibles de porter préjudice aux particuliers.

Aucune de ces compétences réglementaires n'est hermétiquement fermée aux autres. Une concentration élevée des marchés pourrait porter atteinte à la protection de ces droits fondamentaux, même lorsque les autorités antitrust ne constatent pas de comportement anticoncurrentiel. Selon la jurisprudence, les autorités doivent déjà prendre en compte les incitations probables à des abus de position dominante après une concentration[44]. Il a déjà été fait appel dans le passé à l'autorité européenne de la concurrence à des fins politiques plus spécifiques, comme la déréglementation du marché des télécommunications[45]. L'article 21, paragraphe 4, du règlement sur les concentrations, en particulier, établit que les États membres appliquent les contrôles supplémentaires afin de protéger la pluralité des médias, ce qui répond aux craintes qu'une concentration dans le secteur des médias puisse porter atteinte à l'indépendance éditoriale et à la liberté d'expression consacrées par l'article 11 de la Charte[46].

«Même si elles poursuivent des objectifs différents», selon un rapport conjoint sur le droit de la concurrence et les données, publié en mai 2016 par les autorités allemande et française de la concurrence, «les questions de protection de la vie privée ne peuvent être exclues d'un examen au titre du droit de la concurrence au seul motif de leur nature»[47]. Les autorités de protection des données peuvent contribuer à expliquer comment et dans quelle mesure le contrôle des données à caractère personnel est si important pour les sociétés présentes sur les marchés. Les synergies entre les domaines du droit, qui ont fait l'objet de discussions intensives ces dernières années, pourraient déclencher une coopération plus étroite entre les autorités, en particulier lorsqu'il n'existe ni orientations ni jurisprudence. Il ne s'agit pas d'«instrumentaliser» un autre domaine du droit, mais plutôt de synchroniser les politiques et les activités répressives de l'UE, en ajoutant de la valeur lorsqu'une autorité de contrôle manque de l'expertise ou de la compétence juridique requise pour une analyse.

3. Possibilités de travailler ensemble

La stratégie en faveur d'un marché unique numérique contient de nombreuses suggestions prometteuses visant à améliorer les cadres réglementaires en matière de protection des données et des consommateurs. Cette stratégie pourrait toutefois être améliorée en introduisant un mécanisme d'application cohérente des réglementations dans les différents domaines du droit de l'UE imposant des obligations en termes de protection des droits et des intérêts des personnes physiques[48]. Sous l'angle des droits fondamentaux, la stratégie aurait également dû s'intéresser à la manière dont la plupart des gens interagissent aujourd'hui sur la Toile, des services en ligne de tous les jours reposant sur une surveillance de plus en plus granulaire des utilisateurs par les

fournisseurs de services, ce qui contraste souvent avec l'opacité avec laquelle ces mêmes fournisseurs traitent des informations personnelles (ce que l'on appelle le phénomène de la «boîte noire»).

La récente communication de la Commission sur les plateformes en ligne a reconnu que le caractère transfrontière du commerce exigeait une «coopération efficace entre les autorités qui en sont chargées»[49]. La résolution de 2016 des autorités nationales de protection des données en Europe est allée plus loin en appelant instamment à «un dialogue et à un partage d'informations accrus avec d'autres organes réglementaires responsables de la protection des droits et des intérêts des personnes physiques dans la société et l'économie numériques», en reconnaissant les efforts pour renforcer les synergies entre les cadres réglementaires en matière de protection des consommateurs, de législation antitrust et de protection des données[50]. Conformément aux principes de bonne gouvernance et de coopération loyale, les autorités chargées de la protection des données devraient, en tout état de cause, coopérer avec les agences de l'UE et les autorités de régulation nationales compétentes dans d'autres domaines politiques[51]. Un groupe de travail du Centre commun de recherche de la Commission a plaidé en faveur de la création d'une agence spécialisée, qui apporterait le soutien technique aux organes de contrôle enquêtant sur des affaires relatives au marché numérique et contrôlerait la conformité des plateformes en ligne afin de promouvoir la «cohérence entre les autorités réglementaires dans leurs domaines respectifs»[52].

Voici quelques exemples de collaboration pouvant se révéler précieuse pour les autorités réglementaires:

- examiner l'impact à plus long terme des concentrations dans le secteur numérique - comme Facebook et WhatsApp - sur les consommateurs et la question de savoir si les entreprises ou les déclarations des parties à la concentration, faites au moment de celle-ci, ont été respectées par la suite;

- les affaires impliquant des conditions et des politiques déloyales d'utilisation des données sont des occasions évidentes de collaboration entre les autorités chargées de la protection des données et de celle des consommateurs ainsi que pour les autorités de la concurrence, lorsque de telles conditions sont appliquées par des entreprises dominantes sur un marché;

- les affaires impliquant des entreprises dominantes qui se comportent d'une manière susceptible de porter atteinte aux intérêts des consommateurs ou d'exclure des concurrents respectueux de la vie privée seraient aussi des occasions évidentes de dialogue entre les autorités chargées de la protection des données et/ou des consommateurs et les autorités de la concurrence; une start-up a, par exemple, porté plainte contre le système d'exploitation mobile supposément dominant pour avoir exclu de sa boutique d'applications une appli qui permet aux utilisateurs de détecter et de bloquer des services tiers qui les suivent ou peut déclencher des programmes malveillants[53].

Nous considérons que l'article 80 du règlement général sur la protection des données offre une bonne occasion de faire appliquer collectivement la législation. Les États membres doivent appliquer cette disposition sur le recours collectif sans demander un mandat spécifique à une personne concernée. Des groupes de défense ont déjà commencé à engager des actions au titre des règles relatives à la protection des données et à la protection des consommateurs. En voici quelques exemples:

- UFC - Que Choisir et la Fédération allemande des associations de consommateurs (VZBZ) ont intenté une action contre des médias sociaux et des fournisseurs de services

en ligne pour clauses abusives dans des contrats, pratiques commerciales déloyales et violations de la législation en matière de protection des données[54];

- le Conseil norvégien de protection des consommateurs a publié une étude sur les conditions types utilisées par sept fournisseurs de services d'informatique en nuage, en fournissant des examens comparatifs de plusieurs conditions, notamment les politiques de confidentialité. L'étude a abouti à une plainte déposée auprès du Médiateur norvégien des consommateurs contre les conditions appliquées par Apple au motif qu'elles violaient la législation norvégienne et européenne en matière de protection des consommateurs. Apple a accepté de modifier ses conditions et, notamment, son droit unilatéral de modifier l'accord à tout moment, à sa seule discrétion et sans en prévenir les utilisateurs[55];

- une association autrichienne de protection des consommateurs a contesté les conditions imposées unilatéralement par Amazon en invoquant la directive sur les clauses abusives dans les contrats et la directive relative à la protection des données. (La CJUE a statué en août sur les questions de compétences dont elle avait été saisie[56].)

L'application conjointe de la législation et le dépassement de la «fragmentation réglementaire» sont devenus une nécessité pressante, reconnue par la Commission européenne - le président Juncker ayant appelé, au début de son mandat, la Commission à en finir avec le «chacun pour soi» - ainsi que par le BEUC, l'organisation européenne de défense des consommateurs[57]. Le moment est idéal pour transformer ces synergies théoriques en action positive.

FAVORISER LA PROTECTION DE LA VIE PRIVÉE ET LES TECHNOLOGIES QUI LA RENFORCENT - UN AVANTAGE CONCURRENTIEL

1. Confiance et suivi

Il est largement admis qu'il existe un problème de confiance et de manque ressenti de contrôle sur ce qui se passe dans l'environnement en ligne[58]. En 2015, le projet New America Foundation Ranking Digital Rights a étudié un grand nombre des principales entreprises du secteur technologique et a considéré qu'aucune ne répondait aux normes de base en matière de respect de la vie privée et de censure – en ne divulguant pas, par exemple, quand elles publient ou retirent du contenu, avec des résultats médiocres pour le cryptage du contenu privé[59]. Nous avons donc fortement défendu les efforts déployés par l'UE pour remédier à ce manque de confiance, en encourageant la responsabilité et les modèles économiques transparents, la liberté de choix, la portabilité des données et le contrôle de l'utilisateur, ainsi que des moyens effectifs de recours en cas de violation des droits. Plus récemment, en réponse à la consultation sur la réforme de la directive «vie privée et communications électroniques», nous avons formulé les recommandations suivantes à la Commission:[60]

1. en dehors de l'analyse de la première partie, aucune communication électronique ne devrait être tracée – par des cookies, un dispositif de relevé d'empreintes digitales ou tout autre moyen – sans un accord librement consenti que la personne physique peut aisément révoquer si elle le décide;

2. les personnes physiques devraient avoir le droit de choisir quel contenu tiers est autorisé ou bloqué;

3. les «murs de cookies», qui empêchent effectivement l'accès à des sites Internet, à moins que la personne physique ne donne son accord à un suivi généralisé qui n'est pas nécessaire à la fourniture du service, devraient être interdits;

4. les navigateurs et autres logiciels ou systèmes d'exploitation devraient proposer des contrôles par défaut qui facilitent l'accord ou le refus du suivi.

Selon la jurisprudence en matière de concurrence, une entreprise dominante a la «responsabilité particulière de ne pas porter atteinte par son comportement à une concurrence effective et non faussée dans le marché commun»[61]. Sur les marchés numériques, ces entreprises dominantes ont été accusées d'exclure par leur comportement de nouveaux venus proposant des services plus respectueux de la vie privée, comme ceux qui ne suivent pas l'activité en ligne des personnes physiques, hormis lorsque ce suivi est techniquement nécessaire à la fourniture du service. Des initiatives émanant du secteur privé, comme la norme Do Not Track du World Wide Web Consortium, qui a pour but de mettre un terme au suivi clandestin des internautes, doivent encore faire leurs preuves. C'est en partie à la suite de cela qu'est apparu le blocage des publicités, une tactique populaire pour échapper aux publicités ciblées, ce qui a déclenché en réaction des scripts de détection du blocage des publicités, utilisés par des éditeurs qui tentent d'empêcher, voire d'interdire, leur utilisation[62].

En fait, la publicité ciblée n'est pas, *en soi*, un problème de droits fondamentaux. La nécessité pour les personnes physiques de disposer d'options accessibles leur permettant de contrôler les informations personnelles les concernant est beaucoup plus pertinente pour le respect de la vie privée, la protection des données et d'autres droits et libertés fondamentaux. La concentration de données à caractère personnel dans les mains d'un nombre de plus en plus restreint de sociétés, avec peu ou aucune possibilité pour les personnes physiques de récupérer toutes les données les concernant, n'a jamais été l'intention des pionniers de l'Internet. En effet, un projet dirigé par le concepteur du World Wide Web vise à inverser cette tendance en créant un système d'applications sociales décentralisées, dans lequel les consommateurs individuels contrôlent «où, comment et avec qui» leurs données à caractère personnel sont partagées[63].

2. Le respect de la vie privée, un facteur de qualité déterminant le véritable prix des services «gratuits»

Sur les marchés multiformes, la qualité d'un produit ou d'un service, l'un des paramètres de la concurrence, a «plusieurs facettes», est «indistincte» et donc difficile à définir, mais elle demeure un paramètre valable de l'analyse de la concurrence[64]. Le respect de la vie privée et les normes de protection et de sécurité des données font partie de ce paramètre de qualité. Lorsque la protection de la vie privée offerte par un service en ligne se détériore, cela constitue un préjudice pour le consommateur, qui relève à la fois de la protection des consommateurs et du droit de la concurrence[65]. Des problèmes de transparence et d'équité dans les conditions générales de plusieurs services en ligne ont été soulevés par diverses enquêtes nationales sur les médias sociaux et d'autres services en ligne, comme l'enquête allemande sur le possible «abus de pouvoir de marché de Facebook du fait de la violation des règles relatives à la protection des données»[66].

Déterminer la capacité de l'entreprise à augmenter le prix devient problématique dans le cas des services «gratuits», puisqu'il n'existe à ce jour aucune règle commune pour mesurer le prix réel de ces offres. Cependant, les services proposés à prix nul par des entreprises qui maximisent les profits sont aussi préoccupants pour les autorités que des services proposés à tout autre prix, bien que, jusqu'à récemment, les enquêtes aient été rares. Lorsque des informations sont extraites pour une finalité autre que l'amélioration de la qualité ou la baisse du coût du produit à prix nul, la quantité d'informations extraites et les publicités qui attirent l'attention sur ces

produits représentent un coût réel pour les consommateurs. Les prix nuls ont des effets considérables sur le comportement et la demande des consommateurs et les clients posent des jugements subjectifs et pas nécessairement rationnels sur le coût en termes d'attention, d'information et de qualité du produit. L'application de la législation devrait avoir pour but de faire en sorte que lorsque des services sont proposés à prix nul, les clients obtiennent la meilleure qualité et le meilleur choix au coût le plus bas possible en termes d'information et d'attention[67].

3. Déséquilibres dans les transactions numériques

Si, comme indiqué plus haut, la collecte de données à caractère personnel est, dans le monde numérique, un substitut du prix, alors la part du «dividende numérique» entre le responsable du traitement et la personne concernée – l'opérateur et le consommateur – est plus déséquilibrée que jamais. Les plateformes numériques dominantes sont en mesure de pratiquer une discrimination en combinant les connaissances qu'elles extraient des données avec le pouvoir monopolistique et l'intégration verticale des marchés. Des pratiques déloyales et abusives existent, comme l'a révélé l'opération «coup de poing» des autorités européennes chargées de la protection des consommateurs en 2012[68]. On peut s'interroger sur le point de savoir s'il peut être équitable de soumettre des personnes physiques à des conditions générales d'utilisation de services en ligne qui nécessiteraient, en moyenne, 25 jours de lecture par an. La concurrence devrait être bénéfique aux consommateurs en termes de prix, de qualité et de choix[69], mais en l'absence de concurrence, si les consommateurs n'ont pas le choix, une entreprise monopolistique ne sera pas incitée à fournir un bon service[70].

La transparence dans l'utilisation des données est nécessaire, mais, en cas d'absence d'alternative réaliste, elle conduit simplement à une situation du type «à prendre ou à laisser» pour l'utilisateur, une préoccupation pertinente dans l'affaire Facebook en Allemagne[71]. Ces services en ligne se caractérisent par une asymétrie des informations, les personnes physiques ou les petites entreprises manquant de connaissances contextuelles sur le prix et la qualité d'un produit, alors que les grandes entreprises peuvent s'appuyer sur des flux d'information sur les prix et sur des profils de gestion des risques pour maximiser leur capacité à soutirer clandestinement des informations aux consommateurs[72]. Les autorités chargées de la protection des données et des consommateurs sont exceptionnellement bien équipées pour donner des avis sur ces développements.

4. Un marché faible pour les services respectueux de la vie privée

Le marché des technologies renforçant la protection de la vie privée – mesures destinées à réduire le traitement des données à caractère personnel sans perdre la fonctionnalité d'un produit ou d'un service – reste faible[73]. Le respect de la vie privée est un besoin humain universel, en dépit de la volonté de nombreuses personnes de divulguer des détails intimes sur les réseaux sociaux, et l'absence de concurrence en matière de respect de la vie privée représente une défaillance du marché[74]. Le règlement général sur la protection des données impose désormais aux développeurs l'obligation légale de tenir compte de la «protection des données dès la conception» et de la «protection des données par défaut». Le nouveau droit à la portabilité des données, visé dans le règlement général sur la protection des données, s'il est correctement mis en œuvre et appliqué, devrait aider les personnes physiques à éviter d'être enfermées dans des services en ligne. Nous avons également affirmé que les règles en cours de révision sur la confidentialité des communications - l'un des éléments du droit au respect de la vie privée - doivent être effectivement appliquées à toutes les communications numériques et pas uniquement aux télécommunications traditionnelles[75]. Ces développements législatifs offrent des normes minimales de protection, mais ne créent pas nécessairement les conditions de marché permettant au respect de la vie privée et à la liberté d'expression de devenir un objet

de concurrence[76]. Une coopération accrue des autorités de contrôle sur la manière de déployer les outils existants est également nécessaire pour encourager cette concurrence et s'attaquer aux comportements anticoncurrentiels qui inhibent l'innovation ou réduisent la protection de la vie privée en tant qu'élément de la qualité d'un produit.

RECOMMANDATIONS: CRÉER UN CYBERESPACE EUROPÉEN FONDÉ SUR LES VALEURS DE L'UE

En vertu de l'article 51 de la Charte, les «institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu[e les] États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union [...] respectent les droits, observent les principes et [...] promeuvent l'application» des dispositions de la Charte «conformément à leurs compétences respectives [...]»[77]. Le TFUE impose également à l'UE de veiller «à la cohérence entre ses différentes politiques et actions»[78]. Les responsables politiques et les autorités cherchent des moyens de faire connaître au public le plus large les avantages de la connectivité des données massives, d'outils informatiques puissants et de flux de données instantanés. Le Parlement européen a récemment appelé l'UE à lutter contre la fragmentation de la législation au moment d'élaborer de nouvelles dispositions réglementaires et à encourager vivement les États membres à mettre en œuvre de manière cohérente ces dispositions[79]. Les institutions de l'UE doivent donner l'exemple et devraient veiller à cette cohérence dans la protection des droits fondamentaux consacrés par la Charte. Ceci impose d'utiliser les outils existants de l'Union pour créer les conditions indispensables afin que ces droits et libertés puissent prospérer et d'appliquer ensemble les législations pour exploiter les synergies entre les domaines pertinents du droit. Nous souhaiterions proposer trois mesures pratiques pour y parvenir.

1. Mieux refléter les intérêts des personnes physiques dans les concentrations de données massives

Jusqu'à présent, le contrôle des concentrations dans l'UE s'est centré sur les entreprises qui atteignent certains seuils de chiffres d'affaires, à moins que des affaires ne soient signalées par les autorités nationales. On observe aujourd'hui des signes d'un contrôle accru des propositions de rachat d'entreprises numériques moins bien établies, susceptibles d'avoir accumulé des quantités considérables de données à caractère personnel qui doivent encore être traduites en valeur monétaire[80]. Nous sommes favorables à cette tendance et proposerions de faire appel à l'expertise d'autorités indépendantes de protection des données pour conseiller comment évaluer l'importance du bien-être des consommateurs dans ces propositions de rachat.

Par ailleurs, le règlement sur les concentrations devrait être interprété et modifié à la prochaine occasion pour protéger les droits au respect de la vie privée, à la protection des données et à la liberté d'expression en ligne, qui sont consacrés par la Charte, tout comme il protège actuellement la pluralité des médias. Les États membres devraient être autorisés à protéger également ces droits en tant qu'«intérêts légitimes et compatibles avec les principes généraux et d'autres dispositions du droit communautaire»[81].

2. Une chambre de compensation numérique pour l'application de la législation

Notre analyse nous conduit à la conclusion qu'il est aujourd'hui extrêmement urgent de faire appliquer les droits numériques de manière cohérente dans tous les domaines du droit qui régissent les marchés en ligne. L'UE applique différents outils réglementaires à des fins similaires: équité, intégration du marché et bien-être des consommateurs. Si l'application du droit de la concurrence s'est révélée tellement efficace, c'est non seulement en raison du montant des amendes infligées, mais aussi parce que ce droit perturbe le comportement des entreprises et des organisations. Les régimes récemment renforcés de protection des données et de protection des consommateurs pourraient imiter le droit de la concurrence en imposant, par exemple, des changements au traitement des données à caractère personnel qui renforcent l'équité globale et le bien-être des consommateurs.

Nous proposons donc de mettre en place une chambre de compensation numérique[82]**.** La chambre de compensation serait un réseau volontaire de points de contact au sein des autorités réglementaires au niveau tant national que de l'UE, qui sont chargées de la réglementation du secteur numérique, et pourrait également inclure des autorités comme celles du secteur des télécommunications, qui contrôlent la mise en œuvre des règles de confidentialité des communications. Les deux critères de participation à ce réseau seraient les suivants:

1. **un objectif commun** consistant à renforcer mutuellement les activités répressives respectives et à garantir au mieux les droits et le bien-être des personnes physiques, qu'il s'agisse de consommateurs ou de personnes concernées;

2. **une volonté de partager des informations et de collaborer** dans les limites des compétences légales et dans le respect de la confidentialité des enquêtes.

La chambre de compensation numérique pourrait mener à bien les activités suivantes:

1. mener une discussion (sans attribution) sur le régime juridique le plus approprié pour poursuivre des affaires ou des plaintes spécifiques concernant des services en ligne, en particulier dans les affaires transfrontières dans lesquelles plus d'un cadre juridique a pu être violé, et pour recenser les actions coordonnées potentielles ou les initiatives de sensibilisation au niveau européen à même de faire cesser des pratiques préjudiciables ou de dissuader les entreprises d'y avoir recours;

2. utiliser les normes de protection des données et de protection des consommateurs pour déterminer des «théories du préjudice» en rapport avec des affaires de contrôle de concentrations et de pratiques d'exploitation abusives au sens du droit de la concurrence, en application de l'article 106 du TFUE[83], afin d'élaborer des orientations similaires à ce qui existe déjà pour les pratiques d'éviction abusives;

3. discuter de solutions réglementaires pour certains marchés dans lesquels les données à caractère personnel constituent un élément essentiel en tant qu'alternative efficace à une législation sur les marchés numériques qui pourrait étouffer l'innovation;

4. évaluer les effets sur les droits numériques et les intérêts des personnes physiques des sanctions et des recours proposés pour résoudre des affaires spécifiques;

5. de façon générale, trouver les synergies et favoriser la coopération entre les instances répressives et leur compréhension mutuelle des cadres juridiques applicables, y compris par des contacts plus informels et formels entre le réseau européen de la concurrence, le réseau de coopération en matière de protection des consommateurs et le groupe de

travail «Article 29» (qui sera remplacé en 2018 par le conseil européen de la protection des données).

Au départ, la chambre de compensation numérique pourrait être constituée de quelques autorités volontaires, qui conviennent de partager des coordonnées et des informations, dans les limites de leurs compétences, de leur indépendance d'action et d'initiative ainsi que de la confidentialité des procédures répressives. Le CEPD est prêt à faciliter et à soutenir la mise en place et le maintien d'un tel réseau.

3. Un espace commun sur la Toile fondé sur les valeurs de l'UE

L'État a l'obligation positive de veiller au respect de la vie privée «même dans la sphère des relations entre particuliers»[84]. Nous sommes d'avis que l'UE devrait aller au-delà de la tendance actuelle de contrôle des comportements en ligne et envisager la faisabilité d'un espace commun à l'intérieur duquel les particuliers pourraient interagir sans craindre d'être suivis et de faire l'objet de conclusions abusives, une idée recommandée par plusieurs études ces dernières années[85]. Cette approche pourrait perturber le choix binaire entre les services «gratuits», qui ne sont financièrement viables que par le suivi à des fins publicitaires, et les services payants que les utilisateurs ont aujourd'hui tendance à éviter: le respect de la vie privée n'est pas un luxe, mais un droit universel et il ne devrait pas n'être à la portée que de ceux qui ont les moyens de payer. L'espace commun peut se distinguer des «enclos numériques» que la plupart des internautes tendent à utiliser aujourd'hui et qui ont été critiqués par plusieurs éminents spécialistes[86]. Il devrait être un véritable espace commun, assorti de garanties adéquates et parfaitement conforme à la Charte de l'UE, y compris en ce qui concerne les conditions régissant les limitations de l'exercice des droits et libertés visées à l'article 52, paragraphe 1, de celle-ci.

Les services sans suivi ni profilage que proposent déjà des initiatives émanant de la société civile ou de développeurs pourraient servir de modèles et d'expériences pour la promotion de nouvelles approches. Dans le même temps, les autorités de l'UE devraient encourager l'application pratique de solutions techniques pour faire respecter la préférence exprimée par les utilisateurs en matière de protection de leur vie privée, par exemple en précisant comment appliquer la norme W3C de Do Not Track comme outil de protection des données, et elles devraient examiner de quelle manière les pouvoirs répressifs élargis prévus par la réforme du cadre de protection des données pourraient soutenir cet objectif.

Nous allons organiser des discussions avec la Commission européenne et d'autres institutions de l'UE et nous invitons toutes les parties prenantes à approfondir ce débat[87].

CONCLUSION

Les droits de l'homme ont été conçus comme un moyen de protéger les personnes contre l'ingérence de l'État. La législation antitrust trouve son origine dans des décisions politiques visant à faire cesser les abus de positions dominantes pour le bien de la société dans son ensemble. Les droits des consommateurs sont apparus comme un rempart contre les pratiques commerciales abusives des opérateurs.

Les possibilités qu'offrent les données massives de stimuler la productivité et la connectivité devraient aller de pair avec des mesures de protection des données massives. Ces dernières années, l'UE a montré la voie en cherchant à encourager une course au sommet en matière de normes relatives à la protection de la vie privée dans le monde numérique. Le règlement général

sur la protection des données est une référence pour la protection des données à caractère personnel dans l'économie numérique. L'Union européenne peut encore faire plus pour une économie numérique et une société fondée sur les valeurs de l'UE en utilisant les outils disponibles pour garantir des produits et des services respectueux de la vie privée et renforçant les droits fondamentaux. Une transparence accrue, un traitement équitable, un choix effectif, l'absence de verrouillage du marché pour les modèles sans traçage sont autant d'objectifs parfaitement compatibles et complémentaires.

La stratégie pour un marché unique numérique est l'occasion idéale pour l'UE d'œuvrer de manière cohérente à la réalisation de ces objectifs. L'application effective des dispositions existantes du droit de l'UE revêt une importance capitale. Nous sommes convaincus que nos recommandations en faveur de la création d'une chambre de compensation numérique pour l'application de la législation, associée à une approche plus holistique des concentrations, ainsi que la promotion d'un espace commun fondé sur les valeurs de l'UE constitueraient des avancées majeures. Alors que les législations sur la protection des données et la protection de la vie privée se multiplient dans le monde, ceci devrait servir de plateforme pour jeter des ponts vers d'autres régions du monde et renforcer le dialogue et la coopération avec tous les pays confrontés au même défi numérique.

Nous ne sommes pas au bout de ce débat. Le CEPD a l'intention de poursuivre les discussions et de contribuer à abattre les cloisons qui font obstacle à la protection des intérêts et des droits des personnes physiques.

Bruxelles, le 23 septembre 2016

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

Notes

[1] Avis préliminaire du CEPD, 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.
[2] Rapport de l'atelier sur la vie privée, les consommateurs, la concurrence et les données massives, 2 juin 2014, https://secure.edps.europa.eu?EDPSWEB/webdav/site/mySite/shared/Documents/consultation/Big%20data
[3] COM(2015) 192 final, communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions: Stratégie pour un marché unique numérique en Europe.
[4] Avis 7/2015, Relever les défis des données massives.
[5] Plusieurs questions techniques relatives à l'analyse de la concurrence depuis l'avis préliminaire, comme la définition des marchés et le rôle des données en tant que service essentiel, ne sont pas développées plus avant dans le présent avis, qui se concentre sur les grands domaines permettant une application cohérente des règles relatives à la protection des données, à la protection des consommateurs et des règles de concurrence. Ces aspects peuvent faire l'objet de discussions plus structurées que nous entendons faciliter entre les autorités réglementaires.
[6] Avis 4/2015 du CEPD, Vers une nouvelle éthique numérique.
[7] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, 22 mai 2015.
[8] Ocello, E., Sjodin, C. & Subocs, A. (2015): «What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case», Commission européenne, Competition merger brief, 1, p. 1-7.
[9] Tim Berners Lee estimait que la Toile possède le potentiel d'être un grand égaliseur, «uniquement si nous introduisons les droits au respect de la vie privée, à la liberté d'expression (...) dans le jeu»; http://webfoundation.org/2014/12/recognise-the-internet-as-a-human-right-says-sir-tim-berners-lee-as-he-launches-annual-web-index/ [consulté le 17.09.2016]. Voir, aussi, par exemple: Nissenbaum H. et Howe, D., «Track me not: resisting surveillance in the web search»; Julia Angwin *Dragnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance*, 2014.
[10] Competition Law and Data, Autorité de la concurrence et Bundestartellamt, mai 2016.
[11] Sur la possibilité que des algorithmes de fixation des prix conduisant finalement à une intelligence artificielle s'associent de manière anticoncurrentielle et probablement contraire à l'éthique, voir Ezrachi, Ariel et Stucke, Maurice E., Artificial Intelligence & Collusion: When Computers Inhibit Competition, 2015 (8 avril 2015). Oxford Legal Studies Research Paper No. 18/2015; University of Tennessee Legal Studies Research Paper No. 267.
[12] Voir CEPD, Relever les défis des données massives.
[13] Financial Times Global 500.
[14] Monopolkomission report, «Competition policy: The challenge of digital markets», 2015, p. 36.
[15] L'article 3, paragraphe 1, de la proposition de directive de la Commission prévoit que la directive s'applique à tout contrat par lequel «un prix doit être acquitté ou une contrepartie non pécuniaire, sous la forme de données personnes ou de toutes autres données, doit être apportée de façon active par le consommateur». L'article 3, paragraphe 4, exclut du champ d'application de la directive les contrats en vertu desquels les consommateurs ne fournissent que le minimum de données à caractère personnel «strictement nécessaire à l'exécution du contrat ou au respect d'obligations légales, et dans la mesure où le fournisseur ne procède à aucun autre traitement de ces données qui soit incompatible avec cette finalité». La proposition de la Commission admet le principe que les données à caractère personnel peuvent jouer le rôle de l'argent, bien qu'elle exclue, de façon discutable, du champ d'application de la directive les situations dans lesquelles le fournisseur recueille des données à caractère personnel «sans que le consommateur ne les ait fournies activement»: COM(2015)634 final, Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique.
[16] Costa-Cabral, F. et Lynskey, O., «The Internal and External Constraints of Data Protection on Competition Law in the EU», LSE Law, Society and Economy Working Papers 25/2015, p. 11.
[17] Brown I., Marsden C., Regulating Code: Towards Prosumer Law? 25 février 2013, disponible sur: http://dx.doi.org/10.2139/ssrn.2224263 [consulté le 17.09.2016].
[18] «En 1990, les trois principaux constructeurs automobiles de Detroit cumulaient des recettes nominales de 250 milliards de dollars, une capitalisation boursière de 36 milliards de dollars et 1,2 million de salariés. En 2014, les trois plus grandes entreprises de la Silicon Valley enregistraient des recettes de 247 milliards de dollars et une capitalisation boursière de plus de 1 000 milliards de dollars, mais n'employaient que 137 000 salariés», *The Rise of the Superstars*, The Economist, 17.09.2016.
[19] «Concurrence et vie privée sur les marchés des données», discours de Joaquín Almunia, Bruxelles, novembre 2012, affirmant que «la DG Concurrence doit encore traiter un dossier dans lequel des données à

caractère personnel ont été utilisées pour enfreindre le droit européen de la concurrence»; http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm [consulté le 17.09.2016].

[20] Plusieurs études ont affirmé que les marchés comportementaux sont sujets à des défaillances, lesquelles réduisent le bien-être social, et une défaillance du marché survient en matière de respect de la vie privée en ligne lorsque le modèle économique de la publicité comportementale «semble pratiquement avoir été conçu pour tirer profit d'une rationalité limitée». Voir Borgesius, F. Z., «Behavioural Sciences and the Regulation of Privacy in the Internet, Nudging and the Law - What can EU Law learn from Behavioural Sciences»; Acquisti, A., «The Economics of privacy and the economics of personal data», The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 2010, http://www.oecd.org/sti/ieconomy/46968784.pdf [consulté le 17.09.2016].

[21] «Refining the EU merger control system», discours de la commissaire Vestager, Studienvereinigung Kartellrecht, Bruxelles, 10 mars 2016.

[22] Au sujet de l'approche européenne fondée sur les droits au respect de la vie privée et à la protection des données et étroitement liée à la dignité humaine et à l'autodétermination, voir notamment, Consumer Privacy in Network Industries, A CERRE Policy Report, 26 janvier 2016, pp. 35-36.

[23] *Z c. Finlande*, requête nº 22009/93, CouEDH 1997-I, point 95.

[24] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - «RGPD»). L'exigence selon laquelle tout traitement de données à caractère personnel ne peut être excessif au regard des finalités pour lesquelles elles sont collectées et/ou pour lesquelles elles sont traitées ultérieurement était déjà prévue par la directive 95/46/CE (considérant 28 et article 6, point b), concernant les principes relatifs à la qualité des données).

[25] Article 5, paragraphe 1, point c), et articles 14 et 15.

[26] Depuis juin 2014, la directive CE/2011/83 relative aux droits des consommateurs a abrogé la directive 97/7/CE concernant la vente à distance et la directive 85/577/CEE sur le démarchage. La législation européenne en matière de protection des consommateurs fait actuellement l'objet d'un processus de révision complet et d'un test REFIT. Le nouveau règlement (UE) 2016/679 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, et abrogeant la directive 95/46/CE, dont le projet avait été présenté par la Commission en janvier 2012, a finalement été publié le 4 mai 2016.

[27] Arrêt du 3 mai 2014 dans l'affaire C-131/12, *Google Spain SL et Google Inc./Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*. Dans cette affaire, la Cour de justice de l'UE a expliqué que l'opérateur d'un moteur de recherche qui oriente son activité vers les habitants d'un État membre de l'UE est soumis à la législation de l'UE en matière de protection des données.

[28] Rapport de l'atelier du CEPD sur la vie privée, la protection des consommateurs, la concurrence et les données massives, Bruxelles, 2 juin 2014; atelier «Trading in Big Data: if data is the new oil, how should its extraction be regulated?» Brunel University, Londres, 20 avril-1er mai 2015; l'«Independent Review of UK Economic Statistics» de Sir Charles Bean (mars 2016) suggère de mesurer la consommation de produits numériques fournis gratuitement au moyen de la valeur du temps passé sur l'Internet et de l'augmentation du trafic Internet.

[29] «Were America's firms to cut prices so that their profits were at historically normal levels, consumers bills might be 2% lower», The Economist, «The Problem with profits», 26 mars 2016.

[30] Voir Stucke, M.E. et and Grunes, A.P., *Big Data and Competition Policy*, OUP 2016, pp. 223-224; The Economist, «Too much of a good thing», 26.3.2016.

[31] «... quelques entreprises assumant une fonction de gardiennes sont en mesure de contrôler le suivi et la mise en corrélation de (...) comportements entre les plateformes, les services en ligne et des sites destinés à des milliards d'utilisateurs»; Acquisti A., Taylor C., Wagman L., The Economics of Privacy, 8 mars 2016, Sloan Foundation Economics Research Paper No. 2580411, p. 3.

[32] Pew Resarch Centre News Use Across Social Media Platforms, 2016; voir aussi, par exemple, Pariser, E., *The Filter Bubble: What the Internet is Hiding from You*, 2011.

[33] «Facebook: Political bias claim "untrue"», BBC, 10.5.2016; «Google bans payday lender advertising», *FT*, 11.5.2016.

[34] La directive «vie privée et communications électroniques» s'applique, de façon générale, lorsqu'une interférence avec la confidentialité d'une communication est techniquement nécessaire à la fourniture d'un service (par exemple, article 2, point g), article 5, paragraphe 1, article 6, paragraphe 5, et article 9, paragraphes 1 et 3). Sur l'utilisation du consentement dans le règlement général sur la protection des données, voir la note 27 de l'avis préliminaire nº 5/2016 du CEPD sur la révision de la directive «vie privée et communications électroniques» (2002/58/CE).

[35] En vertu du protocole 27 au traité sur l'Union européenne, «le marché intérieur tel qu'il est défini à l'article 3 du traité sur l'Union européenne comprend un système garantissant que la concurrence n'est pas faussée... À cet effet, l'Union prend, si nécessaire, des mesures dans le cadre des dispositions des traités, y compris l'article 352

du TFUE». Affaires jointes C-501/06 P, C-513/06 P, C-515/06 P et C-519/06 P, *GlaxoSmithKline Services Unlimited/Commission*, EU:C:2009:610, point 61.

[36] Conformément à la jurisprudence de la CJUE, l'équité dans la législation relative à la protection des consommateurs est évaluée par rapport au «consommateur moyen» (affaire C-210/96, *Gut Springenheide et Tusky*, Rec. 1998, p. I-4657, point 31); le principe de caractère loyal du traitement de données à caractère personnel est consacré par l'article 8, paragraphe 2, de la Charte de l'UE; les articles 101 et 102 du TFUE régissant le comportement anticoncurrentiel et l'abus de position dominante mentionnent tous deux l'équité.

[37] «Dans la mesure où le droit de la concurrence doit s'occuper des marchés dans lesquels des données à caractère personnel sont présentes, les spécialistes de la concurrence affirment que les données à caractère personnel devraient être analysées en fonction de leurs caractéristiques économiques, comme tout autre bien ou service. À cet égard, la réglementation relative à la protection des données pourrait simplement fixer le "cadre juridique" dans lequel les relations concurrentielles se développent et ne serait pas différente d'autres réglementations du marché. De leur côté, les autorités chargées de la protection des données se sont concentrées sur l'établissement de principes directeurs pour ce nouveau domaine du droit et ont accordé peu d'attention à son interaction avec les domaines du droit de l'UE qui l'ont précédé»; Costa-Cabral et Lynskey, «The Internal and External Constraints of Data Protection on Competition Law in the EU», p. 3. Sur les défis que représentent l'introduction de recours pour les particuliers lésés par des violations de la réglementation sur la protection des données, voir le rapport de l'Agence des droits fondamentaux sur l'accès aux voies de recours en matière de protection des données dans les États membres de l'UE, janvier 2014.

[38] Les objectifs principaux du droit de la concurrence font l'objet d'un litige en cours. Sur le bien-être des consommateurs en tant qu'objectif principal, voir l'affaire C-209/10, *Post Danmark*, et l'affaire C-67/13, *Cartes bancaires*; sur le processus concurrentiel et la structure de la concurrence (dans la mesure où il s'agit d'un indice suffisant de l'impact sur le bien-être des consommateurs), voir les affaires C-501/06 P, *Glaxo, C-95/04, British Airways*, et C/72.

[39] À titre d'exemple, la Commission belge de la protection de la vie privée a commandé un rapport à l'ICRI sur les conditions générales d'utilisation de Facebook, qui a conclu que la déclaration de droits et de responsabilité du réseau social violait la législation européenne en matière de protection des consommateurs; http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf [consulté le 17.09.2016].

[40] 14-MC-02: Mesure conservatoire du 9 septembre 2014 relative à une demande de mesures conservatoires présentées par la société Direct Energie dans les secteurs du gaz et de l'électricité; réponse du commissaire chargé de l'information au document de l'Autorité de la concurrence et des marchés «Enquête sur le marché de l'énergie: avis concernant des voies de recours possibles», août 2015; décision de l'Auditorat nº ABC-2015-P/K-28-AUD du 22 septembre 2015, affaire MEDE-P/K-13/0012 et CONC-P/K-13/0013, Stanleybet Belgium NV/Stanley International Betting Ltd et Sagevas S.A./World Football Association S.P.R.L./Samenwerkende Nevenmaatschappij Belgische PMU S.C.R.L. t. Nationale Loterij NV; le communiqué de presse sur l'enquête allemande concernant Facebook est disponible sur: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568 [consulté le 17.09.2016].

[41]Arrêt de la CJUE du 23 novembre 2006 dans l'affaire C-238/05, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL/Asociación de Usuarios de Servicios Bancarios (Ausbanc)*.

[42] Aux États-Unis, la FTC a adressé un courrier aux deux entités fusionnées concernant la nécessité de continuer d'honorer la promesse faite par WhatsApp à ses clients au sujet de sa politique de protection de la vie privée, bien qu'elle soit supérieure à celle que connaissent les utilisateurs de Facebook. Dans cette lettre, le non-respect de ces promesses conduirait à une violation de l'article 5 du FTC Act, qui interdit les pratiques déloyales ou trompeuses. Dans sa décision sur la concentration proposée, la Commission a déclaré que: «Toute préoccupation liée au respect de la vie privée découlant de la concentration accrue de données contrôlées par Facebook à la suite de la transaction ne relève pas du champ d'application des règles de concurrence de l'UE, mais bien du champ d'application des règles de l'UE en matière de protection des données»; décision de la Commission du 3 octobre 2014 déclarant une concentration compatible avec le marché commun (affaire nº COMP/M.7217 - FACEBOOK/WHATSAP), en vertu du règlement (CE) nº 139/2004 du Conseil. Voir Competition Merger Brief No. 1/2015, «Lessons from the Facebook/WhatsApp EU merger case», p. 7.

[43] «Facebook Grilled by EU's Vestager Over WhatsApp Merger U-Turn», 9.9.2016, http://www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn [consulté le 17.09.2016].

[44] C-12/03, *Commission/Tetra Laval BV*, Rec. 2005, p. I-987.

[45] Pour un examen de la jurisprudence dans laquelle la CJUE a considéré des objectifs de politique publique comme des justifications possibles de violations des règles de la concurrence et la protection des droits fondamentaux comme une justification de la jurisprudence sur le marché intérieur, voir, par exemple, Costa-Cabral et Lynskey, pp. 29-31.

[46] Nonobstant les paragraphes 1 et 2, les États membres peuvent prendre les mesures appropriées pour assurer la protection d'intérêts légitimes autres que ceux qui sont pris en considération par le règlement sur les concentrations et compatibles avec les principes généraux et les autres dispositions du droit communautaire ». Les trois catégories spécifiques d'intérêts, qui sont expressément qualifiés de légitimes, sont la «sécurité publique» (1), la «pluralité des médias» (2) et les «règles prudentielles» (4). (Article 21, paragraphe 4, du règlement (CE) nº 139/2004). http://ec.europa.eu/competition/publications/cpn/2005_1_19.pdfhttp://ec.europa.eu/information_society/media_taskforce/doc/pluralism/media_pluralism_swp_en.pdf [consulté le 17.09.2016].

[47] «Antitrust, Privacy and Big Data», Concurrences, 3 février 2015, atelier conjoint CPD-ERA, «Competition Rebooted: enforcement and personal data in Digital Markets», 24 septembre 2015, Bruxelles; Table ronde de l'*Autorité de la Concurrence*, 8 mars 2016, Paris.

[48] Voir la Stratégie du BEUC, A Consumer-Driven Digital Single Market, septembre 2015: «[Dans un environnement en ligne], les consommateurs éprouvent souvent des difficultés à naviguer, à comprendre les options qui s'offrent à eux et leurs droits et à trouver des solutions quand quelque chose tourne mal».

[49] COM (2016)288, Communication de la Commission, «Les plateformes en ligne et le marché unique numérique - Perspectives et défis pour l'Europe».

[50] Résolution de la conférence de printemps des autorités chargées de la protection des données, mai 2016, disponible sur: http://www.naih.hu/budapest-springconf/files/Resolution---new-frameworks.pdf [consulté le 17.09.2016]. Voir aussi la réponse du CEPD à la consultation publique de la Commission sur le cadre réglementaire relatif aux plateformes, aux intermédiaires en ligne, aux données, à l'informatique en nuage et à l'économie collaborative, 15 décembre 2015; Chambre des Lords, Select Committee of the European Union, 10e rapport de séance 2015-16, Online Platforms and the Digital Single Market, 20 avril 2016.

[51] Hijmans H., The European Union as a constitutional guardian of Internet privacy and data protection, pp.63-65, http://hdl.handle.net/11245/1.511969 [consulté le 17.09.2016]. (Une version modifiée de cette thèse devait être publiée durant l'été 2016 par Springer International Publishing, *The European Union as Guardian of Internet Privacy*).

[52] Rapports techniques du CCR, Institute For Prospective Technological Studies Digital Economy Working Paper 2016/05, An Economic Policy Perspective On Online Platform, pp.42-43; https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf [consulté le 17.09.2016].

[53] Plainte pour violation de la législation antitrust de l'UE, déposée par Disconnect contre Google, en juin 2015, que la plaignante a publiée intégralement sur: https://www.document.cloud.org/documents/2109044-disconnnect-google-antitrust-complaints.html [consulté le 17.09.2016].

[54] Consumer Justice Enforcement Forum (CoJEF), *Enforcement of Consumer rights: strategies and recommendations*, mai 2016.

[55] Le rapport complet de l'étude est disponible sur: http://fbrno.climg.no/wp-content/uploads/2014/02/2014-05-14-Unfair-cloud-storage-terms_report.pdf [consulté le 17.09.2016].

[56] Arrêt du 28 juillet 2016 dans l'affaire C-191/15, *Verein für Konsumenteninformation/Amazon EU Sàrl*.

[57] Les orientations politiques du président Juncker, 15.7.2014, https://ec.europa.eu/priorities/publications/president-junckers-political-guidelines_fr [consulté le 16.09.2016]; réponse du BEUC à la consultation «Autonomisation des autorités nationales chargées de la concurrence afin de les rendre plus efficaces dans l'application de la législation», 2016.

[58] Eurobaromètre Spécial 431, protection des données, juin 2015. Voir aussi l'enquête plus récente d'Opinium Research auprès de 7 000 personnes d'Europe et du Moyen-Orient, qui révèle que 75 % des consommateurs n'ont pas confiance dans la protection des données des médias sociaux et des sociétés de marketing. https://f5.com/about-us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968 [consulté le 17.09.2016]; la Commission européenne a déclaré que «l'Internet de demain est voué à l'échec si les utilisateurs n'ont pas confiance dans les plateformes en ligne et si celles-ci ne respectent pas toute la législation applicable et les intérêts légitimes des consommateurs et autres utilisateurs». Document de travail de la Commission, document d'accompagnement de la communication «Les plateformes en ligne et le marché unique numérique», p. 44. Voir aussi le discours de la commissaire Vestager, «Making data work for us», événement Data Ethics sur les données en tant que pouvoir, Copenhague, 9 septembre 2016: «Les consommateurs utilisent des moteurs de recherche... [et] ... des réseaux sociaux ... Et ils ne paient pas un sou pour ces services. Mais ils paient avec leurs données. Cela ne doit pas nécessairement poser problème, aussi longtemps que les gens considèrent que les données qu'ils partagent sont un juste prix à payer pour les services qu'ils obtiennent en échange. Les données à caractère personnel sont devenus un produit précieux. Mais cela ne peut durer que si les personnes font confiance aux sociétés qui collectent leurs données pour ce qui concerne l'utilisation qu'elles en font. Et cette confiance n'existe pas encore.»

[59] «Aucune entreprise figurant dans l'Index ne fournit aux utilisateurs des informations suffisamment claires, exhaustives et accessibles sur les pratiques qu'elles ont mises en place et qui affectent la liberté d'expression et le respect de la vie privée. Ces pratiques incluent le traitement des informations des utilisateurs, l'application des conditions de service, les demandes du gouvernement et les demandes privées»;https://rankingdigitalrights.org/index2015/findings/ [consulté le 17.09.2016].

[60] Avis préliminaire du CEPD sur le réexamen de la directive «vie privée et communications électroniques» (directive 2002/58/CE), 22 juillet 2016, pp. 14-16.
[61] Affaire 322/81, Michelin/Commission, point 70; voir la page 18 de l'avis préliminaire du CEPD.
[62] Une grande partie du débat sur les technologies de détection du blocage des publicités s'est également centrée sur la question de savoir si la détection de publicités implique le stockage d'informations personnelles, en application de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», et sur la nécessité qui en découle d'obtenir le consentement de l'utilisateur pour lancer une détection de blocage des publicités.
[63] Ce projet baptisé «Solid» (dérivé de «social linked data») est décrit comme «un projet de conventions et d'outils destinés à créer des applications en ligne décentralisées sur la base des principes du Web des données (Linked Data). Solid est un projet modulaire et extensible. Il s'appuie dans toute la mesure du possible sur les normes et protocoles W3C existants»; https://github.com/solid/solid [consulté le 17.09.2016].
[64] OCDE, The Role and Measurement of Quality in Competition Analysis, 2013.
[65] House of Lords Report, p.102. Voir Ezrachi et Stucke, The Curious Case of Competition and Quality, Journal of Antitrust Enforcement 2015,1.
[66] Consumer Justice Enforcement Forum (CoJEF), *Enforcement of Consumer rights: strategies and recommendations*, mai 2016.
[67] Voir, par exemple, Evans, D. S., Antitrust Economics of Free (April 17, 2011), Competition Policy International, Spring 2011); et Newman, J. M., Antitrust in Zero-Price Markets: Foundations (31 juillet 2014), University of Pennsylvania Law Review, Vol. 164; University of Memphis Legal Studies Research Paper No. 151): «Lorsqu'aucune analyse de marché n'a lieu, un préjudice potentiel considérable existe pour le bien-être des consommateurs en raison de la sous-application systématique de la législation antitrust».
[68] Vingt-cinq autorités ont contrôlé 330 sites Internet vendant du contenu numérique et affirment que la moitié contenait des clauses contractuelles abusives ou des informations peu claires sur le droit ou le retrait ou des informations insuffisantes sur l'identité des opérateurs et la manière de les contacter: Réseau CPC, Coup de balai sur le contenu numérique; www.ec.europa.eu/consumers/strategy.../policy.../consumer_policy_report_2014_en.pdf [consulté le 17.09.2016].
[69] 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 [2009] C45/7, 5.
[70] Décision Google/DoubleClick, point 39. L'intégration verticale et la concentration sont mises en évidence dans le rapport conjoint franco-allemand sur le droit de la concurrence et les données, Competition Law and Data, 10 mai 2016, pp. 16-19. Edelman B.G., Does Google Leverage Market Power through Tying and Bundling? Journal of Competition Law and Economics, 11 No. 2, juin 2015. Sur l'effet de levier, voir aussi Competition and Markets Authority, The commercial use of consumer data: Report on the CMA's call for information, mai 2015, paragraphes 3.60-61.
[71] Voir note 40 ci-dessus.
[72] Voir Cohen J.E., *Irrational Privacy?*, 2012; Akerlof, G. The Market for Lemons, Qualitative Uncertainty and the Market Mechanism, Quarterly Journal of Economics 84(3), pp. 488-500, 1970; Ryan Calo, R., Privacy and Markets: A Love Story, University of Washington School of Law, Legal Studies Research Paper N. 2015-26 p. 27. David A. Friedman a affirmé qu'il existe un «encadrement trompeur» de produits gratuits, qui fausse le processus décisionnel des clients; Free Offers: A New Look, 38 N.M. L. REV. 49, 68–69 (2008) .
[73] Communication de la Commission, COM(2007) 228 final, Promouvoir la protection des données par les technologies renforçant la protection de la vie privée; sur le marché des PET, voir, par exemple, «Hiding from big data», The Economist, 7.6.2014.
[74] CMA, The commercial use of consumer data, paragraphe 3.21; Executive Office of the President, President's Council of Advisors on Science and Technology, Report to the President, Big data and Privacy: a technological perspective, mai 2014.
[75] Avis préliminaire du CEPD sur le réexamen de la directive «vie privée et communications électroniques».
[76] Voir les avis du CEPD «Vers une nouvelle éthique numérique» et «Données massives». Voir aussi le rapport CERRE, «Consumer Privacy in Network Industries, Improving Network industries regulation», janvier 2016: «il existe des circonstances dans lesquelles la protection des données peut offrir un point de référence normatif pertinent pour le droit de la concurrence», Costa-Cabral & Lynskeyp.15; J.A.T. Fairfield, C. Engel, Privacy as a Public Good, Duke Law Journal, Vol. 65, Dec. 2015, No.3.
[77] Affaire C-176/12, *Association de médiation sociale/Union locale des syndicats CGT e.a., ECLI:EU: C:2014:2, 42*. Il a également été dit que les obligations découlant de la Charte s'appliquent non seulement au secteur public, mais aussi aux situations «horizontales» entre personnes physiques et morales - «Un droit fondamental serait inefficace s'il n'était protégé que contre les actes des gouvernements», Hijmans, pp. 43-46.
[78] Article 7 du TFUE. La Cour de justice de l'UE a appliqué une méthodologie d'équilibre entre la protection de la structure du marché et l'objectif d'administration de la justice des politiques publiques dans l'arrêt Wouters, C-309/99, *JCJ Wouters/Algemene Raad*, 2002.

[79] Résolution du Parlement européen du 19 janvier 2016, «Vers un acte sur le marché unique numérique», paragraphe 12.
[80] Avis préliminaire du CEPD 2014, p. 30; House of Lords Digital, p. 47. Monopolkommission Special Report No 68, Competition policy: The challenge of digital markets, 2015, pp. 110-111.
[81] Article 21, paragraphe 4, du règlement (CE) nº 139/2004 du Conseil relatif au contrôle des concentrations entre entreprises.
[82] La notion de chambre de compensation s'entend comme une agence centrale ou un canal informel pour régler les comptes, diffuser des informations ou apporter une assistance en vue d'accroître l'efficacité et la stabilité. Elle est généralement associée à l'achat et à la vente d'instruments financiers, mais il existe de multiples exemples de chambres de compensation dans des secteurs aussi variés que les chemins de fer, l'éducation, voire la protection des données et l'accès à l'information.
[83] Costa-Cabral et Lynskey considèrent qu'il peut exister un précédent à l'utilisation d'un autre domaine du droit pour constater une restriction par objet dans l'affaire C-32/11, *Allianz Hungária Biztosító Zrt/Gazdasági Versenyhivatal*, arrêt de la Cour du 14 mars 2013.
[84]*Von Hannover/Allemagne*, 2004, requête nº 59320/0; *K.U. c. Finlande*, requête nº 2872/02, points 43 et 48, CouEDH 2008.
[85] «Un dialogue plus étroit entre les autorités de régulation des différents secteurs pourrait permettre de répondre aux demandes croissantes de mise en place de partenariats mondiaux à même de créer des "communs" de données ouvertes dans lesquels des données et des idées, comme des statistiques et des cartes, peuvent circuler, être mises à disposition et être échangées dans l'intérêt général, avec moins de risques de surveillance, afin de donner aux personnes physiques davantage d'influence sur les décisions qui les concernent», avis du CEPD, Vers une nouvelle éthique numérique, p. 10, et note de bas de page 36, qui cite plusieurs sources avançant des idées similaires dans ce domaine, Schneier, B., *Data and Goliath, the hidden battles to collect your data and to control your world*, 2015.
[86] Voir, par exemple, Andrejevic, M., Surveillance in the digital enclosure, The Communication Review 10: 295-317; Zittrain, J., *The future of the Internet and how to stop it*, 2008.
[87] Voir, par exemple, l'idée proposée durant un séminaire sur la protection de la vie privée organisé par l'Autorité norvégienne de la protection des données et un membre du Conseil norvégien de technologie en 2015, qui vise à mettre en place des noms de domaine légalement tenus de respecter les règles strictes de sécurité et de respect de la vie privée régissant leur utilisation; mentionné dans: http://www.zdnet.com/article/how-two-remote-arctic-territories-became-the-front-line-in-the-battle-for-Internet-privacy/ [consulté le 17.09.2016].