«Législation sur la protection des données dans le contexte des enquêtes en matière de concurrence»

Séminaire Covington & Burling LLP

Bruxelles, le 13 juin 2013

«Protection des données et concurrence: interfaces et interaction»

Peter Hustinx

Contrôleur européen de la protection des données

INTRODUCTION

- Ce séminaire porte sur une interface de la protection des données et de la concurrence, et plus spécifiquement de la législation en matière de protection des données dans le contexte des enquêtes sur la concurrence. C'est la raison pour laquelle il aborde également un nouveau thème de portée plus générale qui a commencé à susciter énormément d'intérêt au cours des derniers mois: l'interaction entre, d'une part, la législation sur le respect de la vie privée et la protection des données et, d'autre part, la législation en matière de concurrence.
- La pertinence de plus en plus grande des données en général et, plus spécifiquement, le rôle des données à caractère personnel, dans les débats politiques et économiques actuels est incontestable: les données ont été qualifiées de «nouveau pétrole»; les données volumineuses semblent représenter la solution pour bon nombre d'activités économiques; l'accès à de grandes séries de données à caractère personnel est essentiel pour un nombre croissant de services.
- Tous ces éléments pertinents ne peuvent tout simplement pas être ignorés par les autorités responsables de l'application de la législation en matière de concurrence. Il en va évidemment de même pour les autorités qui, à l'instar de mon institution, sont chargées de faire appliquer la législation en matière de protection des données.

REMARQUE

- Permettez-moi d'être clair et d'opposer d'emblée un important démenti. Je suis ici aujourd'hui en tant que représentant d'une institution de l'Union européenne, le Contrôleur européen de la protection des données (CEPD). Notre institution remplit un rôle de contrôleur et de conseiller auprès de toutes les institutions européennes et collabore avec les autorités nationales chargée de la protection des données afin d'améliorer la cohérence et les pratiques en matière de protection des données au sein de l'UE.
- Eu égard à la législation en matière de concurrence, notre compétence de *contrôle* s'applique donc aux activités de la direction générale de la concurrence (DG COMP) de la Commission européenne. Notre fonction *consultative* nous permet également d'émettre des avis concernant tout acte législatif proposé par la Commission ou tout autre sujet en rapport avec la protection des données.
- Permettez-moi de déclarer dès le début que je ne suis *pas* en mesure de fournir des conseils ou des recommandations juridiques aux entreprises privées.
- L'intérêt de notre institution sur la question a engagé une profonde réflexion en interne qui sera développée dans un avis qui devrait être publié dans les prochains mois, dans tous les cas avant la fin de cette année.

LARGE VUE D'ENSEMBLE DES INTERFACES

- A priori, il existe des différences notables entre les législations et les politiques en matières de concurrence et celles qui concernent la protection des données.
    - La législation et la politique en matière de concurrence portent sur les comportements des entreprises (par exemple, les accords illégaux, les abus de position dominante, le contrôle des concentrations) susceptibles d'engendrer une distorsion de la dynamique concurrentielle qui existe entre elles et, en définitive, de nuire aux consommateurs. Elles garantissent essentiellement un choix équitable aux consommateurs.
    - La législation et la politique européennes en matière de protection des données visent à garantir que les droits fondamentaux des personnes, notamment leur droit à la vie privée et à la protection des données à caractère personnel, soient respectés et mis en pratique par l'intermédiaire de mesures de sauvegarde et de procédures appropriées.

- Cependant, il existe un point commun entre ces deux matières: la violation de leurs règles nuit aux consommateurs/individus/personnes concernées et elles concernent toutes deux l'intérêt public général d'une société libre et ouverte fondée sur l'état de droit et non uniquement sur la survie du plus fort.

- Il convient de souligner que les règles régissant la protection des données et la concurrence font l'objet de séries d'obligations distinctes reposant sur des bases juridiques différentes et que le respect de ces règles au sein de l'Union européenne est soumis au contrôle d'autorités différentes.
- L'indépendance des autorités responsables de la protection des données est un principe fondamental énoncé à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Ce principe a été clairement confirmé par les tribunaux européens dans deux affaires engagées contre l'Allemagne et l'Autriche. Les rôles de la Commission européenne en matière de droit de la concurrence et de droit de la protection des données sont donc relativement différents eu égard à la définition et à la mise en application des politiques.
- Le respect des règles dans l'un de ces deux domaines ne va pas nécessairement de pair avec le respect des règles dans l'autre domaine, de même que le non-respect des règles dans un des deux domaines ne signifie pas nécessairement le non-respect des règles dans l'autre. Cependant, aux interfaces de ces règles, il peut y avoir bien plus de place pour l'interaction que ce qui est largement admis ou pratiqué aujourd'hui.

INTERFACES ET INTERACTION

- Lorsqu'on pense aux trois branches principales du droit de la concurrence, on peut envisager une interaction avec la législation en matière de protection des données selon différents points de vue.
- Dans le **secteur des ententes et abus de position dominante (antitrust)**, la Commission européenne peut mener des enquêtes sur les présumés accords et pratiques interdits en vertu de l'article 101 TFUE ou les présumés abus de position dominante interdits en vertu de l'article 102 TFUE. La DG COMP effectue aussi régulièrement des enquêtes sectorielles afin de vérifier le respect des règles du traité qui s'appliquent à des secteurs entiers de l'économie.
- Dans ce contexte, la DG COMP peut réaliser des inspections, adresser des demandes d'informations, participer à des réunions et en organiser. Elle consigne toutes ses activités

et elle rend ensuite des décisions qui peuvent être contestées devant les tribunaux européens.

- Pour ce qui est du contenu de ces activités, l'analyse réalisée par la Commission commence toujours par la définition du marché. De nos jours, les données en général, et les données à caractère personnel en particulier, possèdent une valeur économique évidente et certains services nécessiteront que celles-ci soient disponibles dans des conditions acceptables. Il ressort dès lors de manière évidente que, dans certains domaines, les autorités en matière de concurrence devront tenir compte du rôle de plus en plus important accordé aux données à caractère personnel dans leur analyse de la définition du marché. Cela aura également des répercussions au moment d'établir l'existence d'un éventuel abus de position dominante et permettra ensuite de déterminer les types d'abus qui peuvent être identifiés.

- Il est également possible d'établir un rapport similaire concernant l'importance des données dans les activités d'**examen des opérations de concentration** menées par les autorités en matière de concurrence. Dans ce cas, il est probable que l'analyse prospective effectuée par l'autorité en question doive tenir compte du rôle de plus en plus important des données à caractère personnel. L'analyse devra également étudier si l'opération de concentration en tant que telle pourrait déclencher une dynamique par l'intermédiaire de laquelle la concentration du contrôle des données (à caractère personnel ou non) engendrerait une «entrave significative à la concurrence effective», pour reprendre les termes du règlement relatif au contrôle des concentrations.
- De même, en ce qui concerne les opérations de concentration, on pourrait envisager un éventuel conflit entre les règles en matière de protection des données et les éventuels moyens prescrits par l'autorité en ce qui concerne, par exemple, l'accès à certaines séries de données. Si la série de données comporte des données à caractère personnel, survient alors un contexte juridique difficile dans lequel une société concernée peut se voir exiger d'octroyer l'accès à ses données à une tierce partie et pourrait dès lors être confrontée à des exigences contradictoires entre la législation en matière de concurrence et celle dans le domaine de la protection des données.

- En ce qui concerne les domaines d'activité qui impliquent une enquête relative aux **ententes**, je pense principalement à des questions procédurales. C'est dans ce domaine que la Commission effectue le plus grand nombre d'inspections. Elle exige également de grandes quantités d'informations afin d'être en mesure d'enquêter correctement sur

l'éventuelle entente. Toutes ces activités impliquent le traitement de données à caractère personnel et la DG COMP est tenue de respecter le règlement (CE) n° 45/2001, à l'instar de toutes les autres institutions européennes, sous la surveillance du CEPD. Le fait que ces enquêtes portent généralement sur des entreprises à l'échelle nationale débouche également sur une interaction intéressante avec la législation nationale en matière de protection des données.

- De même en ce qui concerne les procédures relatives aux **aides d'État**, je pense que les éléments pertinents concernent principalement la procédure: celle-ci suppose un dialogue entre les États membres et la Commission et peut également porter sur le traitement des données à caractère personnel des personnes physiques qui bénéficient de l'aide. Dans ce contexte, on peut s'attendre à observer le même type d'interactions entre la législation en matière de concurrence et celle en matière de protection des données (tant à l'échelle européenne qu'à l'échelle nationale).

CONTEXTE PERTINENT

- Comme cela a déjà été évoqué, les évolutions technologiques de ces dernières années ont débouché sur une hausse spectaculaire de l'importance des données – y compris des données à caractère personnel – dans tous les secteurs de l'économie: par exemple, les «données volumineuses» *(big data)* ont d'importantes répercussions dans tous les secteurs, qu'il s'agisse du secteur technologique, médical, financier, de la distribution, du transport, etc.
- Il est vrai que les entreprises accordent énormément de valeur aux données concernant les consommateurs. Ces données sont très importantes pour les relations avec les clients existants, de même que pour poursuivre et élargir ces relations («exploiter le potentiel du consommateur»), ainsi que pour obtenir et développer de nouvelles relations, que ce soit par l'intermédiaire de la vente croisée ou d'autres échanges d'expérience.
- Parallèlement, dans l'Union européenne, toutes les entreprises participantes doivent respecter la législation nationale en matière de protection des données qui met en œuvre la directive 95/46/CE. Comme vous le savez certainement, la directive est en cours de révision et le Parlement européen et le Conseil travaillent actuellement sur le texte du règlement général relatif à la protection des données proposé par la Commission en janvier 2012.
- Plusieurs tendances intéressantes peuvent être observées:

- Dans tous les secteurs de l'économie, les sociétés collectent de grandes quantités de données sur les consommateurs; elles se livrent concurrence entre elles dans le but d'y avoir accès; en particulier, le secteur de la publicité semble accorder aujourd'hui une immense valeur aux données à caractère personnel, car la création de profils d'utilisateurs en ligne offre des possibilités de ciblage très sophistiquées qui étaient inimaginables dans l'environnement hors ligne; les sociétés doivent être en mesure de traiter de vastes séries de données afin d'être compétitives et d'anticiper les tendances.
- Les consommateurs maîtrisent également de mieux en mieux les technologies; le commerce électronique est en pleine expansion; les consommateurs recherchent des produits et des services en ligne dans le but de rassembler des informations avant d'effectuer leurs achats hors ligne; à présent, ils demandent également des services en lignes gratuits, tout en n'ayant pas suffisamment conscience du fait que les sociétés actives en ligne peuvent tirer parti de l'utilisation des données à caractère personnel qu'ils divulguent lorsqu'ils sont en ligne.

- D'un point de vue plus strictement juridique, la protection des données à caractère personnel au sein de l'Union européenne est un droit fondamental inscrit dans la Charte des droits fondamentaux et dans le traité sur le fonctionnement de l'Union européenne: ce droit occupe une place très importante dans la hiérarchie des principes de droit – ce qui constitue une différence notable avec les autres systèmes (comme aux États-Unis), où il relève de la protection des consommateurs. La conciliation de ces différences fondamentales dans les relations transatlantiques représente sans aucun doute un défi.
- Toutefois, notre attention se porte désormais sur le renforcement de la pratique de la protection de données dans un environnement numérique de plus en plus dynamique et mondial. Voir la révision de la protection des données mentionnée précédemment.

POLITIQUE EN MATIÈRE DE CONCURRENCE ET DE PROTECTION DES DONNÉES: ÉLÉMENTS DE FOND

- Je voudrais à présent aborder brièvement quelques éléments de fond sur lesquels nous nous penchons en ce moment en tant qu'institution.
- La vie privée en ligne est l'un des éléments utilisés par les **consommateurs** pour comparer les offres des fournisseurs de services – on pourrait dès lors concevoir l'idée d'une «concurrence en matière de vie privée». Un consommateur peut considérer qu'un service plus respectueux de la vie privée est de meilleure qualité qu'un service dont la

politique en matière de vie privée n'est pas claire ou n'est pas transparente. Cependant, les consommateurs ont l'habitude de bénéficier de services en ligne gratuits (comme des outils de recherche, de messagerie électronique, de traitement de texte ou de stockage des données) et pourraient souhaiter fournir des données à caractère personnel en échange d'un service gratuit, rapide et simple d'utilisation. Cela signifie que de meilleures politiques en matière de vie privée ne supposent pas *automatiquement* que le service ou le produit soit nécessairement *perçu* comme étant de meilleure qualité par le consommateur.

- Dans ce contexte, nous constatons également un grave problème d'**inégalité des connaissances** quant à savoir ce qu'il advient des données à caractère personnel du consommateur une fois transmises au fournisseur. Un fournisseur peut secrètement trouver de nouvelles façons d'exploiter les données à caractère personnel transmises par les consommateurs en vue d'offrir de nouveaux types de services (par exemple l'application Beacon de Facebook). La mise au point de ce type de services a de grandes répercussions pour les individus et risque de placer l'entreprise dans les limites de la légalité vis-à-vis de la législation en matière de protection des données, et ce en raison du principe de la «limitation de la finalité» qui exige que les données à caractère personnel soient utilisées uniquement à des fins compatibles avec l'objectif pour lequel elles ont été collectées à l'origine.
- Fixer la limite entre une utilisation compatible et une utilisation incompatible représente souvent un exercice complexe et délicat dans la législation en matière de protection des données. Du point de vue de la concurrence, le manque de transparence concernant les politiques de confidentialité peut sérieusement entraver le choix des consommateurs entre les fournisseurs. C'est pourquoi l'analyse de la dynamique concurrentielle, à savoir la mesure dans laquelle une entreprise est en compétition avec une autre entreprise, devrait également tenir compte de cet aspect particulier. À cet égard, les nouvelles règles de transparence contenues dans la proposition de règlement général sur la protection des données sont susceptibles d'améliorer la comparabilité des offres des différents concurrents.
- L'analyse de la dynamique concurrentielle sur ces marchés doit également prendre en considération la présence de **fournisseurs de services gratuits** qui ont besoin de recueillir d'énormes volumes de données pour être en mesure de monétiser (principalement au moyen de la publicité) tout en livrant concurrence à des fournisseurs de services payants. En d'autres termes, dans un cas les consommateurs paient avec de l'argent, dans l'autre ils paient avec leurs données à caractère personnel. Une bonne analyse de marché devrait tenir compte de ces différents modèles économiques et se pencher sur la question de

savoir si ceux-ci sont *substituables* aux yeux des consommateurs. Il s'agit sans aucun doute d'un exercice difficile, étant donné le fait que les parts de marché d'un fournisseur de services gratuits en ligne ne peuvent être fondées sur les ventes ou sur les volumes de données.

POLITIQUE DE LA CONCURRENCE EN PRATIQUE

- En ce qui concerne plus précisément les activités quotidiennes des autorités de la concurrence, je souhaiterais émettre quelques observations.
- Dans les faits, les données à caractère personnel représentent une importante **ressource** dans de nombreuses activités économiques, comme la publicité, les services de conseils ou les services statistiques. L'analyse concurrentielle au sein de l'Union n'a jamais abordé la **définition du marché** sous cet angle, mais le fait est que les données à caractère personnel sont échangées (par exemple, l'existence de «courtiers en information») à titre de ressources de valeur et que les entreprises peuvent en avoir besoin pour s'établir ou pour poursuivre leurs activités.
- Stricto sensu, la politique en matière de protection des données ne se penche pas sur des séries de données en vrac mais s'intéresse plutôt à l'éventuelle incidence du traitement des données sur chaque individu – la valeur économique de la protection des données ne réside cependant pas dans les données de chaque personne en tant que telles, mais plutôt dans la façon dont celle-ci sont collectées et organisées pour en faire des processus rentables (par exemple, les données – nom, courrier électronique, adresses, adresses IP, historique de navigation – de tous les utilisateurs d'une certaine catégorie de services en ligne ont de la valeur aux yeux des publicitaires désireux de cibler cette catégorie particulière).
- Les profils présentent de la valeur dans la mesure où ils permettent aux entreprises de cibler leur offre aux consommateurs selon des méthodes qui n'étaient pas disponibles avant l'explosion de l'internet. Tous les acteurs ne disposent pas des moyens techniques pour recréer ces séries de données/profils, ce qui se traduit, du point de vue de la concurrence, par de possibles **barrières à l'entrée**. Cependant, les marchés numériques sont très dynamiques et ont été caractérisés par des cycles de «destruction créative» (par exemple, Facebook a remplacé et tout bonnement éliminé MySpace, l'ancien plus grand réseau social). L'analyse relative aux ententes ou aux abus de position dominante exigent un équilibre subtil entre tous ces éléments.

- Un autre aspect de l'interaction entre les politiques en matière de protection des données et de concurrence concerne les cas de **position dominante sur un marché donné ainsi que leurs abus** (article 102 TFUE). Les termes exacts sur lesquels doit reposer l'interaction entre l'application des règles définies par les politiques en matière de protection des données et en matière de concurrence pour lutter contre les abus de position dominante n'ont pas encore été complètement explorés. Il convient de souligner que, du point de vue de la protection des données, si un comportement donné constitue une infraction aux règles en la matière, il importe peu de savoir si, sur le plan juridique, l'entreprise en infraction est dominante ou non (toutes autres conditions étant égales). Au contraire, les abus au sens de l'article 102 TFUE ne peuvent être sanctionnés une fois que la position dominante de l'entreprise a été démontrée.
- Tout d'abord, il convient de préciser quel est le **marché approprié** sur lequel reposera l'évaluation de l'existence d'une **position dominante**. À cet égard, la relation avec les règles en matière de protection des données subsiste tant que des données à caractère personnel sont impliquées. Si les activités de l'entreprise n'impliquent pas le traitement de données à caractère personnel, ce lien est inexistant. En outre, les marchés qui supposent le traitement de données à caractère personnel peuvent inclure les services gratuits: dans ce cas, la preuve de la position dominante ne peut être apportée sur la base du critère traditionnel de la faculté à faire grimper les prix au-dessus du niveau de la concurrence. Les autorités de la concurrence se devront de développer une approche innovante et prospective.
- Ensuite, il faut savoir que plus l'entreprise est grande (par exemple, un fournisseur de services en ligne tel que Google, Yahoo, Facebook, eBay) ou, pour être plus juste, plus son domaine d'activité est vaste, plus il sera difficile de définir les frontières des marchés concernés: les fournisseurs réalisent des financements croisés de services d'un service à un autre (concept de modèle d'activité interactif: par exemple, la société Google offre des services de recherche à titre gratuit qu'elle finance à l'aide de services de publicité en ligne offerts en échange d'une rémunération aux publicitaires et aux éditeurs). Ils peuvent exercer une discrimination entre des utilisateurs et/ou offrir des services évolutifs (par exemple, services de base gratuits pour les utilisateurs de base et augmentation des prix pour les utilisateurs plus avancés/professionnels). En outre, à quel moment un simple service de stockage en nuage n'est-il plus en concurrence avec des services gratuits et entre-t-il en concurrence avec les offres des grandes sociétés? Quel est le rôle des sources ouvertes? Etc.

QUELQUES CONSÉQUENCES

- Je perçois deux conséquences: en ce qui concerne la politique de la concurrence, il est très difficile de définir exactement quels sont les services qui sont en concurrence les uns avec les autres.
- Eu égard à la politique en matière de protection des données, le problème posé par ces entreprises «multiservices» présente plusieurs aspects: à quel moment supposent-elles le traitement de données à caractère personnel? Quelle société est chargée du contrôle des données? Quel est le champ d'application géographique de la législation en matière de protection des données? À quelles fins les données à caractère personnel étaient-elles destinées et existe-t-il un risque de détournement de fonction ou d'utilisation incompatible?
- Ces deux séries de problèmes sont différents mais surviennent parallèlement et une solution dans un domaine devrait être cohérente avec l'évaluation dans l'autre domaine: par exemple, si l'analyse concurrentielle permet de définir une catégorie de services en ligne qui doivent être considérés comme étant substituables entre eux, l'analyse relative à l'utilisation compatible devrait également tenir compte de l'aspect concernant la substituabilité (voir l'avis du groupe de travail «Article 29» sur l'utilisation compatible).
- En d'autres termes, du point de vue de la protection des données, la situation serait problématique si l'on considérait l'utilisation des données à caractère personnel aux fins de la fourniture d'un service autre que celui pour lequel ces données ont été collectées à l'origine comme étant incompatible, alors que l'analyse concurrentielle envisagerait ces deux services comme étant substituables et comme appartenant donc au même marché. Toutefois, on ne peut exclure le fait que les exigences en matière de protection des données soient plus strictes que les forces du marché. En fait, il s'agit là d'une dimension qui joue un rôle important dans l'examen de la protection des données et c'est la raison pour laquelle des sanctions fortes et efficaces (amendes «faramineuses» comme dans la conncurrence) sont véritablement nécessaires.
- On pourrait également considérer que le comportement d'une société qui peut se permettre d'enfreindre constamment les règles de confidentialité au détriment des personnes concernées, sans subir de pressions concurrentielles de la part des autres concurrents, pourrait être considéré comme un élément de l'évaluation de la position de dominance. Autrement dit, le non-respect des règles en matière de protection des données pourrait être conçu comme un «symptôme» de la position de dominance sur le marché.

Dans ce contexte, le droit de la concurrence pourrait servir à confirmer et à soutenir les règles et les principes de la protection des données sur les marchés clés.

- Une fois résolue la question de la définition de la position dominante sur un marché donné (qui ne constitue clairement pas une donnée de base), l'approche adoptée par les autorités de la concurrence consiste à démontrer qu'une pratique pourrait constituer un **abus**. Dans ce domaine, la liste des comportements abusifs possibles est très longue et ne cesse de s'allonger: par exemple, acquérir des données à caractère personnel par des moyens anticoncurrentiels, chercher à empêcher d'autres concurrents de se procurer certaines données (accords d'exclusivité), entraver la portabilité des données.
- Nous réfléchissons en ce moment à un éventuel scénario dans lequel une infraction aux règles relatives à la protection des données par une entreprise dominante pourrait fournir des preuves attestant d'un abus en vertu des critères prévus par le droit de la concurrence, mais nous ne sommes pas encore parvenus à répondre à cette question complexe.
- Parallèlement, du point de vue de la concurrence, la reconnaissance d'une position de dominance pourrait venir à l'appui d'une enquête sur la légalité du consentement accordé par une personne donnée vis-à-vis du traitement: dans quelle mesure ce consentement peut-il être considéré comme valable si le consommateur ne dispose que de peu d'alternatives pour choisir un fournisseur, voire aucune? La question du «déséquilibre significatif» entre les parties et ses répercussions sur le consentement joue désormais également un rôle dans le débat concernant la proposition de règlement sur la protection des données.

PORTABILITÉ DES DONNÉES

- À ce stade, je souhaiterais mentionner que le droit à la **portabilité des données** introduit à l'article 18 de la proposition de règlement de la Commission relatif à la protection des données exerce une incidence positive, tant sur la protection des données (contrôle par un individu de ses propres données à caractère personnel) que sur la concurrence (pas d'effet de verrouillage; plus de transparence quant à la méthode de traitement des données à caractère personnel utilisée par les entreprises; stimulation de la concurrence entre les fournisseurs de services en ligne; identification des abus plus facile en cas d'entrave à la portabilité). À titre d'exemple: la portabilité du profil sur eBay, incluant une note qui reflète la réputation, constitue un bel outil pour stimuler la croissance de plateformes alternatives sur le marché.

POLITIQUE EN MATIÈRE DE CONCURRENCE ET DE PROTECTION DES DONNÉES: ÉLÉMENTS PROCÉDURAUX

- Dans une autre perspective, je souhaite enfin brièvement présenter le rôle de contrôle du CEPD en ce qui concerne toutes les activités de traitement des données à caractère personnel déployées par la Commission, et en particulier par la DG COMP. Il porte sur la méthodologie utilisée par la DG COMP pour le traitement des données à caractère personnel dans ses activités d'enquête quotidiennes (à la fois dans ses propres locaux et à l'occasion d'inspections réalisées en dehors de ses locaux dans les États membres) concernant les atteintes présumées aux articles 101 et 102 TFUE, les concentrations qui lui sont notifiées, ainsi que dans les enquêtes sectorielles et les procédures liées à l'évaluation de la légalité des aides d'État.
- Le règlement (CE) n° 45/2001 fixe les critères sur la base desquels toutes les institutions de l'Union européenne peuvent procéder au traitement des données à caractère personnel. La DG COMP est tenue d'informer le délégué à la protection des données de la Commission de toute opération de traitement poursuivant une même finalité ou des finalités liées. Si ces opérations présentent des risques particuliers compte tenu de leur nature, celles-ci doivent être notifiées au CEPD en vue d'un contrôle préalable. Les personnes concernées peuvent également soumettre leurs réclamations concernant des cas de violation au CEPD ou concernant des actions inappropriées au Médiateur européen. Jusqu'à présent, seules quelques plaintes nous sont parvenues et nous avons rarement trouvé d'autres raisons justifiant d'ouvrir une enquête.
- Cependant, il est vrai qu'il a fallu un certain temps à la DG COMP pour remarquer que ses enquêtes à l'encontre de sociétés pouvaient entraîner le traitement des données à caractère personnel concernant plusieurs personnes concernées (par exemples, les sources, les témoins ou les représentants de la société faisant l'objet de l'enquête en cours). Ces constatations ont également été faites dans le contexte d'enquêtes à grande échelle réalisées dans le secteur de l'électricité d'un État membre. En conséquence, la DG COMP a intégré les aspects liés aux données à caractère personnel dans ses manuels internes (voir CEPD, rapport annuel 2006, p. 33-34).
- Un autre aspect concerne le conflit qui peut survenir entre le respect des demandes envoyées par la DG COMP aux entreprises sur la base du règlement (CE) n° 1/2003 (enquêtes relatives aux ententes et abus de position dominantes) et du règlement (CE) n° 139/2004 (concentrations) et le respect de la législation nationale en matière de

protection des données. Cet aspect sera étudié par d'autres rapporteurs. Cependant, j'ai déjà fait allusion à la possible interaction avec la législation nationale en matière de protection des données et des questions similaires pourraient se révéler pertinentes dans le cadre d'enquêtes internes, lorsque les sociétés sont liées par les droits nationaux en la matière.

CONCLUSIONS

- Pour résumer, le sujet du séminaire d'aujourd'hui est relativement complexe et difficile, mais il est également très pertinent et prospectif. J'ai dressé les grandes lignes sur un certain nombre de points sur lesquels nous nous penchons au CEPD et qui feront l'objet d'un avis que nous prévoyons de rendre dans le courant de l'année.
- Nous avons également discuté avec les autorités et les représentants du secteur privé aux États-Unis et avons constaté un intérêt profond pour la question. La Commission fédérale du commerce aux États-Unis (*US Federal Trade Commission*) joue un double rôle – celui d'une agence de la concurrence et celui d'une agence des consommateurs – et affiche un intérêt grandissant pour les questions qui concernent la vie privée. En ce qui concerne l'application des règles de concurrence, il est bien connu qu'en dépit des différences sur le plan juridique, les systèmes européen et américain sont bien plus proches qu'en ce qui concerne les régimes de protection des données. Cependant, nous avons également observé des similitudes quant aux façons d'aborder l'analyse de l'éventuelle interaction entre la concurrence et la protection des données.
- L'objectif de notre prochain avis sera de contribuer au débat en tant qu'experts de la protection des données, dans l'espoir de déclencher une interaction fructueuse entre la Commission et les autres autorités de mise en œuvre des règles de concurrence et, par-dessus tout, d'apporter plus de cohérence entre les législations et les pratiques dans ces deux domaines respectifs, ainsi que de créer une valeur ajoutée pour les intérêts publics en jeu.