



Les enfants face à la société de l'information

Premier séminaire euro-ibéro-américain sur la protection des données:

«La protection des enfants»

Cartagena de Indias, 26 mai 2009

Giovanni BUTTARELLI

INTRODUCTION

- C'est un grand honneur pour moi d'être avec vous aujourd'hui à Cartagena de Indias. Je tiens à remercier l'Agence espagnole de protection des données de m'avoir transmis une invitation à participer à ce séminaire, qui poursuit l'objectif très important d'examiner les questions relatives à la protection des données à caractère personnel concernant les enfants.
- Je souhaite également féliciter tous ceux d'entre vous qui s'efforcent d'assurer la protection des données à caractère personnel, un droit fondamental pour les citoyens de toute l'Amérique latine.
- À cet égard, je me réjouis en particulier des initiatives réglementaires qui sont prises en Amérique latine dans le domaine de la protection des données. J'encourage pleinement l'adoption de règles visant à soutenir un cadre juridique dans lequel la protection des données est respectée comme un droit fondamental. J'espère que ces initiatives seront soumises en temps utile à la Commission européenne

en vue de l'adoption d'une «décision d'adéquation de l'Union européenne».

- Il m'a été demandé de donner un aperçu de la position de l'Union européenne en matière de protection des données des enfants dans la société de l'information contre les actes arbitraires, préjudiciables ou illicites, comme les sollicitations d'enfants à des fins sexuelles, la discrimination, les intimidations, le harcèlement, la traque ou le profilage illicite à des fins commerciales. Pour ce faire, je vais aborder les trois questions suivantes:

Premièrement, je décrirai brièvement le cadre juridique européen en la matière, y compris les initiatives et les mesures actuelles qui visent à protéger les données concernant les enfants.

Deuxièmement, j'aborderai cette question essentielle: à quel âge les enfants peuvent-ils consentir au traitement des données à caractère personnel les concernant? J'évoquerai aussi les circonstances dans lesquelles le consentement parental s'impose. Nous examinerons l'application de ce consentement dans le contexte des réseaux sociaux. Je survolerai diverses questions pratiques liées à la vérification du consentement parental.

Enfin, j'évoquerai la question de savoir comment appliquer les règles existantes de l'UE pour veiller à une protection adéquate et efficace de la vie privée des enfants.

Mes remarques offriront une vue d'ensemble de ces questions. Je m'efforcerai de préparer le terrain pour les analyses plus approfondies de ces thèmes et d'autres qui concernent la protection des enfants et que vous pourrez entendre lors des séances d'aujourd'hui et de demain. Au sujet des thèmes abordés, je me bornerai à mentionner quelques exemples. Le premier est la masse de contenus accessibles créée par les enfants sur l'internet, qui

compromet leur dignité ou leur vie privée, et par ailleurs, les rend vulnérables, aujourd'hui ou plus tard dans la vie. Le second exemple concerne la nécessité de retirer ou d'effacer ces contenus, y compris leurs traces, dans un délai raisonnablement court.

I. CADRE JURIDIQUE ET AUTRES TYPES D'INITIATIVES

- Il ne fait aucun doute que la protection des enfants, non seulement eu égard à leurs données à caractère personnel mais aussi de façon générale, est et restera une question extrêmement préoccupante pour les Européens.
- Dans le contexte de l'environnement en ligne, le sentiment que les nouvelles technologies et les nouveaux services offrent un potentiel et des possibilités énormes et révolutionnent l'éducation, l'accès à l'information et les interactions sociales est de plus en plus répandu. Par ailleurs, ces technologies et services sont perçus comme faisant peser de nouveaux risques sur les enfants et posent des défis en matière de protection de la vie privée. L'internet est un outil important pour les activités quotidiennes des enfants telles que la communication, l'information, les connaissances, l'éducation et le divertissement.
- Ces nouveaux risques sont notamment la traçabilité des activités des enfants et, dès lors, leur exposition à des activités criminelles; le profilage et la conservation des données des enfants, associés à un risque d'abus, par exemple à des fins commerciales illicites ou déloyales. Dans ce contexte, il est utile de mentionner le fait qu'en février 2008, le Comité des ministres du Conseil de l'Europe a adopté une déclaration soulignant la nécessité de protéger la dignité, la sécurité et la vie privée des enfants sur l'internet.

- Pour faire face aux risques et inquiétudes concernant la protection des données à caractère personnel des enfants sur l'internet, les Européens disposent de différents **outils juridiques**, notamment la législation. De plus, les Européens ont adopté différents **types d'initiatives**. Si vous le permettez, je commencerai par les initiatives déjà en place et j'aborderai ensuite des outils juridiques.

II.1. INITIATIVES AXÉES SUR DES ACTIONS DE PROTECTION DES DONNÉES CONCERNANT LES ENFANTS

- Pour ce qui est des **initiatives** à l'échelle européenne, plusieurs programmes parrainés par l'Union européenne visent à protéger les enfants. Ces programmes complètent des actions similaires mises en place au niveau national.
- Depuis 1996, l'Union européenne a adopté divers programmes véritablement paneuropéens qui recherchent plus de sécurité sur l'internet pour les enfants. Le plus récent de ces programmes a été adopté en février 2008 et est entré en vigueur en janvier 2009. Il est doté d'un budget de 55 millions d'euros.
- Ce programme pluriannuel lancé en 2009 a pour but de protéger les enfants qui utilisent l'internet. La protection de la vie privée et des données à caractère personnel des enfants est l'une des principales problématiques visées dans ce programme pluriannuel.
- Entre autres mesures, le programme pluriannuel propose diverses **actions de sensibilisation**. Celles-ci ont pour but de veiller à ce que les enfants soient conscients des risques qu'ils courent lorsqu'ils dévoilent des détails personnels comme leur nom complet, leur âge, des photos, etc. sur l'internet.

- Il est bien connu que les manières classiques d'informer sur la protection des données à caractère personnel ne sont pas nécessairement efficaces dès lors qu'il s'agit d'enfants. La recherche indique que les jeunes ne lisent que rarement les déclarations de confidentialité. Pour cette raison, **le fait que ce programme pluriannuel lancé en 2009 dans l'UE privilégie la sensibilisation accrue à la nécessité de protéger les données à caractère personnel constitue, à mon avis, la meilleure approche. Nous devrions donc continuer à encourager de telles initiatives.**

II.2 CADRE JURIDIQUE

- Un enfant est un être humain à part entière. L'enfant doit dès lors jouir de tous les droits d'une personne, y compris le droit à la protection des données à caractère personnel le concernant.
- L'enfant doit être considéré comme une personne qui n'a pas encore atteint la maturité physique et psychologique, un être humain en évolution sur les plans physique et mental en voie de devenir adulte.
- Les droits de l'enfant et l'exercice de ces droits – y compris le droit à la protection des données – doivent être exprimés de manière à tenir compte de ces deux considérations.
- L'éducation et la responsabilité sont des outils essentiels à la protection des données relatives aux enfants.
- Selon les critères repris dans la plupart des instruments internationaux en la matière, un enfant est une personne âgée de moins de 18 ans, à moins qu'il n'ait acquis la majorité légale avant cet âge.

- Un premier principe juridique fondamental à respecter est celui de l'intérêt supérieur de l'enfant. Selon ce principe, une personne qui n'a pas encore atteint la maturité physique et psychologique a besoin d'une plus grande protection que les autres.
- Le but est d'améliorer les conditions d'utilisation pour l'enfant et de renforcer son droit au développement de sa personnalité.
- Ce principe est à respecter par toutes les entités, publiques et privées, qui rendent des décisions concernant les enfants. Il s'applique également aux parents et aux autres représentants légaux des enfants, soit quand leurs intérêts respectifs sont en conflit, soit quand l'enfant est représenté.
- Ce principe n'est pas facile à appliquer car, partout dans le monde, des jeunes se connectent à l'internet à partir de chez eux, de l'école ou de dispositifs sans fil. Avec l'augmentation du nombre d'applications informatiques et de technologies basées sur l'internet, de plus en plus d'informations personnelles sont recueillies et conservées. Aujourd'hui déjà, les enfants ignorent souvent que leurs informations, habitudes et comportements sont suivis en ligne, y compris à des fins commerciales et de marketing.
- En examinant le cadre juridique conçu pour protéger les enfants, il importe d'établir une distinction entre les instruments classiques de défense des droits de l'homme et les autres instruments créés plus spécifiquement pour la protection des données et de la vie privée.
- Pour ce qui est du **premier type** (instruments classiques de défense des droits de l'homme), il faut commencer par bien comprendre qu'un enfant est un être humain à part entière. Pour cette raison, l'enfant jouit de tous les droits fondamentaux d'une personne, y compris le droit à la

protection de ses données à caractère personnel. En conséquence, les instruments juridiques relatifs aux droits fondamentaux s'appliquent aussi bien aux enfants qu'aux adultes. Ces instruments sont notamment la Déclaration universelle des droits de l'homme (voir ses art. 25 et 26, para. 3), la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8) et la Charte des droits fondamentaux de l'Union européenne (art. 24).

- D'autres instruments relatifs aux droits fondamentaux contiennent des dispositions spécifiques concernant les droits de l'enfant. C'est le cas de la Déclaration de Genève sur les droits de l'enfant (1923), de la Convention des droits de l'enfant des Nations unies (1989) et de la Convention européenne sur l'exercice des droits des enfants (n° 160 du 25 janvier 1996). Je mentionnerai encore ces cinq autres instruments juridiques: la Déclaration d'Helsinki, la Déclaration des Nations unies sur les droits de l'enfant, la recommandation n° (98) 8 du Comité des ministres du Conseil de l'Europe sur la participation des enfants à la vie familiale et sociale et sur la protection des données médicales, la Convention n° 192 du Conseil de l'Europe du 15 mai 2003 sur les relations personnelles concernant les enfants, et la résolution du Parlement européen du 16 janvier 2008 intitulée «Vers une stratégie européenne des droits de l'enfant».
- Pour ce qui est des instruments du **deuxième type** (instruments dans le domaine de la protection des données et de la vie privée), vous serez peut-être étonnés d'apprendre que l'UE ne dispose pas d'instruments spécifiques de protection des données applicables aux enfants. Au lieu de cela, **on applique les principes généraux de protection des données à caractère personnel consacrés par la directive 95/46/CE relative à la protection des données à caractère personnel et par la directive 2002/58/CE concernant la vie privée et les communications électroniques.** Il est important de souligner que **dans le**

domaine des données à caractère personnel relatives aux enfants, le cadre juridique communautaire susmentionné (les directives de l'UE sur la protection des données) est complété par des dispositions prises à l'échelon national.

- Le Groupe de travail européen «Article 29» qui, comme vous le savez, est un organe consultatif indépendant dans le domaine de la protection des données et de la vie privée, a publié divers documents qui donnent des orientations sur l'application des directives de l'UE aux enfants.
- En particulier, en février 2008, le Groupe de travail «Article 29» a émis un **avis sur la protection des données à caractère personnel de l'enfant** (Principes généraux et cas particulier des écoles). Précédemment, le Groupe de travail «Article 29» avait déjà adopté plusieurs avis portant en partie sur cette question. Les avis qu'il a rendus sur le code de conduite de la FEDMA (avis n° 3/2003), sur la géolocalisation (avis n° 5/2005) et sur les visas et la biométrie (avis n° 3/2007) contiennent certains principes ou recommandations concernant la protection des données à caractère personnel des enfants. On trouve encore des orientations relatives à d'importants aspects de la vie des enfants, notamment leurs activités quotidiennes, dans d'autres avis et déclarations, y compris au sujet des données médicales.
- Par ailleurs, le CEPD, dans son avis du 23 juin 2008, a souligné le lien entre la protection des données et la sécurité des enfants, et attiré l'attention sur le fait que la protection des données relatives aux enfants est une mesure indispensable en vue d'une plus grande sécurité et de la prévention des abus. Il a précisé que la notion de contenu préjudiciable reste, malheureusement, parfois imprécise.
- De plus, le CEPD a souligné le fait que la traçabilité des activités des enfants peut les exposer à des activités

criminelles telles que des sollicitations à des fins sexuelles ou d'autres activités illégales.

- Les pratiques de profilage et la conservation des données à caractère personnel concernant les activités des enfants sont également présentées comme susceptibles de comporter des risques d'utilisation abusive, par exemple à des fins commerciales ou de recherche d'informations par des établissements d'enseignement ou des employeurs potentiels. Il importe donc d'assurer le retrait ou la suppression, dans un délai raisonnablement court, des contenus et des traces laissés par les enfants sur l'internet, et de développer et promouvoir l'information auprès des enfants.
- Enfin, nous avons encouragé l'utilisation d'instruments techniques comme l'une des solutions permettant de s'attaquer aux contenus illicites et aux comportements préjudiciables. Ces instruments sont notamment l'identification de l'âge, la reconnaissance des visages ou les technologies de filtrage mais on peut aussi mettre en place, sur les sites internet, des systèmes d'alerte et de modérateurs afin d'exclure les contenus inappropriés.
- Il faut dès lors utiliser avec précaution les instruments de filtrage ou de blocage visant à contrôler l'accès aux réseaux, en tenant compte des effets inverses qu'ils pourraient avoir et en exploitant pleinement les possibilités qu'offre la technologie pour renforcer le respect de la vie privée. La participation des entreprises est nécessaire à cet égard.
- Ces instruments devraient être mieux adaptés aux besoins pratiques et être accessibles aux parties prenantes concernées. Une autre solution suggérée consiste à mettre à la disposition du public des points de contact pour le signalement des contenus illicites et des comportements préjudiciables en ligne.

- Plus loin, j'examinerai plus en détail un aspect essentiel relevant de la législation nationale, à savoir, la détermination de l'âge auquel les enfants peuvent donner leur consentement, par comparaison avec l'âge auquel le consentement doit être donné par leurs parents ou représentants légaux.

III. L'ÂGE AUQUEL LES ENFANTS PEUVENT DONNER LEUR CONSENTEMENT, EN APPLICATION DE LA LÉGISLATION DE L'UE SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Ce chapitre couvre diverses questions dans ce domaine. D'abord, nous verrons à quel âge les enfants peuvent légalement donner leur consentement et à quel âge le consentement parental est nécessaire. Deuxièmement, nous évoquerons les aspects pratiques de la vérification du consentement parental. Troisièmement, nous aborderons les problèmes de consentement et de sensibilisation dans le contexte des réseaux sociaux et des services de localisation. Enfin, nous examinerons les garanties supplémentaires qui s'appliquent à la collecte des données à caractère personnel des enfants.

Permettez-moi de préciser que notre propos n'est pas d'examiner le bien-fondé de l'exigence de consentement parental pour la commande de biens ou services. Il s'agit là d'une question relevant de la protection du consommateur ou des contrats plutôt que du domaine de la protection des données.

Pour déterminer si le consentement parental doit être exigé, il convient de garder à l'esprit que la finalité de ce consentement, dans le contexte de la protection des données, est de préserver les intérêts de l'enfant, et non des parents.

L'autorisation parentale est souvent présentée comme une solution partielle aux problèmes auxquels sont exposés les enfants et les

jeunes lorsqu'ils sont en ligne. Néanmoins, on s'interroge sur la façon dont le consentement parental doit être considéré eu égard à la protection de la vie privée et des données à caractère personnel.

Comme l'a déclaré le Groupe de travail international sur la protection des données dans les télécommunications (IWGDPT), le consentement parental ne devrait pas être exigé dans les cas où l'enfant est capable de prendre lui-même une décision rationnelle.

Le consentement parental ne doit pas devenir un mécanisme par lequel la décision du parent supplante celle de l'enfant, sauf s'il existe un risque réel que l'enfant ne mesure pas les conséquences de sa décision ou qu'un tiers profite de sa naïveté.

En substance, le consentement parental devrait être exigé lorsqu'il est dans l'intérêt de l'enfant qu'une décision relative à un traitement loyal de ses données à caractère personnel soit prise mais qu'elle ne peut raisonnablement être laissée à la seule appréciation de l'enfant.

De toute évidence, la conversion de ces principes généraux en règles pratiques pose des difficultés.

Tous les enfants n'ont pas la même capacité à un âge déterminé.

Des enfants pourraient être tentés de donner de fausses informations s'ils estiment pouvoir en retirer un avantage. Cela ne signifie pas qu'il est inutile de demander son âge à un enfant, mais que la possibilité d'enfants ne disant pas la vérité doit être envisagée et ne doit pas être exploitée par les responsables du traitement. La prudence est de mise.

Selon certains, le consentement parental n'a de valeur que s'il est vérifiable. Toutefois, les avis divergent sur ce point.

III.1 LE CONSENTEMENT DES ENFANTS EN APPLICATION DE LA LÉGISLATION DE L'UE

- La directive 95/46/CE établit les critères à respecter pour assurer la légitimité du traitement des données. Premièrement, elle indique que le traitement peut être autorisé si la personne concernée a indubitablement donné son consentement. Il existe d'autres critères qui permettent le traitement de données sans consentement.
- Si le consentement est nécessaire, en application de la législation communautaire, les personnes de 18 ans ou plus peuvent toujours donner leur propre consentement, à moins qu'elles ne soient considérées incapables de le faire.
- **Dans le contexte de la collecte de données concernant des enfants, un point essentiel consiste à déterminer à quel âge les enfants peuvent donner leur consentement. En d'autres termes, il s'agit de savoir à quel âge les enfants peuvent être jugés capables de consentir au traitement de leurs données à caractère personnel, et jusqu'à quel âge ce consentement doit être obtenu de leurs parents ou représentants légaux.** Dans le contexte de la collecte de données en ligne, il s'agit de l'âge à partir duquel les opérateurs de sites internet ou de services en ligne commerciaux doivent obtenir le consentement directement des enfants ou, dans l'autre cas, l'âge jusqu'auquel ils doivent obtenir le consentement parental avant de recueillir des informations personnelles.
- **Les directives de l'UE ne prévoient aucune règle particulière établissant l'âge auquel les enfants peuvent donner leur consentement, par opposition aux situations dans lesquelles les parents ou représentants légaux doivent le donner à leur place.** En réalité, ces questions relèvent de l'interprétation du droit national et sont souvent liées à la capacité contractuelle, c.-à-d. l'âge auquel l'enfant peut accepter des engagements par voie contractuelle. Il s'agit de l'âge auquel l'enfant est censé avoir atteint un certain degré de maturité.

- Par exemple, comme vous le savez peut-être, et les collègues espagnols ne manqueront pas de l'évoquer, la législation espagnole exige le consentement parental pour recueillir des données concernant des enfants n'ayant pas encore atteint l'âge de **14 ans**. Passé cet âge, les enfants sont jugés capables de donner leur propre consentement¹. Au Royaume-Uni, la loi sur la protection des données ne mentionne pas d'âge ou de seuil d'âge en particulier. Toutefois, l'autorité britannique chargée de la protection des données a donné une interprétation selon laquelle les enfants de **plus de 12 ans** peuvent donner leur consentement. En revanche, les enfants de moins de **12 ans** ne peuvent donner leur consentement. Pour obtenir des données à caractère personnel les concernant, il faut d'abord obtenir la permission d'un parent ou des représentants légaux.
- Il ressort de ce qui précède que l'âge à partir duquel les enfants peuvent consentir à la collecte de leurs données à caractère personnel relève du droit national, c'est-à-dire de législation de chaque État membre. Dès lors, **ce domaine n'a pas fait l'objet d'une harmonisation au niveau de l'UE.**
- Afin de fournir aux États membres des orientations dans ce domaine, en 2002, le **Groupe de travail international sur la protection des données dans les télécommunications** a adopté une déclaration en la matière. Cette déclaration s'intitule «**Children's Privacy On Line: The Role of Parental Consent**» (*Vie privée des enfants en ligne: rôle du consentement parental*). Elle prévoit que des données à caractère personnel ne peuvent être recueillies auprès d'enfants qu'avec le consentement explicite et vérifiable d'un parent de l'enfant (ou de son tuteur ou éducateur principal), **sauf si: 1) l'enfant est âgé de 12 ans ou plus et 2) les informations recueillies se limitent aux données nécessaires pour**

¹ Article 13 du *Reglamento de Protección de Datos* (règlement relatif à la protection des données).

permettre l'envoi ultérieur à l'enfant de communications licites en ligne et 3) l'enfant comprend de quoi il s'agit. Cette déclaration précise aussi que le recours au consentement parental pour le traitement des données concernant un enfant devrait être limité dans le temps.

- Il est intéressant de comparer l'approche assez fragmentée de l'Union européenne à la situation en vigueur aux **États-Unis**, où une loi fédérale régit cette question. Cette loi votée en 1998 est le Children's Online Privacy Protection Act (COPPA - *Loi de protection de la vie privée des enfants en ligne*). La COPPA exige des opérateurs de sites internet ou services en ligne commerciaux 1) s'adressant aux enfants de moins de 13 ans et 2) s'adressant à un public général en sachant que des enfants les consultent, qu'ils obtiennent un consentement parental vérifiable avant de recueillir en ligne des données à caractère personnel auprès d'enfants.

III.2 CONSENTEMENT PARENTAL

- Si le consentement d'un parent ou représentant légal est nécessaire, **certaines garanties doivent être appliquées pour assurer la protection de l'enfant.**
- Premièrement, comme le recommande le Groupe de travail «Article 29», si des parents ou représentants légaux doivent décider de donner ou non leur consentement, leur décision doit se fonder sur l'intérêt supérieur de l'enfant. En particulier, ils doivent prendre en considération l'éventualité que la divulgation de données entraîne une menace pour la vie privée et les intérêts vitaux de leurs enfants.
- Ensuite, si le consentement parental est nécessaire, deux questions clés s'ensuivent: premièrement, comment authentifier l'âge de l'enfant (comment savoir que l'enfant est mineur)? Deuxièmement, comment vérifier le consentement

parental? Au sujet de cette dernière question, mon avis est que **le consentement parental n'a aucune valeur s'il n'est pas «vérifiable»**. Toutefois, en pratique, vérifier le consentement parental n'est pas chose aisée. Par exemple, la méthode de vérification qui consiste simplement à poser la question à l'enfant («Tes parents sont-ils d'accord?») offre une protection très limitée.

- **La directive ne contient pas de règles qui définissent les modalités de vérification du consentement parental. Le Groupe de travail «Article 29» n'a pas non plus donné d'orientations autres que dans le contexte des réseaux sociaux, que j'évoquerai plus tard.** Il incombe donc aux autorités nationales de protection des données de mettre en application la législation nationale qui fixe les exigences en la matière.
- Aux États-Unis, la COPPA détermine une situation entièrement différente. La FTC a adopté une approche de type «échelle mobile» pour le consentement parental. Selon cette approche, la méthode de consentement requise dépend de la façon dont l'opérateur utilise les données à caractère personnel de l'enfant.
- Ainsi, si l'opérateur transmet ces informations à autrui – ou permet à l'enfant de les transmettre à autrui par le biais d'un compte de messagerie électronique, d'un salon de discussion, d'un tableau de messages ou d'un autre moyen –, une **méthode de consentement très fiable** est exigée car cette situation entraîne des risques considérables pour l'enfant. En revanche, si l'opérateur n'utilise qu'à des fins internes les données à caractère personnel recueillies auprès de l'enfant, une méthode moins rigoureuse de consentement est exigée (par exemple un message électronique de confirmation ultérieure).
- Les méthodes d'obtention du consentement parental qui satisfont aux normes de «**grande fiabilité**» comprennent: l'obtention d'un formulaire signé par le parent par courrier postal ou télécopie; l'acceptation et la vérification d'un

numéro de carte de crédit; la réception d'un appel téléphonique des parents par un service de numéro vert doté de personnel compétent; l'envoi d'un message électronique accompagné d'une signature numérique.

III.3 SENSIBILISATION ET CONSENTEMENT DANS LE CONTEXTE DES RÉSEAUX SOCIAUX ET DES SERVICES DE LOCALISATION

- Le Groupe de travail prépare actuellement un avis sur les **réseaux sociaux**. Dans ce contexte, le Groupe de travail est confronté aux problèmes liés à la vérification de l'âge dans la mesure où les enfants sont des utilisateurs de réseaux sociaux.
- Le Groupe de travail reconnaît les difficultés inhérentes à la vérification de l'âge et préconise de nouvelles recherches pour trouver les moyens de résoudre ces difficultés, notamment l'utilisation de logiciels spécialisés.
- Dans son avis, qui devrait être publié sous peu, le Groupe de travail encourage les initiatives de sensibilisation, recommande aux réseaux sociaux de ne pas solliciter de données sensibles dans leurs formulaires d'inscription et de ne pas entreprendre de marketing direct ciblé sur les mineurs.
- **La question de la vérification de l'âge et du consentement des enfants se pose non seulement dans le contexte des réseaux sociaux mais également dans celui des services de localisation.**
- En 2005, le Groupe de travail «Article 29» a publié un document à ce sujet. Il a analysé la situation des parents qui souhaitent localiser leur enfant grâce à son téléphone portable.

- À cet égard, le Groupe de travail «Article 29» est d'avis que les fournisseurs de services doivent adopter des procédures adéquates pour identifier les personnes qui s'inscrivent en tant que parents et restreindre l'accès à leurs services à ces seules personnes.
- Par ailleurs, la question du consentement du mineur à faire l'objet d'une demande de localisation peut aussi être posée. Sur ce point, le Groupe de travail a observé qu'il était impossible de vérifier, lors d'une demande de localisation, si l'utilisateur du téléphone est bien le mineur concerné et non une autre personne, éventuellement majeure, à qui l'abonné au service aurait confié le téléphone en question. Le Groupe de travail a donc recommandé de recueillir le consentement de l'utilisateur du téléphone (l'enfant), à tout le moins lors de l'inscription au service. Afin d'éviter les inscriptions frauduleuses de téléphones, les fournisseurs de services devraient, par exemple, envoyer des messages aux téléphones en question pour informer leurs utilisateurs que leur appareil fait l'objet d'une demande de localisation, afin que ces derniers sachent qu'ils sont localisables.

III.4 AUTRES ASPECTS LIÉS AU CONSENTEMENT

- Les autorités nationales de protection des données sont d'accord sur l'application de certaines règles supplémentaires concernant la collecte en ligne de données auprès d'enfants. En particulier:
- Premièrement, on ne peut recueillir auprès d'enfants des informations personnelles relatives à d'autres personnes (par exemple les parents).
- Deuxièmement, le transfert à des tierces parties d'informations personnelles recueillies auprès d'un enfant

doit faire l'objet du consentement explicite et vérifiable d'un parent de l'enfant ou de son représentant légal.

- Troisièmement, les enfants ne peuvent être appâtés par une promesse de gain ou autre incitation en l'échange de la divulgation d'informations personnelles.
- Quatrièmement, le recours au consentement parental pour le traitement des données d'un enfant doit être limité dans le temps. Quand une personne cesse d'être un enfant ou devient manifestement capable de prendre elle-même des décisions rationnelles la concernant, le traitement des données doit se baser sur les décisions de cette personne et non plus sur celles de ses parents.

IV. SÉLECTION DE PRINCIPES DE PROTECTION DES DONNÉES APPLICABLES AUX ENFANTS

- Outre les règles qui s'appliquent concernant le consentement, je tiens à souligner **certains principes et aspects de la protection des données** qui peuvent s'avérer particulièrement importants dans le contexte de la protection des données des enfants. Étant donné le temps qui m'est imparti, je me bornerai à évoquer quelques dispositions des directives de l'UE ainsi que leur application à la collecte de données relatives aux enfants.
- D'après l'**article 6, paragraphe 1, point b)**, de la directive 95/46/CE, les données d'enfants ne peuvent être traitées de manière incompatible avec les finalités qui justifient leur collecte.
- Dans certains cas, des responsables du traitement, comme des écoles ou opérateurs de sites internet, fournissent les noms et adresses de leurs élèves à des tiers, très fréquemment à des fins de marketing. Cela arrive par

exemple lorsque les données sont transmises à des entreprises de produits pour enfants, lesquelles cherchent à attirer ces enfants pour en faire des clients.

- Cette pratique peut constituer une violation du principe de finalité car les données destinées aux écoles ou à certains sites internet ne sont pas censées être utilisées à des fins de marketing. Un tel traitement des données n'est possible que si le responsable du traitement a obtenu le consentement adéquat, éventuellement des parents des enfants ou de leurs tuteurs. Malheureusement, des données sont souvent exploitées en ligne pour du microciblage ou de la publicité comportementale.
- **L'article 6, paragraphe 1, point c),** de la directive 95/46/CE dispose que seules des données adéquates, pertinentes et non excessives peuvent être collectées et traitées.
- Afin d'appliquer ce principe à la collecte de données relatives à des enfants, les responsables du traitement doivent prêter une attention particulière à la situation de l'enfant et, pour ce faire, veiller à ce que seules des données pertinentes soient collectées. Les responsables du traitement ne devraient pas profiter des enfants et devraient s'abstenir de demander des informations qui ne sont pas absolument pertinentes aux fins du traitement des données.
- **L'article 10** de la directive 95/46/CE exige que des informations soient fournies concernant le traitement des données à caractère personnel.
- Dans le contexte de la collecte de données concernant des enfants, la notification est particulièrement importante pour sensibiliser ces derniers aux risques et dangers qui peuvent découler des activités en ligne.

- À cet égard, il est essentiel que les avertissements soient publiés au bon endroit et au moment opportun. En d'autres termes, ils devraient être affichés directement à l'écran avant que les informations ne soient collectées.
- Le Groupe de travail a recommandé aux responsables du traitement de donner des avertissements progressifs rédigés dans un langage simple, concis, pédagogique et facile à comprendre. Un avertissement plus court devrait contenir les informations de base à fournir au moment de recueillir les données à caractère personnel. Cet avertissement doit s'accompagner d'un avertissement plus détaillé, éventuellement assorti d'un lien hypertexte, reprenant toutes les considérations pertinentes. Toutefois, il faut préciser que, à l'instar de nombreux adultes, les jeunes ne lisent que rarement l'intégralité de la déclaration de confidentialité affichée par les sites internet qu'ils consultent. Sur bon nombre de sites Web, la déclaration de confidentialité est rédigée dans un langage spécialisé, technique ou juridique qui est difficile à comprendre.

V. CONCLUSION

- À mon sens, le cadre juridique de l'Union européenne, en particulier ses directives, prévoit somme toute une solide protection des données à caractère personnel relatives aux enfants.
- Il faut cependant admettre que des améliorations sont possibles concernant la façon dont ces directives s'appliquent à la collecte d'informations personnelles concernant les enfants dans la société de l'information.
- Les travaux du Groupe de travail «Article 29», qui fournissent des orientations sur les modalités de mise en œuvre des principes de collecte de données à caractère

personnel relatives aux enfants, sont particulièrement utiles. Toutefois, ils ne sont peut-être pas suffisants.

- Des travaux complémentaires du Groupe de travail «Article 29» pourraient s'avérer nécessaires. Par exemple, il serait probablement très utile que le Groupe de travail complète son document en y intégrant d'autres orientations sur les méthodes permettant de vérifier l'âge des enfants et le consentement parental, en particulier dans le contexte de la collecte de données en ligne. Des travaux supplémentaires dans ce domaine seraient fort appréciés.
- Ainsi qu'il ressort de la résolution sur la vie privée des enfants en ligne adoptée lors de la 30^e conférence internationale des commissaires à la protection des données et de la vie privée (Strasbourg, le 17 octobre 2008), il faudra impérativement adopter une approche axée sur l'éducation, s'agissant également des contenus créés par les enfants, en combinaison avec une réglementation sur la protection des données.

Le CEPD et toutes les autorités chargées de la protection des données sont les interlocuteurs compétents dans ce contexte.

Je vous remercie de votre attention.

Giovanni BUTTARELLI