

**AVIS N° 38 / 2002 du 16 septembre 2002.**

*N. Réf. : 10 / A / 2002 / 029*

**OBJET : Avis d'initiative relatif à la protection de la vie privée des mineurs sur l'Internet.**

---

La Commission de la protection de la vie privée,

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier l'article 29;

Vu le rapport du Président,

Émet, d'initiative, le 16 septembre 2002, l'avis suivant :

## I. LA SPÉCIFICITÉ DE LA SITUATION DES MINEURS SUR L'INTERNET :

---

### ***Une relation déséquilibrée.***

Le réseau Internet est un moyen de communication qui, comparé aux autres modes de communication, favorise une diffusion et une accessibilité à l'information sans contraintes, à l'échelle planétaire. Une telle diffusion peut facilement entraîner une perte de maîtrise de l'individu sur les données qu'il communique en ligne.

Si de nombreuses personnes n'imaginent pas, lorsqu'elles communiquent en ligne des informations personnelles, les multiples réutilisations dont ces données peuvent faire l'objet, ce constat est encore plus vrai lorsque ce sont des enfants qui surfent sur l'Internet.

L'enfant est en situation de faiblesse lorsqu'il communique avec des tiers sur l'Internet : il est plus influençable qu'un adulte, moins méfiant, et il ne connaît pas forcément ses droits.

La loi du 8 décembre 1992 relative à la protection de la vie privée <sup>(1)</sup> n'opère pas de distinction entre la protection des données personnelles des enfants et celle des adultes.

Nombre de ses articles laissent néanmoins une marge d'appréciation, et exigent de celui qui les applique qu'il mette en balance les droits et intérêts des parties en présence (celui qui collecte, et celui dont les données sont traitées).

Lorsque l'on traite des données à caractère personnel relatives à des enfants sur l'Internet, il s'agit donc d'interpréter la loi en gardant à l'esprit le déséquilibre qui caractérise la relation entre le responsable du traitement et le sujet de données. Cette interprétation se traduira notamment par une application stricte des principes suivants : la transparence de l'information fournie à l'enfant, la loyauté de la collecte, et une limitation stricte des types de données collectées.

Ces différents principes sont explicités au point II du présent avis.

### ***La question de la limite d'âge.***

Si le mineur est défini par le Code Civil comme la personne de l'un ou de l'autre sexe qui n'a point encore l'âge de 18 ans accomplis,<sup>(2)</sup> l'on admet de façon générale une gradation dans la protection du mineur, qui se trouve renforcée dans les premières années, pour s'atténuer lorsque le mineur approche de l'âge de 18 ans.

Certains aspects de la protection s'atténuent ainsi entre 13 et 16 ans, lorsque le mineur passe du stade d'enfant à celui d'adolescent. Ainsi, les règles relatives aux programmes de télévision pour enfants s'adressent aux mineurs de moins de 12 ans; les règles de protection des jouets sont déterminées par rapport aux mineurs de moins de 14 ans; le mineur peut retirer de l'argent de son compte d'épargne, avoir accès à certains types de films, consommer une boisson alcoolisée dans un débit de boissons ou conduire un cyclomoteur à partir de 16 ans. Il peut également défendre seul certains intérêts liés à son statut personnel en justice.<sup>(3)</sup> Mais il ne peut en principe <sup>(4)</sup> contracter et exercer pleinement ses droits qu'à partir de 18 ans.

---

<sup>1</sup> Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ci-après « la loi ».

<sup>2</sup> Article 388 C.C.

<sup>3</sup> Tels que l'établissement de sa propre filiation ou le droit de former une action en réclamation d'état.

<sup>4</sup> Avec quelques exceptions, notamment dans le cadre du droit du travail.

Cette transition s'appuie notamment sur le critère de la capacité de discernement de l'enfant. Si ce critère peut être variable compte tenu du contexte pratique et juridique, on le situe néanmoins souvent entre 12 et 14 ans.<sup>(5)</sup>

Au regard de ce critère, et tenant compte du contexte spécifique de l'Internet, la Commission est d'avis que le mineur, et de façon plus spécifique l'enfant qui n'a pas encore une capacité de discernement suffisante, nécessite une protection particulière au regard de l'application de la loi relative à la protection de la vie privée.

## II. APPLICATION DES PRINCIPES DE LA LOI :

---

### A. Les sites destinés aux enfants :

Les responsables de ce type de sites s'adressent à un public spécifique. Si la présentation et les objectifs du site sont adaptés en conséquence (couleurs, taille des caractères, style rédactionnel, présentation de jeux,...), les aspects juridiques et éthiques liés au contenu du site doivent eux aussi être appréhendés en tenant compte de la perception propre des mineurs.

Plusieurs principes nécessitent de ce fait une application particulière, afin que tout traitement de données à caractère personnel relatives aux mineurs soit effectué de façon légitime.

#### ➤ L'information à fournir (principe de transparence).

L'article 9 de la loi prévoit pour tout responsable une obligation de fournir à la personne dont les données sont collectées différentes informations :

- a) *le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;*
- b) *les finalités du traitement;*
- c) *l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing;*
- d) *d'autres informations supplémentaires, notamment :*
  - *les destinataires ou les catégories de destinataires des données,*
  - *le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,*
  - *l'existence d'un droit d'accès et de rectification des données la concernant; (...)*

Cette information doit être fournie en tenant compte de l'âge de celui à qui elle est destinée : la formulation doit être simple et accessible, et le responsable devrait utiliser un style direct en s'adressant personnellement au mineur.

Ainsi, le responsable du site doit se présenter de façon claire, indiquer son adresse et la façon dont le mineur peut obtenir plus d'informations le concernant (adresse e-mail et adresse physique);

---

<sup>5</sup> C'est notamment le cas en Espagne (le code de conduite de l'association espagnole de commerce électronique relatif à la protection des données sur l'Internet prévoit des dispositions protégeant les mineurs de moins de 13 ans), aux Etats-Unis (le texte du Children On-line Privacy Protection Act du 21 octobre 1998 prend comme critère l'âge de 13 ans ), et en Allemagne (la référence est l'âge de 14 ans : loi réglementant la dissémination de contenus écrits et média dommageables pour les enfants - Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte, GjSM, 12 juillet 1985).

Il doit indiquer pourquoi certaines informations personnelles relatives au mineur lui sont nécessaires, et insister sur le fait que le mineur garde toujours la maîtrise de ces informations : il peut toujours décider de ne plus participer ou de se désabonner du site (forum, newsletter, ...), et demander la correction ou la suppression de ses données au responsable par un moyen simple et bien mis en évidence.

Le mineur devrait, par ailleurs, être encouragé à informer ses parents de ses activités en ligne, à les faire participer à ces activités, et à leur demander leur avis avant de transmettre des données à caractère personnel.

Un encart destiné aux parents pourrait être ajouté sur la première page du site et les pages où des données sont collectées, afin de les informer de la politique du site en matière de traitement de données à caractère personnel.

### ➤ **Le principe de nécessité** <sup>(6)</sup>

Les sites destinés aux mineurs ne devraient procéder à une collecte de données que dans des circonstances limitées, et lorsque cette collecte est strictement nécessaire à la finalité poursuivie : la distinction que l'on opère parfois dans les formulaires usuels à destination d'adultes, entre information « nécessaire » et « facultative » ne peut être utilisée dans le cadre d'une collecte auprès d'un mineur.

Les données permettant une identification directe du mineur, telles que son nom de famille, son adresse, son numéro de téléphone, sa photo ou le nom de son école, ne devraient en principe pas être collectées.

Ainsi :

Lorsqu'il est proposé au mineur d'obtenir une adresse e-mail, la procédure d'obtention ne devrait pas inclure de données permettant son identification directe. En outre, il devrait être conseillé au mineur de ne pas faire figurer son vrai nom, mais un pseudonyme, de préférence ludique ou de fantaisie, dans son adresse e-mail.

Si le site propose un forum de discussion, un minimum de données à caractère personnel doit être fourni dans le cadre de la procédure d'inscription. Ces informations doivent rester limitées (adresse e-mail, pseudonyme).

Par ailleurs, l'attention du mineur doit être attirée sur le fait qu'il faut éviter de diffuser des informations trop personnelles (telles que ses véritables nom et adresse) sur un site ouvert à tous, afin de limiter les risques de collecte sauvage par des tiers – collecte bien entendu illégale - des données ainsi publiées.

De la même manière, un responsable de traitement qui propose un abonnement à une lettre d'information ne doit collecter que les informations lui permettant l'envoi électronique de ce courrier : l'adresse e-mail, éventuellement l'âge (et non la date de naissance exacte) doivent suffire. Le nom de famille, l'adresse ou le numéro de téléphone du mineur ne sont pas nécessaires et ne doivent pas être repris dans le formulaire.

Dans ces différentes hypothèses, il ne s'agit pas d'encourager le mineur à fournir de fausses informations, comme par exemple une fausse identité présentée comme étant la vraie, mais de privilégier la constitution d'un profil peu détaillé, qui corresponde strictement à ce qui est nécessaire pour utiliser le service en ligne.

---

<sup>6</sup> Article 4, § 3 de la loi.

Les données collectées dans un contexte spécifique ne peuvent en aucun cas être utilisées à des fins différentes de celles pour lesquelles elles ont été collectées et qui ont été annoncées dans le cadre de l'obligation d'information.

En outre, dans une optique de protection des mineurs, elles ne devraient pas être cédées à des tiers.

➤ **Les principes de légitimité et de loyauté <sup>(7)</sup>**

Le caractère influençable du mineur est un élément déterminant quant à l'application du principe de légitimité et de son corollaire, le principe de loyauté, dans le traitement des données.

De façon générale, toute collecte à des fins de marketing de données relatives à des mineurs qui n'ont pas atteint l'âge de discernement doit ainsi être considérée comme non légitime.

Il apparaît également déloyal et illicite de collecter via un mineur des données concernant son entourage, telles que les centres d'intérêts ou les habitudes de consommation des membres de sa famille.

Il en va de même pour toute collecte de données qui serait effectuée par le truchement d'un jeu ou d'un cadeau.

Certaines catégories de données à caractère personnel, considérées comme des données sensibles, sont énumérées aux articles 6 et 7 de la loi et font l'objet d'une protection spécifique.

En ce qui concerne les mineurs, il peut s'agir en particulier de données qui révèlent l'origine raciale ou ethnique (questions relatives à la couleur de peau, au pays d'origine), les convictions religieuses ou philosophiques, de données relatives à la vie sexuelle, ainsi que de données relatives à la santé.

La loi interdit le traitement de ces données, sauf dans des cas limitativement indiqués.

En principe, aucune donnée sensible aux termes de la loi ne devrait pouvoir être collectée auprès de mineurs qui n'ont pas atteint l'âge de discernement. Dans certains cas spécifiques, tel qu'une nécessité de transmettre des données relatives à la santé du mineur via l'Internet, le traitement devrait pouvoir être effectué avec le consentement parental, et bien entendu sous réserve du respect des autres obligations de la loi (notamment, la fourniture d'informations détaillées par le responsable sur les conditions de traitements des données)<sup>(8)</sup>

---

<sup>7</sup> Article 4, §§ 1<sup>er</sup> et 2 de la loi.

<sup>8</sup> Voyez les articles 25 à 27 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B., 13.03.02.

## ➤ **Le traitement d'images.**

La diffusion de photos de mineurs sur l'Internet est de plus en plus souvent envisagée dans le milieu scolaire, qu'il s'agisse de la mise en ligne de la photo de classe sur le site web de l'école, ou de la publication de photos individuelles, parfois échangées avec les élèves d'autres écoles.

De la même façon que les données sensibles, les photos font l'objet d'une protection spécifique, encadrée par la théorie du droit à l'image.<sup>(9)</sup>

En vertu de ces dispositions, le consentement de la personne concernée doit en principe être obtenu avant toute utilisation de sa photo.

Lorsque la diffusion concerne des mineurs, il s'agit d'obtenir leur consentement préalable, ainsi que celui des parents lorsque l'enfant n'a pas atteint l'âge de discernement.

Ce consentement doit être obtenu de façon spécifique et explicite : la signature d'une autorisation générale en début d'année scolaire, qui couvrirait en même temps d'autres activités des élèves, n'est pas suffisante. Le document à signer doit se référer de façon précise au(x) type(s) de photos qui feraient l'objet d'une diffusion sur Internet, au but de cette diffusion, et demander le consentement pour chaque type de publication envisagé, de façon à permettre par exemple à un parent de s'opposer à la mise en ligne du portrait de son enfant, tout en acceptant la diffusion de la photo de classe.

### ***A propos du consentement parental.***

La Commission est d'avis que le consentement d'un parent ne doit pas être systématiquement requis lorsque des données relatives à un mineur sont traitées sur l'Internet. Elle souligne ainsi que le consentement parental ne devrait pas être un mécanisme permettant à un parent de passer outre la décision de l'enfant, sauf s'il existe un risque sérieux que l'enfant n'apprécie pas correctement les conséquences de sa décision, ou que sa naïveté naturelle soit exploitée.<sup>(10)</sup>

C'est la raison pour laquelle la Commission insiste dans ce document sur la nécessité d'obtenir un consentement parental dans des circonstances déterminées, et notamment :

- ◆ lorsque l'enfant n'a pas atteint l'âge de discernement,
- ◆ lorsque des données à caractère sensible sont collectées,
- ◆ lorsque la finalité poursuivie n'est pas dans l'intérêt direct du mineur (marketing, transmission des données à des tiers)
- ◆ lorsque les données sont destinées à être rendues publiques (diffusion d'informations sur un forum de discussion, ou sur le site Internet d'une école).

---

<sup>9</sup> Article 10 de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins.

Pour plus de détails sur la protection de la vie privée dans le cadre de la prise d'images, une note élaborée par la Commission sera prochainement disponible en ligne : <http://www.privacy.fgov.be>

<sup>10</sup> Voyez, à titre informatif, le document de travail du Groupe de travail International relatif à la protection des données dans les télécommunications « Childrens' privacy on line : the role of parental consent », 31<sup>st</sup> meeting of the International working group on data protection in telecommunications, Auckland, 26/27 March 2002, [http://www.datenschutz-berlin.de/doc/int/iwgdpt/child\\_en.htm](http://www.datenschutz-berlin.de/doc/int/iwgdpt/child_en.htm).

## **B. Les sites non destinés aux enfants :**

La question de la protection des données à caractère personnel d'un mineur se pose également lorsque ce dernier visite des sites qui ne lui sont pas directement destinés.

Sans être forcément de nature illégale, le contenu disponible en ligne (contenu à caractère violent ou sexuel par exemple) ou les pratiques de collectes de données à caractère personnel sur ces sites peuvent être dommageables pour le mineur.

Différentes mesures de protection, dont certaines ont déjà été préconisées par une recommandation du Conseil de l'Union européenne du 24 septembre 1998,<sup>(11)</sup> devraient être mises en œuvre afin de limiter l'accès des mineurs à de tels sites :

- ◆ un étiquetage descriptif et/ou une classification des contenus,
- ◆ une page d'avertissement, un signal sonore ou visuel,
- ◆ des systèmes de vérification de l'âge des visiteurs.

Ce dernier moyen de protection fait ici l'objet d'un examen plus approfondi, dans la mesure où il implique un traitement de données à caractère personnel des visiteurs de sites Internet dont le contenu risque de « nuire à l'épanouissement physique, mental ou moral » des mineurs.

La Commission de la protection de la vie privée, en accord avec ses homologues des différents pays de l'Union européenne, a insisté à diverses reprises<sup>(12)</sup> pour que soit préservée la vie privée des internautes qui visitent le web, et pour que chacun puisse surfer de façon anonyme ou pseudonyme.

La Commission admet cependant que dans certains cas, l'absence de toute possibilité d'identifier son interlocuteur sur Internet peut avoir des conséquences préjudiciables: un adulte peut ainsi se faire passer pour un enfant pour accéder à certains sites qui leur sont réservés, de la même façon qu'un enfant peut prétendre être un adulte afin d'accéder à d'autres sites.

Il s'agit dès lors de combiner le principe fondamental de limitation de la collecte de données à caractère personnel avec la nécessité de protéger certaines catégories d'internautes en fonction de leur âge, et de favoriser les moyens de vérification de l'âge les moins intrusifs possibles .

Différentes techniques d'identification peuvent être employées, allant de l'envoi sur support papier d'une photocopie de la carte d'identité, au développement récent des services d'authentification ou de certification en ligne.

---

<sup>11</sup> Recommandation du Conseil du 24 septembre 1998 concernant le développement de la compétitivité de l'industrie européenne des services audiovisuels et d'information par la promotion de cadres nationaux visant à assurer un niveau comparable et efficace de protection des mineurs et de la dignité humaine. Cette recommandation s'inscrit dans un cadre plus large, incluant le "Livre vert" sur le même sujet (COM(96)483 , <http://europa.eu.int/en/record/green/gp9610/protec.htm>) ainsi que le dernier Rapport d'évaluation de la Commission au Conseil et au Parlement européen sur la protection des mineurs et la dignité humaine (COM(2001)106 final, [http://europa.eu.int/comm/avpolicy/regul/new\\_srv/pmhd\\_en.htm](http://europa.eu.int/comm/avpolicy/regul/new_srv/pmhd_en.htm))

<sup>12</sup> Voyez notamment :

- Au niveau national : L'avis 34/2000 du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique: <http://www.privacy.fgov.be>,
- Au niveau européen, la recommandation 3/97 « L'anonymat sur l'Internet », WP 6, 3 décembre 1997; le document de travail « Le respect de la vie privée sur Internet - Une approche européenne intégrée sur la protection des données en ligne » WP 37, 21 novembre 2000 : [http://www.europa.eu.int/comm/internal\\_market/fr/dataprot/wpdocs/index.htm](http://www.europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm)

➤ **L'envoi d'une copie de pièce d'identité** (carte d'identité, passeport, permis de conduire...) :

Une telle communication peut être effectuée par fax ou par courrier ordinaire. Une utilisation systématique d'un tel procédé, outre sa lourdeur, a également pour conséquence la diffusion de données d'identification non nécessaires au but poursuivi (nationalité, sexe, photo), et dont certaines, tel le numéro de registre national, font l'objet d'une protection particulière.<sup>(13)</sup>

➤ **La transmission d'un numéro de carte de crédit :**

Seul un adulte étant en principe habilité à détenir une carte de crédit, l'envoi du numéro tendrait à assurer que le visiteur du site a atteint la majorité.

On relève toutefois que ce système se base sur l'utilisation, à des fins de vérification de l'âge, d'informations qui sont à l'origine destinées à effectuer des paiements. Si un tel détournement de finalité n'est pas forcément illégitime en soi, il n'en faut pas moins souligner que la généralisation de la transmission de ce type de données en dehors du contexte de paiements multiplie les risques de réutilisations frauduleuses.

Enfin, il est relativement aisé même pour un mineur de se procurer le numéro de carte d'un proche ou de générer soi-même un numéro au hasard.

➤ **La garantie donnée par un tiers de confiance :**

Différents types de procédure peuvent être envisagés, qui ont pour point commun de partir d'une vérification unique de l'âge de la personne concernée par un tiers de confiance, qui fournira ensuite un moyen de vérification électronique de l'âge aux responsables de sites Internet.

Ce moyen de vérification électronique pourra être par exemple la fourniture d'un code, d'un numéro d'identification et/ou d'un mot de passe spécifique, que l'internaute pourra présenter afin d'accéder au contenu des différents sites. Il peut également consister en une signature électronique certifiée.<sup>(14)</sup>

Le tiers de confiance pourrait avoir différents statuts : il pourrait s'agir d'un organisme de certification, dont le statut est déjà réglementé, ou par exemple d'un fournisseur d'accès à Internet, si les contraintes techniques et organisationnelles le permettent. Celui-ci délivrerait au moment de la conclusion d'un contrat de connexion (notamment par le câble ou l'ADSL) différents codes d'accès « enfants » ou « adultes » destinés aux membres de la famille.

La mise en place d'un tel système devrait en tout état de cause s'accompagner d'une harmonisation des normes techniques et des critères de classification utilisés par les différents acteurs de l'Internet.

Le principe de l'intervention d'un tiers de confiance permet ainsi de garantir que le visiteur est un adulte – ou un mineur, dont l'âge se situe dans une tranche déterminée (par exemple, en dessous de 13 ans, entre 13 et 16 ans, entre 16 et 18 ans).

Il ouvre la possibilité de moduler non seulement l'accès aux sites pour adulte, mais de protéger également les sites pour enfants contre d'éventuels visiteurs indésirables.

---

<sup>13</sup> La loi limite aussi bien les conditions d'accès au registre national que les conditions d'utilisation du numéro de registre national proprement dit. Seuls certaines autorités publiques ou organismes définis par la loi du 8 août 1983 organisant un registre national des personnes physiques peuvent, selon les conditions de cette loi, faire usage du numéro ou accéder aux données du registre.

Ces mesures, conformes au prescrit de la directive européenne 95/46 relative à la protection des données à caractère personnel, sont destinées à limiter les risques d'interconnexion de fichiers sur la base d'un identifiant unique.

<sup>14</sup> De tels systèmes de certification se développent actuellement aux Etats-Unis, suite à l'adoption d'une réglementation protectrice des droits des enfants sur l'Internet (le « Children Online Privacy Protection Act »).



Le système a, en outre, l'avantage de limiter la diffusion des données détaillées figurant sur la carte d'identité : celles-ci sont communiquées une seule fois, au tiers de confiance. Celui-ci ne retient que les données qui devront être certifiées auprès des responsables de sites Internet, ici l'âge de la personne concernée.

La Commission juge utile de rappeler à cet égard la position déjà développée dans son avis 34/2000 relatif au commerce électronique :

*« La Commission considère qu'une distinction doit être faite entre les certificats qui concernent l'identité de l'utilisateur, et ceux qui concernent les attributs, ou certaines qualités de cet utilisateur. **Parmi les différents attributs que peuvent comporter les certificats, l'utilisateur auquel se rapportent ces informations devrait techniquement être mis en mesure de sélectionner ceux des attributs qu'il désire faire parvenir à son interlocuteur dans le cadre d'une communication déterminée.** Un certificat pourrait ainsi être utilisé de façon à communiquer au correspondant une certaine qualité de l'utilisateur – comme sa fonction professionnelle, si cela s'avère nécessaire dans le cadre de cette communication, sans que d'autres attributs non nécessaires, par exemple sa qualité de membre d'une association, ne soient transmis. Il importe également que l'utilisateur puisse utiliser et envoyer un certificat concernant son identité sans que ne soient joints des certificats concernant ses différents attributs.*

*La Commission souligne en outre que dans certaines circonstances, **la transmission d'informations contenues dans le certificat relatives à l'identité de l'utilisateur ne doit pas être requise** : ainsi, une transaction qui dans la vie « réelle », peut être effectuée sans communication d'identité, doit pouvoir l'être de la même façon sur Internet, à partir du moment où le vendeur a obtenu des garanties suffisantes quant à la fiabilité (en particulier la solvabilité) de son interlocuteur<sup>(15)</sup> »*

### III. LES MODES D'ACTION :

---

Pour que ces systèmes soient efficaces, il est indispensable, d'une part, que les tiers de confiance remplissent des critères d'indépendance et d'intégrité particulièrement stricts,<sup>(16)</sup> et d'autre part, que les parents soient informés et formés à utiliser ce type de services, pour eux et pour leurs enfants.

Il s'agit en outre de combiner ces services avec d'autres types de protection tels que ceux décrits dans la recommandation susmentionnée du Conseil de l'Union européenne du 24 septembre 1998, et en particulier, l'étiquetage et le filtrage des sites Internet.

Des campagnes d'information et de formation, d'une part des adultes (plus spécialement des parents, des enseignants et éducateurs), d'autre part des enfants, s'avèrent de ce fait indispensables.

L'efficacité des mesures passe également par la sensibilisation des professionnels, tels que responsables de sites Internet, fournisseurs de service et de contenu.

---

<sup>15</sup> Voyez à cet égard les dispositions relatives à l'utilisation de pseudonymes, telles que prévues à l'article 8 de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, J.O., L13/12 du 19 janvier 2000.

<sup>16</sup> En ce qui concerne les prestataires de services de certification : voyez la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, M.B., 29.09.2001.

Des initiatives de sensibilisation sont envisagées dans ce contexte à différents niveaux : la Commission européenne finance un grand nombre de projets réunis sous le thème « Plan d'action pour la promotion d'une utilisation plus sûre d'Internet », <sup>(17)</sup> dont des travaux sur les filtres et la labellisation des sites, <sup>(18)</sup> ainsi que des actions de sensibilisation, mises en œuvre dans le cadre de projets nationaux ou transnationaux. <sup>(19)</sup> D'autres initiatives nationales telle que celle du Délégué général aux droits de l'enfant, <sup>(20)</sup> ainsi que les travaux actuellement poursuivis par l'Observatoire des droits de l'Internet <sup>21</sup> sur le sujet, doivent également être salués.

La Commission entend poursuivre l'examen de la problématique des droits des mineurs sur l'Internet en collaboration avec ses homologues européens, et procéder à une évaluation concrète de la protection actuelle offerte par les sites Internet destinés aux enfants.

Ces travaux effectués en collaboration avec d'autres instances pourront donner lieu à l'adoption de remarques complémentaires par la Commission.

En outre, ils ne préjugent pas de l'adoption d'un avis ultérieur dans la mesure où une initiative législative viserait à préciser au niveau national les règles de protection des mineurs sur l'Internet.

Pour le secrétaire,  
légitimement empêché :

Le président,

(sé) D. GHEUDE,  
conseiller.

(sé) P. THOMAS.

---

<sup>17</sup> Pour une vue d'ensemble : [http://europa.eu.int/information\\_society/programmes/iap/index\\_en.htm](http://europa.eu.int/information_society/programmes/iap/index_en.htm)

<sup>18</sup> Voyez en particulier le site <http://www.icra.org>

<sup>19</sup> Voyez, entre autres :

- le projet ONCE : Online children education : <http://www.theonceproject.net/be/once.asp>

- le site « for kids by kids » : <http://www.fbkko.org/>,

- le site « netconsumers » qui fournit des conseils aux enfants et aux parents :

<http://www.net-consumers.org/erica/francais.htm>

<sup>20</sup> Un logiciel de filtrage destiné aux parents est disponible gratuitement (en phase test) sur le site du délégué général aux droits de l'enfant de la Communauté française de Belgique : <http://www.cfwb.be/dgde/neox.htm>

<sup>21</sup> Voyez le site <http://www.internet-observatory.be>