GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES

00483/08/FR
WP 147

Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)

Adopté le 18 février 2008

Le groupe a été créé en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (justice civile, droits fondamentaux et citoyenneté) de la direction générale « Justice, liberté et sécurité » de la Commission européenne, B-1049 Bruxelles, Belgique, bureau LX-46 06/80.

Site web : http://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm

I – Introduction

1) – Contexte

Le présent avis porte sur la protection des informations concernant les enfants. Il est essentiellement destiné aux personnes qui gèrent les données à caractère personnel des enfants. Dans les écoles, il s'agit plus particulièrement des enseignants et des autorités scolaires. Il s'adresse également aux autorités nationales de contrôle de la protection des données, qui sont chargées de surveiller le traitement de ce type de données.

Ce document doit être envisagé dans le contexte de l'initiative générale de la Commission européenne décrite dans sa communication « Vers une stratégie européenne sur les droits de l'enfant ». En contribuant à cet objectif général, il cherche à renforcer le droit fondamental des enfants à la protection des données à caractère personnel.

Ce sujet n'est pas totalement nouveau pour le groupe de travail « Article 29 », qui a déjà adopté plusieurs avis relatifs à cette question. Ses avis sur le code de conduite « FEDMA » (avis 3/2003), sur l'utilisation des données de localisation (avis 5/2005) et sur les visas et les éléments d'identification biométrique (avis 3/2007) contiennent certains principes ou recommandations concernant la protection des données relatives aux enfants.

Le présent document a pour objectif de synthétiser cette question de manière structurée, en définissant les principes fondamentaux applicables (partie II) et en les illustrant par des références aux données scolaires (partie III).

Le domaine des données scolaires a été sélectionné car c'est l'un des plus importants secteurs de la vie des enfants et il représente une part significative de leurs activités quotidiennes.

Son importance tient également au caractère sensible de la plupart des données traitées dans les établissements scolaires.

2) – Objectif et champ d'application

L'objectif du présent document est d'analyser les principes généraux relatifs à la protection des données relatives aux enfants et d'expliquer leur pertinence dans un domaine sensible particulier, celui des données scolaires.

Ce faisant, il vise à identifier les questions importantes pour la protection des données relatives aux enfants en général et à donner des orientations aux personnes travaillant dans ce domaine.

Selon les critères définis dans les principaux instruments internationaux applicables dans ce domaine, un enfant est une personne de moins de 18 ans, à moins qu'il ou elle n'ait acquis la majorité légale avant cet âge.

Un enfant est un être humain dans toute l'acception du terme. À ce titre, il doit jouir de l'ensemble des droits d'une personne, y compris le droit à la protection de ses données à caractère personnel. Cependant, la situation de l'enfant est particulière et doit être envisagée sous deux perspectives, statique d'une part et dynamique d'autre part.

D'un point de vue statique, l'enfant est une personne qui n'a pas encore atteint la maturité physique et psychologique. D'un point de vue dynamique, l'enfant est dans la phase de développement physique et intellectuel qui fera de lui un adulte. Les droits de l'enfant et leur exercice, y compris le droit à la protection des données, doivent être exprimés de manière à tenir compte de ces deux perspectives.

Le présent avis est fondé sur la conviction que l'éducation et la responsabilité sont essentielles à la protection des données de l'enfant. Il examine les grands principes applicables dans ce domaine. La plupart se rapporte aux droits de l'enfant, mais sera envisagée dans le contexte de la protection des données.

Ces principes sont tous énoncés dans les principaux instruments internationaux en vigueur, dont certains se rapportent aux droits fondamentaux de l'homme mais comprennent également des règles spécifiques aux enfants. Les plus importants sont les suivants :

- Déclaration universelle des droits de l'homme du 10 décembre 1948 – articles 25 et 26, paragraphe 3
- Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 – article 8
- Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 – article 24[1]

Les autres instruments qui se rapportent directement aux droits de l'enfant sont les suivants :

- Déclaration de Genève des droits de l'enfant de 1923
- Convention des Nations unies relative aux droits de l'enfant du 20 novembre 1989
- Convention européenne sur l'exercice des droits des enfants, Conseil de l'Europe, n.º 160, du 25 janvier 1996[2]

---

[1] Et aussi :
- Déclaration d'Helsinki, juin 1964, Pr. I-11,
- Pacte international relatif aux droits économiques, sociaux et culturels du 16 décembre 1966 – art. 10, paragraphe 3,
- Pacte international relatif aux droits civils et politiques du 16 décembre 1966 – arts. 16 et 24,
- Protocole facultatif du 16 décembre 1966.

[2] Et aussi :
- Déclaration des Nations unies des droits de l'enfant du 20 novembre 1959.
- Recommandations de l'Assemblée parlementaire du Conseil de l'Europe sur différents aspects de la protection des enfants (n. 1071, 1074, 1121, 1286, 1551).
- Recommandations du Comité des ministres du Conseil de l'Europe sur la participation des enfants à la vie familiale, R (98)8, et la protection des données médicales, R (97), 5.
- Convention du Conseil de l'Europe sur les relations personnelles concernant les enfants, n.192, du 15 mai 2003.

Il va de soi que la perspective générale de la protection des données à caractère personnel doit être systématiquement considérée telle qu'elle est consacrée dans les directives sur la protection des données (directive 95/46/CE du 24.10.1995 et directive 2002/58/CE du 12.7.2002) et, partiellement, dans d'autres instruments.[3]

II – Principes fondamentaux

A – Remarques générales

1) – Intérêt supérieur de l'enfant

Le principe juridique de base est celui de l'intérêt supérieur de l'enfant.[4]

Ce principe repose sur le raisonnement qu'une personne n'ayant pas encore atteint la maturité physique et psychologique a besoin d'une protection plus importante que les autres. Son objectif est d'améliorer les conditions pour l'enfant et de renforcer son droit au développement de sa propre personnalité. Ce principe doit être respecté par toutes les entités, publiques ou privées, qui prennent des décisions relatives aux enfants. Il s'applique également aux parents et aux autres représentants de l'enfant, lorsque leurs intérêts respectifs sont comparés ou lorsque l'enfant est représenté. Les représentants de l'enfant doivent appliquer ce principe en règle générale mais, en cas de conflit entre les intérêts de l'enfant et ceux de ses représentants, la décision revient au tribunal ou, le cas échéant, aux autorités chargées de la protection des données (DPA).

2) – Protection et soins nécessaires au bien-être des enfants

Le principe de l'intérêt supérieur de l'enfant exige une appréciation adéquate de sa situation. Cela implique la reconnaissance de deux éléments. Premièrement, l'immaturité de l'enfant le rend vulnérable, ce qui doit être compensé par une protection et des soins appropriés. Deuxièmement, l'enfant ne peut jouir de son droit au développement qu'avec l'assistance ou la protection d'autres entités et/ou personnes.[5]

Cette protection incombe à la famille, à la société et à l'État.

---

[3] - Lignes directrices de l'OCDE du 23 septembre 1980,
- Convention 108 du Conseil de l'Europe du 28 janvier 1981 et protocole additionnel du 8 novembre 2001,
- Principes directeurs des Nations unies du 14 décembre 1990.

[4] Inscrit dans la Convention des Nations unies relative aux droits de l'enfant (article 3), puis réaffirmé par la Convention 192 du Conseil de l'Europe (article 6) et la Charte des droits fondamentaux de l'Union européenne (article 24, paragraphe 2).

[5] Le droit à la protection est si fondamental qu'il est inscrit dans la Déclaration universelle des droits de l'homme (article 25) et a été confirmé dans le Pacte international relatif aux droits civils et politiques (article 24), dans le Pacte international relatif aux droits économiques, sociaux et culturels (article 10, paragraphe 3) et, plus récemment, dans la Charte des droits fondamentaux de l'Union européenne (article 24).

L'on doit admettre que, pour garantir aux enfants le niveau de soins dont ils ont besoin, leurs données à caractère personnel devront parfois être traitées très largement et par plusieurs personnes. C'est principalement le cas dans les domaines sociaux : l'éducation, la sécurité sociale, la santé, etc. Ce n'est toutefois pas incompatible avec la protection adéquate et renforcée des données dans ces secteurs, même s'il convient d'être prudent lorsque l'on partage des données concernant les enfants. Ce partage peut faire perdre de vue le principe de finalité (limitation de la finalité) et créer le risque que des profils soient créés sans tenir compte du principe de proportionnalité.

3) – Droit au respect de la vie privée

En tant qu'être humain, l'enfant a droit au respect de sa vie privée.

L'article 16 de la Convention des Nations unies relative aux droits de l'enfant prévoit que nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.[6]

Toute personne, y compris les représentants de l'enfant, est tenue de respecter ce droit.

4) – Représentation

Les enfants ont besoin de représentants légaux pour exercer la plupart de leurs droits. Cela ne signifie pas pour autant que le statut de représentant prime de manière absolue ou inconditionnelle sur celui de l'enfant. En effet, l'intérêt supérieur de l'enfant peut parfois lui conférer des droits relatifs à la protection des données susceptibles de dépasser les souhaits de ses parents ou représentants. De même, l'obligation de représentation n'implique pas que l'enfant ne doit pas être consulté, à partir d'un certain âge, sur les sujets le concernant.

Si le représentant d'un enfant consent au traitement des données concernant celui-ci, l'enfant pourra, à sa majorité, revenir sur ce consentement. En revanche, s'il souhaite la poursuite du traitement de ses données, il doit donner son consentement explicite, si nécessaire.

Par exemple, si un représentant a donné son consentement explicite à la participation de son enfant à une étude clinique, le responsable du traitement des données devra s'assurer, à la majorité de la personne concernée, d'avoir une base valable pour poursuivre le traitement des données à caractère personnel de celle-ci. Le responsable doit en particulier obtenir le consentement explicite de la personne concernée afin de poursuivre l'étude, car des données sensibles sont en jeu.

À ce sujet, il convient de rappeler que le droit à la protection des données appartient à l'enfant et non à ses représentants, qui ne font que l'exercer.

---

[6] Ce droit est une confirmation du droit général au respect de la vie privée, inscrit à l'article 12 de la Déclaration universelle, à l'article 17 du Pacte international relatif aux droits civils et politiques et à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme.

5) – Intérêts concurrents : respect de la vie privée et intérêt supérieur de l'enfant

Le principe de l'intérêt supérieur peut jouer un double rôle. A priori, ce principe exige que la vie privée de l'enfant soit protégée le mieux possible, en donnant le plus large effet possible au droit à la protection des données de l'enfant. Cependant, dans certaines situations, l'intérêt supérieur de l'enfant et son droit au respect de la vie privée entrent en conflit. Dans ce cas, le principe de l'intérêt supérieur peut prévaloir sur le droit à la protection des données. C'est notamment le cas dans le domaine médical où, par exemple, les services d'aide sociale à la jeunesse peuvent exiger des informations pertinentes dans les affaires de négligence ou d'abus. De même, un enseignant peut révéler des données à caractère personnel à un assistant social afin de protéger un enfant physiquement ou psychologiquement.

Dans des cas extrêmes, le principe de l'intérêt supérieur peut également entrer en conflit avec l'obligation d'obtenir le consentement des représentants. Dans ce cas, l'intérêt supérieur de l'enfant doit également être privilégié, par exemple lorsque son intégrité mentale ou physique est en jeu.

6) – Adaptation au degré de maturité de l'enfant

Dans la mesure où l'enfant est une personne en développement, l'exercice de ses droits, y compris ceux relatifs à la protection des données, doit être adapté à son niveau de développement physique et psychologique. Non seulement les enfants sont en développement, mais ils ont droit à ce développement.[7] Les systèmes juridiques gèrent ce processus différemment d'un État à l'autre mais, dans toute société, les enfants devraient être traités en fonction de leur degré de maturité.[8]

Quant au consentement, il peut s'agir d'une simple consultation de l'enfant, d'un consentement parallèle de l'enfant et du représentant, voire du seul consentement de l'enfant, en fonction de son degré de maturité.

7) – Droit d'être consulté

Les enfants acquièrent progressivement la capacité de contribuer aux décisions qui les concernent. En grandissant, ils doivent être consultés plus régulièrement sur l'exercice de leurs droits, y compris ceux relatifs à la protection des données.[9]

Ce devoir de consultation consiste à prendre en compte les opinions de l'enfant, sans nécessairement s'y conformer.[10] Le droit d'être consulté s'applique à différents domaines, comme la géolocalisation, l'usage des images de l'enfant, etc.

---

7 Convention des Nations unies relative aux droits de l'enfant – articles 27 et 29.

8 Certains systèmes juridiques appliquent ce principe général en distinguant les périodes suivantes : avant 12 ans, entre 12 et 16 ans, et de 16 à 18 ans.

9 Convention des Nations unies relative aux droits de l'enfant (article 12), Charte des droits fondamentaux de l'Union européenne (article 24, paragraphe 1), Convention sur les relations personnelles concernant les enfants (article 6).

B – Dans la perspective de la protection des données

1) – Champ d'application du cadre juridique existant en matière de protection des données

Les directives relatives à la protection des données, à savoir les directives 95/46/CE et 2002/58/CE, ne mentionnent pas explicitement le droit au respect de la vie privée des mineurs. Ces instruments juridiques s'appliquent à toute personne physique mais aucune disposition particulière n'est prévue concernant les questions spécifiques aux enfants. Cela ne signifie pas pour autant que les enfants n'ont pas droit au respect de la vie privée et qu'ils ne relèvent pas desdites directives. D'après la formulation des directives, elles s'appliquent à toute « personne physique » et comprennent par conséquent les enfants.

Eu égard au champ d'application personnel et matériel limité de la directive, un certain nombre de questions relatives à la protection de la vie privée des enfants dans le cadre de la directive subsiste. En effet, la plupart des dispositions ne tient pas directement compte des particularités de la vie des enfants. Le degré de maturité individuelle d'un enfant, ainsi que l'obligation de représentation pour les actes juridiques, posent des problèmes.

La nécessité de protéger les données de l'enfant doit prendre en compte deux aspects importants : d'une part, les différents degrés de maturité déterminant quand l'enfant peut commencer à gérer ses données à caractère personnel et, d'autre part, la mesure dans laquelle les représentants ont le droit de représenter le mineur lorsque la révélation des données à caractère personnel risque de porter préjudice à l'intérêt supérieur de l'enfant. Le point suivant traitera de la meilleure manière d'appliquer les règles existantes de la directive pour garantir la protection adéquate et efficace de la vie privée des enfants.

2) – Principes de la directive 95/46/CE

a) <u>Qualité des données</u>

Les principes généraux relatifs à la qualité des données prévus dans la directive 95/46/CE doivent être adaptés de manière adéquate aux enfants.
Cela signifie :

a.1) <u>Loyauté</u>

L'obligation de traiter les données à caractère personnel conformément au principe de loyauté (article 6, point a)) doit être interprétée strictement lorsqu'un enfant est concerné. Dans la mesure où un enfant n'est pas encore complètement mûr, les responsables du traitement doivent en avoir conscience et agir en toute bonne foi lors du traitement de ses données.

---

[10] Ce critère est clairement indiqué dans la Recommandation du Comité des ministres du Conseil de l'Europe relative à la protection des données médicales – Rec. nº R (97) 5 du 13 février 1997, paragraphes 5.5 et 6.3.

a.2) Proportionnalité et pertinence des données

Le principe fixé à l'article 6, point c), de la directive 95/46/CE dispose que seules les données adéquates, pertinentes et non excessives peuvent être collectées et traitées.

En appliquant les principes de l'article 6, point c), les responsables du traitement doivent accorder une attention particulière à la situation de l'enfant car ils doivent toujours respecter son intérêt supérieur.

Aux termes de l'article 6, point d), de la directive 95/46/CE, les données doivent être « exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ».

L'enfant étant en évolution constante, les responsables du traitement des données devront être particulièrement attentifs à l'obligation de mise à jour des données à caractère personnel.

a.3) Conservation des données

À cet égard, il convient de garder à l'esprit le « *droit à l'oubli* » qui protège toute personne concernée, et *particulièrement* les enfants. L'article 6, point e), de la directive doit être appliqué en conséquence.

Dans la mesure où les enfants sont en développement, leurs données changent et peuvent être rapidement dépassées et non pertinentes pour l'objectif initial de la collecte de données. Dans ce cas, les données ne devraient pas être conservées.

b) Légitimité

La directive 95/46/CE fixe les principes fondamentaux de la protection des données que les États membres doivent respecter et mettre en œuvre. S'agissant du droit au respect de la vie privée des enfants, les articles 7 et 8 revêtent une importance majeure car ils fixent les critères légitimant le traitement des données.

Avant tout, le traitement est autorisé si la personne concernée a donné son consentement sans ambiguïté. La définition du terme « consentement » est précisée à l'article 2, point h), de la directive.

En d'autres termes, le consentement doit être éclairé et libre. Le consentement n'est cependant pas obligatoire dans tous les cas. En effet, le traitement peut être légitime si d'autres exigences légales sont remplies conformément à l'article 7, points b) à f). Ainsi, le traitement peut être autorisé lors de la signature d'un contrat.

Si les représentants portent atteinte à la vie privée de l'enfant en vendant ou en publiant ses données, la question se pose alors de savoir comment protéger le droit au respect de la vie privée si l'enfant concerné n'est pas conscient de ces atteintes. Les enfants ont

besoin d'un tuteur légal mais, dans un cas comme celui-ci, ne peuvent exercer leurs droits. Si les enfants sont suffisamment mûrs pour déceler une atteinte à leur droit au respect de la vie privée, ils ont le droit d'être entendus par les autorités compétentes, y compris les autorités chargées de la protection des données.

Concernant les autres conditions de l'article 7 de la directive qui légitiment le traitement des données, les principes de l'intérêt supérieur de l'enfant et de la représentation doivent également être respectés. Ainsi, à partir d'un certain âge, les enfants ont la capacité juridique de s'engager contractuellement, par exemple dans le domaine de l'emploi. Or, ces contrats ne sont valables qu'avec le consentement des représentants. Préalablement à la conclusion d'un contrat ou pendant son exécution, l'autre partie peut vouloir collecter des données sur l'enfant en tant qu'employé.

Les représentants facilitent le traitement des données en donnant leur consentement. Les parents ou les tuteurs doivent prendre les décisions en se fondant sur l'intérêt supérieur de l'enfant. Ils doivent prendre en considération la menace que peut constituer la révélation des données pour la vie privée de l'enfant et ses intérêts vitaux, par exemple en ne révélant pas ses données médicales. Il existe d'autres domaines dans lesquels même les enfants sont autorisés à prendre des décisions indépendamment de leurs représentants.

En ce qui concerne la condition précisée à l'article 7, point e), il convient de noter que le principe de l'intérêt supérieur de l'enfant peut également être considéré comme un intérêt public. Cela peut être le cas lorsque les services d'aide sociale à la jeunesse ont besoin des données à caractère personnel d'un enfant pour s'occuper de lui. Les dispositions de la directive s'appliquent alors directement à ces circonstances.

Cependant, la question se pose de savoir si les enfants habilités à conclure, dans certains cas, des actes juridiques sans le consentement de leurs représentants (dans les cas où ils jouissent de droits partiels) peuvent également donner un consentement valable au traitement de leurs données.

Selon les réglementations locales en vigueur, cela peut être le cas du mariage, de l'emploi, des questions religieuses, etc. Dans d'autres cas, le consentement de l'enfant peut être valable, à condition que le représentant ne s'y oppose pas. Il est également clair que le degré de maturité physique et psychologique de l'enfant doit être pris en compte et qu'à partir d'un certain âge, il est en mesure de prendre des décisions le concernant. Cela peut être important dans le cas où le représentant est en désaccord avec l'enfant, mais où celui-ci est suffisamment mûr pour prendre des décisions dans son propre intérêt, pour des questions d'ordre médical ou sexuel par exemple. Les cas où l'intérêt supérieur de l'enfant limite ou même prévaut sur le principe de représentation ne doivent pas être négligés et devraient être approfondis.

Le motif le plus large autorisant le traitement des données concerne l'intérêt légitime poursuivi par le responsable du traitement ou par un tiers (article 7, point f)), à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée. En évaluant la situation, il faut particulièrement prendre en compte le statut de l'enfant dont les données font l'objet d'un traitement, en gardant à l'esprit son intérêt supérieur.

c) Sécurité des données

L'article 17 de la directive 95/46/CE dispose « *Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés* » et précise que :

« *Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger* ».

Les responsables du traitement et les sous-traitants doivent être conscients que les données relatives aux enfants exigent un niveau élevé de protection.

d) Droits de la personne concernée

d.1) Droit d'être informée

Il convient de noter que l'exigence de consentement dans le cadre de la directive est indissociable de l'obligation d'informer de manière adéquate la personne concernée (articles 10, 11 et 14).

Le groupe de travail a déjà abordé l'obligation d'information dans plusieurs documents. L'avis sur les « Dispositions davantage harmonisées en matière d'informations » (WP 100) et la « Recommandation concernant certaines exigences minimales pour la collecte en ligne de données à caractère personnel dans l'Union européenne » (WP 43) devraient particulièrement être pris en compte, dans la mesure où ces documents fournissent des orientations claires à ce sujet.

Pour informer les enfants, priorité doit être donnée aux messages structurés, rédigés dans un langage simple, concis et pédagogique facilement compréhensible. Un message court doit contenir les informations de base à fournir lors de la collecte des données à caractère personnel soit auprès de la personne concernée soit auprès d'un tiers (articles 10 et 11). Ce message doit être accompagné d'informations plus détaillées, éventuellement accessibles grâce à un lien hypertexte, où tous les détails pertinents sont fournis. Comme le groupe de travail l'avait souligné dans sa recommandation sur le traitement en ligne de données, il est essentiel de publier les informations à l'endroit et au moment appropriés, c'est-à-dire directement sur l'écran, préalablement à la collecte de données. Outre le fait qu'elle est exigée par la directive, cette mesure est particulièrement importante pour sensibiliser les enfants aux risques et dangers potentiels des activités en ligne. En effet, on peut affirmer que, dans l'environnement virtuel, contrairement au monde réel, il s'agit de la seule occasion pour l'enfant d'être informé de ces dangers.

d.2) Droit d'accès

Le droit d'accès est, en principe, exercé par le représentant de l'enfant, mais toujours dans l'intérêt de ce dernier. En fonction du degré de maturité de l'enfant, ce droit peut être exercé à sa place ou avec lui. Dans certains cas, l'enfant peut aussi être autorisé à exercer seul son droit d'accès.

Lorsque des droits très personnels sont en jeu (par exemple dans le domaine de la santé), l'enfant peut même demander à son médecin de ne pas révéler ses données médicales à son représentant.

Cela peut être le cas lorsqu'un adolescent donne des informations d'ordre sexuel à un médecin ou à une ligne d'assistance téléphonique, excluant explicitement ses représentants de ces informations.

Cela peut également être le cas lorsqu'un enfant ne fait pas confiance à son représentant et contacte les services d'aide sociale à la jeunesse, par exemple s'il est toxicomane ou a des tendances suicidaires.

La question se pose de savoir si les représentants peuvent avoir accès à ces détails et si l'enfant peut s'y opposer. Pour déterminer si le droit au respect de la vie privée de l'enfant prévaut sur le droit d'accès des représentants, les intérêts de toutes les parties concernées doivent être attentivement pesés. Lors de l'évaluation, l'intérêt supérieur de l'enfant revêt une importance particulière.

Dans le cas de l'accès aux données médicales, l'appréciation du médecin peut être utile pour évaluer s'il est opportun que les représentants aient accès aux données.

Les pratiques nationales peuvent également constituer des exemples utiles : au Royaume-Uni, les adolescents de plus de 12 ans sont autorisés à exercer seuls leur droit d'accès.

Dans plusieurs pays, le droit d'accès des représentants aux données de leur fille adolescente est limité en cas d'avortement.

D'une manière générale, les critères fixant les conditions d'accès aux données ne relèvent pas uniquement de l'âge de l'enfant, mais également de son degré de maturité et d'autonomie. Par exemple, savoir qui a fourni les données, les parents ou l'enfant, peut donner une indication sur ce point.

d.3) Droit d'opposition

L'article 14, point a), dispose que la personne concernée a le droit de s'opposer au traitement de ses données, au moins dans les cas visés à l'article 7, points e) et f), pour des raisons prépondérantes et légitimes. S'agissant d'enfants, ces raisons peuvent être particulièrement prépondérantes. Il convient également de rappeler que la personne concernée est autorisée, dans tous les cas, à s'opposer au traitement de ses données à des fins de prospection (article 14, point b)).

III – À l'école

Dans cette section, le présent avis s'attachera à montrer comment les principes fondamentaux rappelés ci-dessus peuvent être précisés dans le contexte scolaire. En effet, la vie d'un enfant se déroule autant à l'école qu'au sein de sa famille. Il est donc naturel que plusieurs questions relatives à la protection des données se posent dans le cadre de la vie scolaire des enfants. De nature très diverse, ces questions soulèvent différents problèmes.

1) – Dossiers scolaires

a) Information

Les questions relatives à la protection des données des enfants (et parfois de leur famille) peuvent se poser au sujet du dossier scolaire dès l'inscription à l'école. En effet, dans certains pays, la législation autorise les autorités scolaires à demander de compléter des formulaires contenant des données à caractère personnel afin de constituer un dossier scolaire, informatisé ou conservé sur d'autres supports.

Sur ce type de formulaires, la personne concernée doit être informée de la collecte et du traitement de ses données à caractère personnel, ainsi que des éléments suivants : la finalité, les responsables du traitement et les modalités d'exercice de son droit d'accès et de rectification sur ses données. Si ses données sont communiquées à un tiers, elle doit également en être informée.

b) Proportionnalité

Les données demandées ne doivent pas être excessives. Par exemple, les données concernant les diplômes universitaires des parents, leur profession ou leur situation d'emploi ne sont pas toujours nécessaires. Les responsables des données doivent évaluer si elles sont réellement nécessaires. Il convient d'être particulièrement attentif car ces informations peuvent être à l'origine de discriminations.

c) Non-discrimination

Certaines données contenues dans ces formulaires peuvent être à l'origine de discriminations, notamment les données relatives à la race, à la situation d'immigré ou à certains handicaps.

Ces informations sont généralement collectées pour s'assurer que l'école est sensibilisée et consacre l'attention nécessaire aux élèves rencontrant des difficultés culturelles (par exemple d'ordre linguistique) ou économiques.

Les principes d'intérêt supérieur et de limitation de la finalité doivent être les critères retenus lors du traitement de ces informations.

Une approche très stricte doit être adoptée concernant l'inscription de la religion des élèves. Celle-ci n'est acceptable que lorsque la nature (école religieuse) et l'objectif administratif le justifient, et uniquement dans la mesure strictement nécessaire. Aucune déduction superflue sur la religion de l'élève ne doit être tirée lorsque les données sont

uniquement nécessaires à des fins administratives (par exemple, la participation à un cours de religion ou l'indication des préférences alimentaires).

Les informations sur le patrimoine et les revenus de la famille d'un enfant peuvent également être à l'origine de discriminations, mais peuvent être traitées dans l'intérêt de l'enfant, par exemple si les représentants demandent une bourse ou une réduction des frais de scolarité.

Toutes les données susceptibles d'entraîner une discrimination doivent être protégées par des mesures de sécurité appropriées, comme le traitement dans des dossiers distincts par du personnel qualifié et attitré, soumis au secret professionnel, et d'autres mesures adéquates.

Le consentement au traitement de toutes les données susceptibles d'entraîner une discrimination doit être clair et explicite.

d) Principe de finalité

d.1) Communication des données

Dans certains cas, les autorités scolaires fournissent le nom et l'adresse de leurs élèves à des tiers, très souvent à des fins de prospection.

C'est notamment le cas lorsque les données sont transmises à des banques ou des compagnies d'assurance souhaitant attirer des élèves dans leur clientèle ou lorsque des données scolaires sont communiquées aux élus locaux. Cela constitue une atteinte au principe de finalité, dans la mesure où les données fournies à des fins scolaires sont utilisées de manière incompatible avec ces finalités.

Conformément à l'article 6, paragraphe 1, point b), de la directive 95/46/CE, les données relatives aux enfants ne peuvent pas être traitées ultérieurement de manière incompatible avec les finalités qui justifient leur collecte.

La question ici n'est pas que les enfants soient la cible d'une prospection, ce qui relève de la protection des consommateurs. Le problème est la collecte préalable de données à caractère personnel afin d'envoyer ultérieurement des messages de prospection aux personnes concernées. Ce traitement doit toujours être soumis au consentement préalable des représentants (et de l'enfant, en fonction de son degré de maturité).

Dans tous les cas où une opération de prospection est considérée comme légitime et compatible, ce traitement doit toujours être effectué de la manière la moins intrusive possible.

Outre les conditions mentionnées ci-dessus, si des données sur les parents et/ou les élèves sont demandées par un tiers à des fins de prospection, leur transmission doit toujours être soumise à l'information et au consentement préalables des représentants (et de l'enfant, en fonction de son degré de maturité).

d.2) Accès aux données

Les données contenues dans le dossier scolaire sont soumises à une stricte confidentialité, conformément au principe général énoncé à l'article 16 de la directive 95/46/CE.

Le traitement des données d'une nature particulière est soumis à des exigences spécifiques de sécurité.

La liste ci-dessous fournit des exemples de ce type de données :

- procédures disciplinaires,
- consignation de cas de violence,
- traitement médical à l'école,
- orientation scolaire,
- enseignement spécialisé pour les personnes handicapées,
- assistance sociale pour les élèves défavorisés.

Les représentants de l'élève (et l'élève lui-même, en fonction de son degré de maturité) doivent avoir accès aux données. Cet accès doit être strictement réglementé et limité aux autorités scolaires, aux inspecteurs, au personnel de santé et aux services répressifs.

d.3) Résultats scolaires

Selon les pays, les traditions diffèrent quant à la publication des résultats scolaires. Dans certains pays, publier les résultats est une tradition établie de longue date.

Elle a pour objectif de permettre la comparaison des résultats et de faciliter les éventuelles plaintes ou recours.

Dans d'autres pays, même les résultats sont soumis à la règle générale de la confidentialité applicable aux données contenues dans le dossier scolaire. Dans ces cas, les résultats peuvent être révélés aux représentants de l'élève exerçant leur droit d'accès.

D'une manière générale, les résultats ne devraient être publiés que lorsque c'est nécessaire et seulement après avoir informé les élèves et leurs représentants des objectifs de la publication et de leur droit d'opposition.

Un problème particulier se pose avec la publication des résultats scolaires sur l'internet, qui représente un moyen pratique de les communiquer aux personnes concernées. Les risques inhérents à ce mode de communication exigent que l'accès à ces données soit protégé par des garanties spécifiques, par exemple un site internet sécurisé ou l'attribution de mots de passe personnels aux représentants ou à l'enfant, en fonction de son degré de maturité.

Les modalités du droit d'accès sont différentes en fonction du degré de maturité de l'enfant. Selon toute probabilité, à l'école primaire, l'accès sera principalement exercé par les représentants, tandis qu'à l'école secondaire, les élèves pourront également accéder à leurs données.

d.4) Conservation et suppression

Le principe général selon lequel aucune donnée ne doit être conservée plus longtemps qu'il n'est nécessaire aux finalités de la collecte s'applique également dans ce contexte. Dès lors, une attention particulière doit être portée aux données des dossiers scolaires à conserver pour des raisons pédagogiques ou professionnelles, et à celles à supprimer, par exemple celles concernant les procédures et les sanctions disciplinaires.

2) – Vie scolaire

Des questions relatives à la protection des données dans le cadre de la vie scolaire se posent dans les domaines suivants.

a) Données biométriques – accès à l'école et à la cantine

Ces dernières années ont été marquées par une augmentation des contrôles d'accès aux écoles pour des raisons évidentes de sécurité. Ces contrôles d'accès impliquent la collecte, à l'entrée, de données biométriques, comme les empreintes digitales, l'iris ou le contour de la main. Or, dans certaines situations, de tels moyens sont disproportionnés par rapport à l'objectif et ont des effets excessivement intrusifs.

D'une manière générale, le principe de proportionnalité doit également être appliqué à l'utilisation de ces éléments biométriques.

Il est vivement recommandé de permettre aux représentants légaux de s'opposer facilement à l'utilisation des données biométriques de leur enfant. S'ils exercent ce droit, l'enfant devrait recevoir une carte ou un autre moyen d'accès aux locaux de l'école.

b) Télévision en circuit fermé (CCTV)

Les écoles ont de plus en plus tendance à recourir à la télévision en circuit fermé pour des raisons de sécurité. Il n'existe pas de solution recommandée convenant à tous les aspects de la vie scolaire et à tous les lieux d'une école.

Dans la mesure où la télévision en circuit fermé peut porter atteinte aux libertés individuelles, son installation dans les écoles exige une attention particulière. Elle ne sera installée que si nécessaire et s'il n'existe pas d'autres moyens moins intrusifs donnant le même résultat. La décision d'installer un système de télévision en circuit fermé doit être précédée d'une discussion approfondie entre les enseignants, les parents et les représentants des élèves, en prenant en compte les objectifs affichés de cette installation et l'adéquation des systèmes proposés.

À certains endroits, la sécurité revêt une importance primordiale. La télévision en circuit fermé se justifie alors plus facilement, par exemple à l'entrée et à la sortie des écoles, ainsi que dans d'autres lieux de passage, pas uniquement du personnel scolaire, mais également d'autres personnes visitant les locaux de l'école pour quelque raison que ce soit.

Le choix de l'emplacement des caméras de télévision en circuit fermé doit toujours être pertinent, adéquat et non excessif par rapport à la finalité du traitement. Dans certains pays, par exemple, le recours à des caméras de télévision en circuit fermé en dehors des horaires scolaires a été considéré comme adéquat au regard des principes de la protection des données.

En revanche, dans la plupart des autres endroits de l'école, le droit des élèves au respect de la vie privée (ainsi que celui des enseignants et de l'ensemble du personnel scolaire) et la liberté fondamentale d'enseignement mettent en question la nécessité d'une surveillance permanente par la télévision en circuit fermé.

C'est particulièrement le cas dans les salles de classe, où la vidéosurveillance peut entraver non seulement la liberté d'apprentissage et de parole des étudiants, mais également la liberté d'enseignement. Cela s'applique également dans les espaces de loisirs, les gymnases et les vestiaires, où la surveillance peut porter atteinte au droit au respect de la vie privée.

Ces remarques sont également fondées sur le droit de tous les enfants au développement de leur personnalité. En effet, la conception qu'ils se forgent progressivement de leur propre liberté peut être faussée s'ils supposent, dès le plus jeune âge, qu'il est normal d'être surveillé par télévision en circuit fermé. C'est d'autant plus vrai si des webcams ou des dispositifs similaires sont utilisés pour surveiller les enfants à distance pendant les horaires scolaires.

Dans tous les cas où la télévision en circuit fermé est justifiée, les enfants, le reste de la population scolaire et les représentants doivent tous être informés de l'existence de cette surveillance, des personnes qui en sont responsables et de ses objectifs. L'information destinée aux enfants doit être appropriée à leur niveau de compréhension.

La justification et la pertinence d'un système de télévision en circuit fermé doivent être revues régulièrement par les autorités scolaires pour décider s'il doit être maintenu. Les représentants des enfants doivent en être informés.

c) <u>État de santé</u>

Les données sur l'état de santé des élèves sont des données sensibles. Pour cette raison, leur traitement doit respecter strictement les principes de l'article 8 de la directive. Ces données doivent être traitées uniquement par des médecins ou par les personnes qui « prennent soin » directement des élèves, comme les enseignants et les autres membres du personnel scolaire liés au secret par l'éthique du secret professionnel.

Le traitement des données de ce type dépend du consentement des représentants de l'enfant ou de ses intérêts vitaux en cas d'urgence liée à la vie scolaire ou éducative.

d) Sites internet des écoles

De plus en plus d'écoles créent leur site internet pour les étudiants/élèves et leur famille. Ces sites deviennent le principal outil pour les communications externes. Les écoles doivent avoir conscience que la diffusion d'informations personnelles demande un respect plus strict des principes fondamentaux de la protection des données, notamment la minimisation des données et la proportionnalité. De plus, il est recommandé de mettre en place des systèmes de contrôle d'accès afin de protéger les informations personnelles (par exemple grâce à un identifiant utilisateur et un mot de passe).

e) Photos

Les écoles sont souvent tentées de publier (dans la presse ou sur l'internet) des photos de leurs élèves. Elles doivent être mises en garde au sujet de cette publication sur l'internet. Il s'agira de toujours évaluer le type de photo, la pertinence de la mise en ligne et l'objectif visé. Les enfants et leurs représentants doivent être informés de la publication et le consentement préalable des représentants (ou de l'enfant, en fonction de son degré de maturité) doit être obtenu.

Des dérogations sont admissibles pour les photos collectives, notamment de manifestations scolaires si, par nature, elles ne permettent pas l'identification facile des élèves.

f) Cartes scolaires

Pour le contrôle de l'accès et la surveillance des achats : de nombreuses écoles utilisent des cartes scolaires non seulement pour contrôler l'accès à l'école, mais également pour surveiller les achats des enfants. On peut se demander si le second objectif est entièrement compatible avec le respect de la vie privée de l'enfant, particulièrement à partir d'un certain âge.

Quoi qu'il en soit, ces deux fonctions doivent être distinctes, la seconde étant susceptible de soulever des questions relatives au respect de la vie privée.

Pour la localisation des élèves[11]: une autre méthode de surveillance utilisée dans certaines écoles (par carte ou non) est la localisation des élèves par l'intermédiaire de badges IRF. Dans ce cas, la pertinence d'un tel système doit être justifiée au regard des risques spécifiques en jeu, particulièrement lorsque d'autres méthodes de surveillance existent.

[11] Cf. WP 115 (adopté le 25 novembre 2005) sur les principes relatifs à la localisation des mineurs.

g) Visiophones à l'école

Les écoles peuvent jouer un rôle déterminant dans la mise en place de mesures de précaution quant à l'usage de MMS et d'enregistrements audio et vidéo, qui impliquent des données à caractère personnel de tiers, sans que la personne concernée en soit consciente. Les écoles doivent avertir leurs étudiants que la circulation illimitée d'enregistrements vidéo ou audio et d'images numériques peut entraîner de graves violations du droit au respect de la vie privée de la personne concernée et à la protection des données à caractère personnel.

3) – Statistiques scolaires et autres études

Les données à caractère personnel ne sont généralement pas nécessaires à l'établissement de statistiques (néanmoins, cela peut exceptionnellement être le cas, par exemple pour des statistiques sur l'intégration professionnelle).

Conformément à l'article 6, point e), de la directive, les résultats statistiques ne doivent pas permettre l'identification des personnes concernées directement ou indirectement.

Les études menées utilisent souvent diverses données à caractère personnel des élèves, obtenues par des questionnaires plus ou moins détaillés. La collecte de ces données doit être autorisée par les représentants (en particulier s'il s'agit de données sensibles) et les représentants doivent être informés de l'objectif et des destinataires de l'étude.

En outre, lorsqu'il est possible d'effectuer ces études sans identifier les enfants, cette procédure doit toujours être privilégiée.

IV – Conclusion

1) La législation

Le présent avis montre que, dans la plupart des cas, les dispositions fixées dans le cadre juridique actuel protègent efficacement les données relatives aux enfants.

L'application desdites dispositions conformément au principe de l'intérêt supérieur de l'enfant est cependant une condition préalable à la bonne protection de la vie privée des enfants. À cet effet, il convient de prendre en compte la situation particulière des mineurs et celle de leurs représentants. Les directives 95/46/CE et 2002/58/CE doivent être interprétées et appliquées en conséquence.

En cas de conflit d'intérêts, la solution pourra être recherchée dans l'interprétation des directives conformément aux principes généraux de la Convention des Nations unies relative aux droits de l'enfant, à savoir l'intérêt supérieur de l'enfant, ainsi que dans les autres instruments juridiques déjà mentionnés.

Les États membres sont encouragés à aligner leur législation sur l'interprétation mentionnée ci-dessus, en prenant les mesures nécessaires. D'autre part, au niveau

communautaire, des recommandations ou d'autres instruments appropriés sur ce sujet seraient souhaitables.

Comme indiqué précédemment, le présent avis aborde uniquement les principes généraux pertinents pour la protection de la vie privée et des données des enfants, et leur application au domaine essentiel de l'éducation. D'autres domaines spécifiques pourraient justifier à l'avenir des études distinctes du groupe de travail.

2) La pratique

Le présent avis expose les préoccupations et considérations générales que suscitent la protection des données et de la vie privée en ce qui concerne les enfants. Le groupe de travail a choisi le domaine de l'éducation comme première étape pour aborder cette question en raison de l'importance que revêt l'éducation dans la société. Comme on peut le constater, l'approche retenue pour protéger la vie privée des enfants est fondée sur l'éducation – assurée par la famille, l'école, les autorités chargées de la protection des données, les groupes d'enfants, etc. –, concernant l'importance de la protection des données et de la vie privée, et les conséquences de la révélation des données à caractère personnel lorsque ce n'est pas nécessaire.

Si nos sociétés veulent créer une véritable culture de la protection des données, en particulier, et de la vie privée, en général, il convient de commencer par les enfants, non seulement parce qu'ils constituent une catégorie de personnes nécessitant une protection ou parce qu'ils sont titulaires de droits à la protection, mais également parce qu'ils doivent être informés de leur devoir de respecter les données à caractère personnel des autres.

Afin d'atteindre cet objectif, l'école doit jouer un rôle central.

Les enfants et les élèves doivent être éduqués de façon à devenir des citoyens autonomes dans la société de l'information. À cet effet, il est fondamental qu'ils apprennent dès leur plus jeune âge l'importance du respect de la vie privée et de la protection des données. Ces notions leur permettront par la suite de prendre des décisions en connaissance de cause sur les informations qu'ils souhaitent divulguer, à qui et dans quelles conditions. La protection des données doit être systématiquement intégrée dans les programmes scolaires, en fonction de l'âge des élèves et de la nature des matières enseignées.

Il ne devrait jamais arriver que, pour des raisons de sécurité, les enfants soient confrontés à une surveillance excessive limitant leur autonomie. Dans ce contexte, un équilibre doit être trouvé entre la protection de l'intimité et de la vie privée des enfants, et leur sécurité.

Les législateurs, les dirigeants politiques et les organismes éducatifs doivent, dans le cadre de leurs domaines de compétence respectifs, prendre des mesures efficaces pour résoudre ces questions.

Le rôle des autorités chargées de la protection des données repose sur quatre axes : éduquer et informer, particulièrement les enfants et les autorités responsables du bien-être des jeunes ; amener les décideurs politiques à prendre les bonnes décisions concernant les enfants et la vie privée ; sensibiliser les responsables du traitement des données à leurs devoirs ; exercer leurs pouvoirs à l'encontre de ceux qui enfreignent la législation ou ne respectent pas les codes de conduite ou les meilleures pratiques dans ce domaine.

Dans ce contexte, une stratégie efficace peut être la conclusion d'accords entre les autorités chargées de la protection des données, les ministères de l'éducation et les autres organismes responsables, définissant des conditions claires et concrètes de coopération mutuelle dans ce domaine afin de diffuser l'idée que la protection des données est un droit fondamental.

Il faut notamment apprendre aux enfants qu'il leur incombe d'être les principaux protecteurs de leurs données à caractère personnel. C'est là un domaine où l'efficacité de la responsabilisation peut être démontrée.

Consultation publique

Le groupe de travail « Article 29 » invite les personnes qui gèrent les données à caractère personnel des enfants, notamment les enseignants et les autorités scolaires, ainsi que les particuliers, à formuler des commentaires sur le présent document de travail.[12]

Fait à Bruxelles, le 18 février 2008

Pour le groupe de travail
Le Président
Peter SCHAAR

[12] Vous pouvez envoyer vos commentaires sur le présent document de travail au groupe de travail « Article 29 » - Secrétariat - Commission européenne, direction générale « Justice, liberté et sécurité »
Unité C.5 – Protection des données
Bureau : LX 46 6/80
B - 1049 Bruxelles
E-mail : Amanda.JOYCE-VENNARD@ec.europa.eu et Kalliopi.Mathioudaki-Kotsomyti@ec.europa.eu;
Fax : +32-2-299 80 94

Tous les commentaires des secteurs public et privé seront publiés sur le site internet du groupe de travail « Article 29 », à moins que les répondants n'indiquent explicitement que certaines informations doivent rester confidentielles.