Janvier 2004

Guide juridique de l'internet scolaire

AVANT-PROPOS

L'auteur tient à préciser que ce guide doit beaucoup à la réflexion menée depuis 1999 avec le Centre de Recherche en Droit Public (Université de Montréal) sur la régulation de l'Internet en général et l'élaboration de règles de conduite par les acteurs (co et autorégulation) en particulier.

Fruit de ces recherches, c'est ainsi que Pierre TRUDEL et France ABRAN, membres du CRDP avec qui l'auteur a collaboré, ont publié avec le soutien du Ministère de l'éducation du Québec et de la Direction générale de l'autoroute de l'information un « Guide pour gérer les aspects juridiques d'Internet en milieu scolaire »

http://www.crdp.umontreal.ca/

Le guide français suit la même démarche de responsabilisation des acteurs et de gestion des risques et emprunte un plan similaire.

Philippe AMBLARD oct. 2003

Introduction, démarche et objectifs

Ce guide est destiné à toutes les personnes, acteurs ou utilisateurs de l'Internet en milieu scolaire. Sous forme de fiches pratiques, il a pour ambition de les soutenir dans les écoles, collèges, lycées ou universités quant à la gestion des aspects juridiques liés à la mise en place ou au déroulement d'activités en ligne.

Aujourd'hui et plus encore demain, l'Internet se présente comme un outil pédagogique de premier ordre grâce aux facilités d'échanges et d'accès au savoir qu'il offre. Du courrier électronique au site web, tous les services en ligne sont potentiellement intéressants à utiliser pour l'apprentissage des connaissances. Ceci dit, cette facilité de création, d'échange ou de consultation de contenus ouvre de nouvelles perspectives à l'enseignement à la condition **de respecter les valeurs et principes du système éducatif.** Il ne serait question, sous prétexte de nouvelles capacités techniques, de bafouer les droits et intérêts des enseignants, des élèves ou des tiers. S'agissant de l'Internet, en particulier en milieu scolaire, **possible techniquement ne signifie pas préférable socialement, moralement et en définitive légalement.**
C'est pourquoi, à la demande du Ministère de l'éducation nationale, ce guide se propose de promouvoir une utilisation responsable de l'Internet afin de ne nuire à personne.
La démarche de ce guide débute d'un constat. Il ne suffit malheureusement pas de rappeler les lois et règlements en vigueur dans le milieu scolaire pour accomplir notre tâche. A l'école comme partout ailleurs, l'accès et l'usage de l'Internet ne se déroulent jamais dans un cadre normatif pleinement maîtrisé par l'État. Nous concernant, il faut toujours avoir à l'esprit que les aspects juridiques liés aux ressources en ligne dépassent largement l'espace contrôlé de l'école. L'Internet demeure un environnement international et complexe.
International dans le sens où selon sa définition strictement technique, il s'agit du «réseau d'interconnexion mondiale des réseaux informatiques».
Complexe dans la mesure où, comme nous le verrons tout au long du guide, de nombreux acteurs interagissent dans des contextes de communication variés.
Tirant les conséquences de cette réalité de l'Internet, la démarche de la présente série de fiches pratiques repose sur le principe que le concours de tous est donc indispensable pour réguler cet espace.
Se contenter de décréter des conditions d'utilisation «fourre- tout» standard est insuffisant pour prévenir tout risque lié à l'Internet. A l'inverse, créer un cadre sécuritaire où l'usage de l'Internet serait entravé par des conditions, des contrôles et des processus bureaucratiques trop sévères manquerait également son but. Les usagers seraient enclins à contourner des règles tatillonnes qui ne répondent pas à leurs attentes. Ainsi, plutôt que d'utiliser des services de communication censurés à l'excès, les élèves préféreront se connecter à des services commerciaux de messagerie électronique n'offrant pas toutes les garanties quant à la protection des mineurs mais permettant pourtant les échanges recherchés.
L'enjeu est donc de permettre à chacun de participer à l'élaboration d'un cadre normatif adapté aux besoins de tous. La démarche adoptée par ce guide est d'accompagner utilement toute personne concernée par l'Internet à l'école dans sa participation plus ou moins grande au respect des principes fondamentaux du monde académique.
L'important est de viser un usage informé et responsable plutôt qu'une réglementation caporaliste. L'objectif de ce guide est d'éclairer les acteurs et les utilisateurs de l'Internet sur leurs responsabilités respectives afin d'éliminer les risques qu'ils peuvent facilement maîtriser.

UN PROCESSUS EN TROIS PHASES

Même en milieu scolaire, de nombreux choix normatifs sont sous la maîtrise des acteurs et des utilisateurs de l'Internet. Ce guide entend donc les informer clairement afin qu'ils assument leurs justes responsabilités des risques liés à la mise en place ou à l'usage de services en ligne.
Au niveau des acteurs et des utilisateurs, des enseignants et des élèves, les aspects juridiques liés à l'Internet doivent être abordés suivant une approche de gestion des risques.
Garantes des valeurs de liberté et de respect de la personne humaine, les lois, en particulier celles relatives à l'éducation nationale, demeurent le cadre obligatoire des activités en ligne. Elles doivent toujours être respectées. Cependant leur caractère général n'indique aux internautes que les principes à suivre. Compte tenu de la variété des personnes comme des activités en jeu, il est impossible au législateur d'envisager toutes les situations à encadrer, en milieu scolaire comme ailleurs.
Au delà des principes légaux, incontournables mais insuffisants, il semble surtout opportun d'adopter une démarche préventive. Toute personne concernée doit prévoir les difficultés juridiques soulevées par la mise en place ou l'utilisation de services en ligne qu'elle permet, accueille, offre ou utilise en évaluant les risques. Autrement dit, pour encadrer des situations par nature spécifiques, il s'agit au préalable d'analyser les risques liés aux personnes comme aux activités afin de personnaliser les règles en vigueur. Ce guide accompagne donc les acteurs à prendre les mesures préventives propres à réduire les risques de se trouver en contravention avec la loi.
Le processus se déroule en trois phases qui découpent le guide en trois parties complémentaires et

autonomes à la fois :

1- L'étude des responsabilités distinctes des différentes personnes concernées

Premièrement, il faut identifier les personnes responsables de la mise en place ou de l'utilisation de l'Internet en milieu scolaire.
Qui fait quoi ou qui doit répondre de ce qui se passe lors des activités en ligne ?

2- La définition technique et pratique des différentes activités en ligne et de leurs risques spécifiques.

Deuxièmement, il faut définir les risques liés aux activités en ligne.
Quels types de services en ligne sont utilisés et quels risques les accompagnent ?

3- La prise en charge des risques par le choix d'une politique de prévention faisant intervenir l'ensemble des personnes responsables.

Troisièmement, il faut gérer ou prendre en charge les risques définis dans les limites des responsabilités identifiées par le choix d'une politique de prévention personnalisée.
Quel mode de régulation adopter, puis quels types de règles prendre ?
En définitive, comme le démontre la raison d'être de ce guide, il existe de nombreuses situations jugées à risque qui se résolvent plus efficacement au niveau des acteurs directement concernés. Eux seuls peuvent adapter la réponse normative à la juste mesure des risques réellement encourus.

Remarque
Enfin **ce guide ne constitue pas un traité de droit**. Malgré le soin apporté dans l'exactitude de l'information quant aux dispositions légales, celles-ci restent de portée trop générale pour pouvoir remplacer un avis juridique, seule réponse possible pour des cas particuliers

La responsabilité de l'État

Vis-à-vis des technologies de l'information en milieu scolaire, l'État assume des responsabilités de natures différentes :

- D'une part, **des responsabilités d'ordre politique et pédagogique au sens de prérogatives**. La responsabilité est ici synonyme de capacité de prendre des décisions sans en référer préalablement à une autorité supérieure.

- D'autre part, **des responsabilités d'ordre juridique au sens d'obligations**. La responsabilité signifie là l'obligation de réparer un préjudice résultant de son action ou de celle de ses agents.

1- Responsabilité d'ordre politique

La première des responsabilités de l'État est d'ordre **politique**. Le gouvernement et en premier lieu le ministre de l'éducation ont le pouvoir d'arbitrer les choix politiques en matière d'éducation et de fixer les grandes orientations. C'est à ce titre que depuis quelques années le Ministère de l'éducation nationale entend promouvoir le développement des technologies de l'information au sein des enceintes scolaires. Ainsi, dans le Bulletin officiel de l'éducation nationale n° 9 du 10 septembre 1998, la circulaire n° 98-171 du 2 septembre 1998 décrit le dispositif de soutien au développement des ressources multimédias et audiovisuelles pédagogiques. Le ministère se propose de soutenir financièrement la réalisation de produits électroniques utilisant toutes les potentialités offertes par l'Internet comme la mise à jour des informations, l'accès à des données distantes, le courrier électronique ou la maintenance en ligne. Plus récemment et plus généralement, les technologies de l'information et de la communication (TIC) sont l'objet du plan RE/SO 2007 pour une république numérique de la société de l'information, lancé par le Premier ministre le 12 novembre 2002.

2- Responsabilité d'ordre pédagogique

La seconde des responsabilités est d'ordre **pédagogique**. Il revient à l'administration de l'éducation de définir les programmes des différentes matières dans le cadre des objectifs et missions de l'enseignement

scolaire (art. L122-1 et s. du Code de l'éducation - CE ci-après).
Concernant spécifiquement l'utilisation de l'Internet, il faut mentionner l'existence du **brevet informatique et internet (B2i)** qui concerne les écoles primaires et les collèges. Comme le rappelle la note de service n° 2000-206 du 16 novembre 2000, « son rôle est de dispenser à chaque futur citoyen la formation qui, à terme, le mettra à même de faire des technologies de l'information et de la communication une utilisation raisonnée, de percevoir les possibilités et les limites des traitements informatisés, de faire preuve d'esprit critique face aux résultats de ces traitements, et d'identifier les contraintes juridiques et sociales dans lesquelles s'inscrivent ces utilisations ». Suivant cet esprit, l'élaboration de règles que ce guide propose d'accompagner prend une dimension éducative.

Il ne faut enfin pas oublier la répartition des compétences entre l'État et les collectivités publiques :

- art. L211-1 CE (compétence de l'Etat)

- art. L212-1 CE (compétence des communes)

- art. L213-1 CE (compétence des départements)

- art. L214-1 CE (compétence des régions)

En définitive, les projets d'utilisation de l'Internet en milieu scolaire ne peuvent s'envisager que soutenus matériellement par les collectivités locales pour mieux atteindre les objectifs fixés par les programmes scolaires.

Plus généralement, l'usage de l'Internet est préconisé pour permettre aux élèves d'acquérir une certaine autonomie dans l'acquisition des connaissances.

L'exemple type est l'organisation des enseignements de technologie et d'informatique prévu par l'article L312-9 du Code de l'éducation.

3- Responsabilités d'ordre juridique

Enfin, outre les responsabilités d'ordre politique et pédagogique, l'État assume également une **responsabilité juridique.**
Le droit français connaît 3 régimes distincts de responsabilité. Lors d'activités scolaires en ligne, l'État peut être appelé à réparer un éventuel préjudice au titre soit de la responsabilité administrative, soit de la responsabilité civile. Par contre, la responsabilité pénale reste supportée par son auteur.
Pourquoi trois régimes de responsabilité ? Parce que le préjudice peut résulter de trois situations différentes qui sont encadrées par le droit administratif, le droit civil ou le droit pénal.

Dans le cas de la **responsabilité administrative**, l'État est reconnu responsable lorsqu'une faute de service à l'origine du préjudice est prouvée. Une **faute de service** correspond au fait ou agissement résultant d'une «mauvaise organisation ou un fonctionnement défectueux du service public de l'enseignement» (TRIB. CONFL. 6 mars 1989), c'est-à-dire une faute fatale, anonyme, que n'importe quel fonctionnaire aurait commise dans les mêmes conditions. Bien que l'auteur de la faute soit l'agent public, l'État est responsable car la faute est inséparable du service public de l'éducation. C'est pourquoi les juridictions de l'ordre administratif et à leur sommet le Conseil d'État sont seuls compétents pour ce type de litige car cela implique de porter une appréciation sur le fonctionnement de l'administration. A titre d'exemple, la violation par un établissement scolaire d'une règle de droit ou une négligence, une erreur, une omission dans le fonctionnement du service (aucun système de filtrage sur les postes informatiques) sont des situations qui engage la responsabilité administrative de l'État, des collectivités publiques ou des établissements publics.
Il faut savoir que la jurisprudence du Conseil d'État a élargi la responsabilité administrative de l'État en admettant dans certains cas une responsabilité sans faute qui se fonde sur le risque. Par exemple, le risque peut être l'existence d'une activité ou d'une situation reconnues comme dangereuses. Jusqu'à présent, aucune activité en ligne n' a été reconnue comme dangereuse par le Conseil d'État.

Dans le cas de la **responsabilité civile**, l'État est indirectement reconnu responsable lorsqu'une faute personnelle d'un enseignant à l'origine du préjudice est prouvée. **La faute personnelle** correspond au fait ou agissement dommageable commis à l'occasion du service, mais qui peut se détacher de la fonction. La faute résulte non pas du dysfonctionnement du service, mais du comportement individuel de l'agent public, de son humeur ou de sa volonté de sorte qu'un autre agent dans les mêmes circonstances aurait pu agir autrement. Ici, l'agent est personnellement responsable de la faute à l'origine du préjudice. C'est pourquoi les juridictions de l'ordre judiciaire et à leur tête la Cour de cassation sont compétentes pour ce type de litige, car cela n'implique qu'une appréciation du comportement de l'agent sans considération de sa fonction. Le principe de séparation des autorités administratives et judiciaires est donc respecté. En vertu du droit commun de la responsabilité civile dite délictuelle (voir fiche n° 5), l'agent public auteur d'une faute personnelle devrait réparer le préjudice subi par la victime (Art. 1384 du Code civil).

Cependant, **la loi du 5 avril 1937** substitue à la responsabilité des membres de l'enseignement public ou assimilés celle de l'État qui doit réparer le dommage subi par la victime.
L'État peut éventuellement se retourner contre l'enseignant (action récursoire). Il s'agit donc d'**un régime de responsabilité civile dérogatoire au droit commun**, où l'État est reconnu indirectement responsable par le jeu d'une substitution légale au profit des enseignants.
A titre d'information, dans une même affaire, les juges peuvent apprécier qu'il y a cumul des fautes (faute personnelle de l'enseignant et faute de service). Cela conduit à deux procédures parallèles, administrative et judiciaire par le jeu des questions préjudicielles.

La responsabilité pénale est engagée lorsqu'un agent public commet une infraction définie au Code pénal. Dans ce cas, il ne s'agit plus de faute de service ou de faute personnelle, mais de contravention, délit ou crime selon la gravité des faits. Restant rares dans l'exercice des fonctions des agents publics de l'enseignement, ces infractions peuvent être soit des infractions intentionnelle, soit des infractions involontaires.

Devant la juridiction pénale, la loi du 5 avril 1937 ne s'applique pas. Le fonctionnaire auteur d'une infraction doit répondre seul des conséquences de ses actes en supportant personnellement une condamnation pénale. Dans certains cas, l'État peut éventuellement apporter une assistance juridique lors de la procédure pénale (voir fiche n°6).

La responsabilité de l'institution publique d'enseignement

1- Responsabilité d'ordre éducatif

La première des responsabilités de l'institution d'enseignement est d'ordre éducatif.
Il revient à chaque établissement public d'enseignement de prendre les mesures générales pour organiser la vie scolaire et en particulier les conditions d'enseignement.
Pour être plus précis, il faut distinguer entre les établissements d'enseignement de premier degré (**écoles maternelles et élémentaires**) et les établissements de second degré **(lycées et collèges)**.

1.1 Organisation administrative des écoles

Les écoles maternelles et élémentaires sont sous l'autorité administrative de l'inspecteur de l'Éducation nationale (IEN) de leurs circonscriptions respectives. Mais l'organisation des enseignements et de la vie scolaire est la mission du conseil d'école présent dans chaque établissement d'enseignement de premier degré. Ce conseil est composé du directeur d'école, du maire (ou son représentant), du corps enseignant, des représentants des parents d'élèves, du délégué départemental de l'Éducation nationale (DDEN) et de l'inspecteur de l'Éducation nationale compétent (IEN).
Se réunissant une fois par trimestre, les conseils d'écoles ont pour principale mission de voter le règlement intérieur de l'école, le projet d'école ; d'établir le projet d'organisation de la semaine scolaire ; de donner leur avis et de présenter toutes les suggestions concernant le fonctionnement de l'école ou les questions intéressant la vie de l'école telles que les actions pédagogiques ou l'utilisation des moyens alloués à l'école…(Art. L 411-1 et s. du Code de l'éducation).

1.2 Organisation administrative des collèges et lycées

Les collèges et lycées sont des établissements publics locaux d'enseignement (EPLE) administré par un conseil d'administration sous la responsabilité d'un chef d'établissement (proviseur dans les lycées et principal dans les collèges). Le principe est l'autonomie pédagogique et éducative des établissements du second degré sous le contrôle des autorités de tutelle. Les décisions concernant le contenu et l'organisation de l'action éducative sont transmises à l'autorité académique (rectorat pour les lycées, inspection académique pour les collèges) et deviennent exécutoires dans un délai de 15 jours sans réaction de l'autorité de tutelle. Les mêmes règles sont suivies pour les décisions concernant le fonctionnement de l'établissement sauf que les actes sont transmis cette fois au préfet, au conseil régional et au rectorat pour les lycées, au conseil général et à l'inspection académique pour les collèges.
L'organe de décision des lycées et collèges est le conseil d'administration. Présidé par le chef d'établissement, sa composition est tripartite : un tiers de représentants de l'administration et des élus locaux, un tiers de représentants du personnel de l'éducation, un tiers de représentants des élèves et des parents d'élèves (Art. L 421-2 du Code de l'éducation).
Se réunissant au moins trois fois par an, le conseil d'administration a pour principales fonctions de fixer les principes de mise en œuvre de l'autonomie pédagogique et éducative, d'adopter le projet d'établissement et d'établir le règlement intérieur…(Art. L 421-4 du Code de l'éducation).
Pour information, concernant spécifiquement les TIC, l'article L 312-9 du Code de l'éducation détermine les dispositions générales concernant l'organisation des enseignements de technologie et d'informatique.

2- Responsabilité d'ordre juridique

Parallèlement à cette mission d'enseignement, comme l'indique la circulaire n° 96-248 du 25 octobre 1996 relative à la surveillance des élèves, l'institution scolaire assume également la responsabilité des élèves qui lui sont confiés. « Elle doit veiller à ce que ces derniers ne soient pas exposés à subir des dommages, et n'en causent pas à autrui, qu'il s'agisse d'autres usagers ou tiers au service ». Cela vaut pour l'ensemble des activités prises en charge par l'établissement.
De cette obligation de surveillance découle le **règlement intérieur** de l'établissement élaboré par le conseil des écoles ou le conseil d'administration. Il doit fixer de manière simple et exhaustive les modalités de surveillance des élèves dans le respect des droits et obligations de chacun, élèves comme enseignants. Dans un souci de formation civique des élèves, le règlement intérieur doit toujours être affiché dans un endroit accessible de l'établissement. De plus, souvent, à l'occasion de la rentrée, le règlement intérieur est commenté et signé par les élèves et leurs parents.
Le règlement intérieur résume ainsi les limites d'un des aspects de la responsabilité administrative à la charge de l'établissement. En effet selon les principes généraux du droit administratif, la réparation de tout dommage causé par un mauvais fonctionnement du service public d'enseignement incombe aux établissements scolaires (voir fiche n°2).
Le champ de cette responsabilité est la contrepartie des pouvoirs d'organisation des activités scolaires reconnus aux établissements. Sur ce point, il faut distinguer entre les écoles et les EPLE (collèges et lycées).
Concernant les écoles primaires, la responsabilité administrative incombe principalement à l'inspecteur de l'éducation nationale (IEN) dont dépend l'école. En cas de mise en cause de l'école élémentaire lors d'activités en ligne pour non-respect du règlement intérieur, seul l'IEN peut représenter l'école.
Concernant les collèges et lycées auxquels est reconnue une autonomie juridique, la responsabilité administrative incombe principalement au chef d'établissement, qui en tant que représentant légal de l'établissement doit assurer le bon ordre, la sécurité des biens et des personnes, l'application du règlement intérieur ou l'organisation du personnel lors des activités en ligne.
Souvent annexées au règlement intérieur des établissements d'enseignement, les chartes d'utilisation de l'Internet en milieu scolaire sont élaborées par les conseils d'écoles ou les conseils d'administration des EPLE.
Comme le règlement intérieur, ces chartes d'utilisation doivent être l'objet d'un large débat au sein des conseils de chaque établissement afin de posséder une fois votées par les membres des conseils d'écoles ou d'administration une légitimité permettant un meilleur respect des règles.

La responsabilité de l'institution d'enseignement privé

En vertu du principe de la liberté d'enseignement reconnu par l'article L 151-1 du Code de l'éducation, coexistent en France deux types d'institutions d'enseignement : public ou privé.
Comme nous l'avons précédemment vu, les établissements publics sont soumis aux principes de la responsabilité administrative auxquels les établissements privés échappent partiellement.

1- Responsabilité civile d'ordre délictuel

Concernant la **responsabilité délictuelle**, il faut en effet distinguer entre les établissements d'enseignement privé associés et non associés.
Dans le premier cas, l'institution privée est liée à l'État par un contrat d'association qui soumet l'enseignement aux mêmes règles que le service public d'enseignement, en vertu des articles L 442-5 et s. du Code de l'éducation. C'est pourquoi depuis le décret n°60-389 du 22 avril 1960, l'État se substitue aux membres enseignants de ces établissements pour la réparation des dommages causés par leur faute. Il s'agit donc d'un régime de responsabilité dérogatoire au droit commun.
Par contre, dans le second cas, les établissements privés sous contrat simple régis par l'article L 442-12 du Code de l'éducation, les règles du droit commun s'appliquent, c'est-à-dire l'article 1384 alinéa 5 du Code civil. L'établissement d'enseignement privé, en tant que commettant doit réparer les dommages subis ou causés par un élève suite à une faute d'un membre de son personnel enseignant, considéré comme préposé.

2- Responsabilité civile d'ordre contractuel

Enfin, quelque soit le statut de l'établissement, la **responsabilité contractuelle** des écoles privées est identique. Toutes se voient confier des élèves suite à un **contrat d'enseignement** qui les lient aux parents. Outre à titre principal une obligation de dispenser un enseignement conforme aux programmes, le contrat d'enseignement comprend également une obligation accessoire de sécurité. Avant 1995, contractuellement tenu d'assurer la sécurité dans leurs locaux, la responsabilité des établissements était engagée seulement si lors de la survenance d'un accident était prouvé un défaut de surveillance ou un mauvais aménagement des locaux imputable aux établissements.
Depuis un arrêt du 17 janvier 1995, la Cour de cassation considère que les établissements d'enseignement privé sont responsables contractuellement et sans faute des choses qu'ils mettent en œuvre. Cela signifie que la faute de l'école n'est plus à prouver par la victime pour se voir réparer un dommage survenu lors des activités d'enseignement. L'existence d'un dommage suffit au constat de l'inexécution de l'obligation de sécurité.

La lourde charge de cette responsabilité devrait inciter fortement les responsables d'établissement à élaborer des règles dédiées à l'utilisation de l'Internet en milieu scolaire afin de prévenir les situations où la responsabilité de l'établissement pourrait être invoquée.

La responsabilité civile de l'enseignant/éducateur

Accessoire à sa mission d'apprentissage (art. L 912-1 du Code de l'éducation), l'enseignant assume une **responsabilité délictuelle** qui découle de son obligation de surveillance de ses élèves, ainsi qu'une **responsabilité pénale** lorsqu'il commet une faute d'imprudence ou de négligence (voir fiche n°6).
En vertu de l'article 1384 du Code civil, « les instituteurs (...) sont responsables du dommage causé par leurs élèves pendant le temps qu'ils sont sous leur surveillance et (…) les fautes, imprudences ou négligences invoquées contre eux comme ayant causé le fait dommageable, devront être prouvées, conformément au droit commun, par le demandeur à l'instance ».

1- QUE FAUT-IL COMPRENDRE SOUS LE TERME JURIDIQUE « INSTITUTEUR » DÉSIGNANT LES ENSEIGNANTS?

Pour désigner le corps enseignant, le Code civil parle « d'instituteur », mais pour les tribunaux, ce terme doit être entendu plus largement que le langage courant ne l'entend.
Suivant une conception extensive, il s'agit de «toute personne qui donne l'enseignement d'un art ou d'une science, à titre onéreux ou gratuit» (Dalloz action responsabilité, n°3535, 1998). Plus exactement, la condition déterminante à la reconnaissance de la qualité d'instituteur au sens juridique du terme est la surveillance effective des élèves attachée à la fonction d'éducation. C'est ainsi que la Cour de cassation admet que « la mise en jeu de la responsabilité des maîtres est liée au devoir de surveillance qui leur incombe en contrepartie de l'autorité que leur confèrent leurs fonctions » (Civ. 2ème, 15 avril 1961, Bull. civ. II, n°276).

Le terme « instituteur » comprend donc les professeurs des écoles, de collèges ou de lycées, à l'exception de certaines matières techniques (art. L 412-8-2 du Code de la sécurité sociale) et de l'enseignement supérieur. En effet, les professeurs d'université exercent leurs enseignements devant des étudiants qui n'ont plus à surveiller car ces derniers ont un statut d'auditeurs et non plus d'élèves, sauf en période d'examens.

2- QUELS DOMMAGES ?

Seuls les dommages causés pendant que l'élève est sous la surveillance de l'instituteur peuvent entraîner sa responsabilité civile.
Le temps de surveillance comprend les heures d'enseignement, mais aussi la récréation ou les temps de pause entre ses cours. Au collège ou au lycée, l'enseignant qui a terminé son cours doit se préoccuper de la prise en charge de ses élèves par le professeur qui donne le cours suivant (Civ. 1er, 20 déc. 1982, Bull. civ. I, n°369). L'obligation de surveillance s'étend également aux sorties scolaires que l'enseignant organise, même avec des accompagnateurs. Pour la jurisprudence, « la responsabilité de l'instituteur est permanente à l'égard des enfants de sa classe, les accompagnateurs participant sous sa responsabilité générale à l'encadrement…à son bon déroulement » (CA Grenoble, 12 juin 1988, Gaz. Pal. 1988.2.460, note S. Petit).
En revanche, l'élève cesse d'être sous la surveillance de l'instituteur lorsqu'il quitte régulièrement le cours pour se rendre de sa propre initiative seul ou avec d'autres élèves à la mairie, à la bibliothèque ou tout autre lieu pour se documenter ou compléter le cours (Civ. 2ème, 3 oct. 1990, D. 1990, IR 237).
Sous sa surveillance, la responsabilité de l'enseignant est selon les cas engagée totalement ou partiellement lorsque un dommage est causé à l'élève par l'instituteur lui-même ou par un autre élève ou un tiers, mais aussi lorsque l'élève cause un dommage à lui-même ou à un tiers.

3- QUELLES FAUTES ?

Il ne suffit pas qu'un dommage survienne lors du temps de surveillance de l'instituteur. La loi du 5 avril 1937 exige également la preuve d'une faute de l'instituteur pour engager sa responsabilité. Il s'agit d'une **responsabilité sur faute prouvée**.
Il est impossible de donner une liste exhaustive des fautes possibles. Elles sont appréciées souverainement par les juges du fond, au cas par cas. Les magistrats ne se suffisent pas de la preuve de la négligence de l'établissement d'enseignement. La négligence de l'instituteur doit être déduite des circonstances de la cause. **La responsabilité de l'enseignant/éducateur sera retenue uniquement s'il existe un lien de causalité suffisant entre le dommage causé par l'élève ou subi par lui et la faute reprochée à l'instituteu**r. Les juges tiennent compte de l'âge et du comportement des enfants placés sous la surveillance de l'enseignant.
Pour des jeunes enfants, la surveillance doit être continue et l'enseignant ne peut pas quitter son poste sans s'assurer de la continuité de la prise en charge des élèves. Par contre, pour des élèves âgés de 16 ans, il est admis que la surveillance peut être moins constante.

Souvent, la faute consiste en un manque de vigilance, d'initiative ou de diligence. Ceci dit, il faut distinguer la faute caractérisée de l'enseignant de l'organisation déficiente ou des matériels non adéquats qui sont des fautes ou des négligences imputables aux établissements eux-mêmes et non aux personnels enseignants.

4- QUELLES RÉPARATIONS ?

L'article L 911-4 du Code de l'éducation (article 2 de la loi du 5 avril 1937) édicte un principe de substitution de responsabilité de l'État au profit des **membres de l'enseignement public**. Lorsque les conditions d'application de la loi de 1937 vues plus haut sont réunies, cela signifie que la victime est indemnisée de son préjudice par l'État et non pas de l'enseignant, reconnu pourtant comme responsable de la faute à l'origine du préjudice. Selon un mécanisme proche de la subrogation par changement de débiteur, l'État se substitue à l'enseignant pour assumer les conséquences du comportement fautif de l'enseignant.
Outre les enseignants ou les éducateurs, fonctionnaires de l'éducation nationale, cette substitution s'étend également aux enseignants des établissements privés sous contrat d'association, rémunérés par l'État ou sous la tutelle de l'Éducation nationale.
En revanche, pour **les membres de l'enseignement privé sous contrat simple**, la substitution ne joue pas. Ici l'enseignant fautif est entièrement responsable et doit réparer personnellement le préjudice dont il est l'auteur, en vertu du droit commun de la responsabilité pour fait personnel (art. 1384 al. 8 du code civil).
En pratique, l'enseignant est souvent incapable d'indemniser seul la victime du dommage. C'est pourquoi il est conseillé à la victime du dommage de faire jouer également la responsabilité pour fait d'autrui (art. 1384 al. 5 du code civil) de l'établissement privé, reconnu alors comme commettant de l'enseignant fautif (V. Dalloz Action, responsabilité n°3566, 1998). Cela signifie que l'établissement privé sera appelé à réparer les dommages causé par la faute personnelle de son enseignant, en vertu du contrat de travail qui le lie à lui.

La responsabilité pénale de l'enseignant/éducateur

Outre une responsabilité civile, l'enseignant peut aussi devoir assumer une responsabilité pénale lorsqu'il commet une faute d'imprudence ou de négligence. Du fait de l'obligation de surveillance, le monde enseignant connaît un changement de régime de cette responsabilité pénale depuis la loi du 10 juillet 2000. **L'application jurisprudentielle de ces nouvelles dispositions fait débat et peut à l'avenir évoluer.** C'est pourquoi seule la position présente et non définitive de la jurisprudence actuelle est ici exposée.

1- PRINCIPES DU DÉLIT NON INTENTIONNEL

Avant l'adoption de la loi du 10 juillet 2000, toute personne ayant commis une faute d'imprudence ou de négligence, même vénielle, pouvait voir sa responsabilité pénale engagée, dès lors que cette faute avait été appréciée par les juges comme l'une des conditions nécessaires à la réalisation du dommage.
Pour plus de sécurité, la loi n° 2000-647 du 10 juillet 2000 en son article 1 donne à présent **une définition légale du délit non intentionnel** :
« il y a délit,
1 - lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, s'il est établi que **l'auteur des faits n'a pas accompli les diligences normales** compte tenu, le cas échéant de la nature de ses missions ou de ses fonctions, de ses compétences ainsi que du pouvoir et des moyens dont il disposait.
2 - lorsque les personnes physiques qui n'ont pas causé directement le dommage, mais (…) **ont crée la situation qui a permis la réalisation du dommage ou (…) n'ont pas pris les mesures permettant de l'éviter**,(…).
Autrement dit, les enseignants sont responsables pénalement s'il est établi qu'ils ont , soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée qui exposait autrui à un risque d'une particulière gravité qu'ils ne pouvaient ignorer ».

Il convient donc de distinguer les deux hypothèses suivantes :

1ère hypothèse : L'auteur a causé le dommage directement.

Une faute ordinaire « d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement » suffit pour engager la responsabilité pénale.

2ème hypothèse : l'auteur a seulement « créé ou contribué à créer la situation qui a permis la réalisation du dommage ou (…) n'a pas pris les mesures permettant de l'éviter ».

La nouvelle loi impose la preuve d'une faute qualifiée, l'auteur du dommage devant avoir :

- soit violé de façon manifestement délibérée une obligation de prudence ou de sécurité prévue par la loi ou le règlement,

- soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'il ne pouvait ignorer.

Ainsi on pourra constater que la loi du 10 juillet 2000 a institué en matière d'infractions non intentionnelles **un régime de responsabilité pénale** plus favorable que par le passé et qui trouvera bien évidemment application dans le cas d'un membre de l'équipe éducative ayant la charge des activités liés à l'Internet et à l'informatique.

Ces textes ne peuvent être mis en application qu'à la demande soit du Procureur de la République, soit sur plainte avec constitution de partie civile auprès d'un Juge d'Instruction, soit par voie de citation directe.

2- LA PROTECTION DUE AUX MEMBRES DE L'ÉQUIPE ÉDUCATIVE ÉVENTUELLEMENT POURSUIVIS

L'article 11 alinéa 4 de la loi n°83-634 du 13 juillet 1983, modifié par la loi n° 96- 1093 du 16 décembre 1996, protège les fonctionnaires si les faits qualifiés de délits sont non détachables de l'exercice de la fonction du service public d'enseignement.
Aux termes dudit article : « La collectivité publique est tenue d'accorder sa protection au fonctionnaire ou à l'ancien fonctionnaire dans le cas où il fait l'objet de poursuites pénales, à l'occasion de faits qui n'ont pas le caractère d'une faute personnelle ».
Cela signifie que l'État assure une assistance juridique lors de la procédure pénale engagée à l'encontre des agents de l'Éducation nationale poursuivis pénalement, à condition que le délit non intentionnel qui est reproché aux agents ne résulte pas d'une faute personnelle, mais d'un dysfonctionnement du service.

En tout état de cause, même si l'enseignant est condamné pénalement, c'est l'Etat qui, in fine, assumera l'indemnisation civile du préjudice, consécutivement à la procédure pénale.

La responsabilité du personnel assistant

Compte tenu de la dimension technique de l'utilisation de l'Internet, les établissements scolaires font quelquefois appel à des informaticiens capables de former les élèves ou les enseignants à l'usage des multiples services en ligne qui nécessitent la maîtrise de logiciels et une connaissance de base des réseaux informatiques.
Le statut de ce personnel dépend de l'organisation pédagogique de chaque établissement, mais deux situations sont à distinguer :

1- L'ANIMATION D'UN LABORATOIRE INFORMATIQUE

Soit l'établissement lui confie l'animation d'un laboratoire informatique où il accueille seul les élèves afin de les initier à l'usage des services en ligne. Dans ce cas, d'un point de vue juridique, il doit être assimilé à un éducateur et est donc soumis au régime de responsabilité sur faute prouvée des instituteurs (article 1384 al. 8 du code civil). La substitution de l'État ne joue que s'il est rémunéré par l'État. Dans le cas contraire, outre la responsabilité personnelle de l'éducateur, l'établissement pourrait également être tenu pour responsable à titre de commettant de l'éducateur.

2- L'ASSISTANCE DES ENSEIGNANTS

Soit l'informaticien assiste les différents enseignants et leurs classes à gérer les aspects techniques de l'utilisation de l'Internet. Dans ce cas, les élèves restent sous la surveillance de l'enseignant qui d'un point de vue juridique demeure seul responsable si un dommage survient pendant le cours. L'informaticien doit ici être assimilé à un assistant d'éducation qui exerce sa fonction d'éducateur sous la responsabilité de l'enseignant (art. L 916-1 CE).

3- CONSEILS

Quelque soit le cas de figure, étant souvent le mieux placé pour connaître les risques inhérents à l'utilisation des services en ligne, il incombe à l'informaticien d'informer les utilisateurs novices. Cette information sur les risques fait partie de la formation des élèves ou des enseignants. Sur ce point, l'élaboration de règles d'utilisation adaptées au contexte favorise grandement la sensibilisation des

utilisateurs aux risques, l'information pouvant alors se limiter à un commentaire pratique des règles.

De plus, indispensable par ses connaissances techniques, l'informaticien ne doit pas bien entendu se limiter à l'information, mais également le cas échéant être étroitement associé à l'élaboration des chartes d'utilisation de l'Internet au sein de l'établissement scolaire qui l'emploie.

La responsabilité des intermédiaires techniques

L'Infrastructure technique de l'Internet rend indispensable la prestation des intermédiaires techniques qui dans certaines conditions peuvent aussi assumer une part de responsabilité lors du développement d'activités en ligne en milieu scolaire.

1- PRÉSENTATION TECHNIQUE DE L'INTERNET

Concrètement, l'Internet se présente comme un réseau mondial d'interconnexion des réseaux informatiques. Cette prouesse repose sur l'utilisation d'un protocole de communication dit TCP/IP commun à toutes les machines connectées au réseau Internet.
Schématiquement, **TCP** signifie Transmission Control Protocol et renvoie à l'organisation des données en paquets lors de la transmission d'informations entre machines. **IP** signifie Internet Protocol et désigne le langage informatique permettant l'acheminement des données de machine à machine jusqu'à leur destination finale. Pour être reconnue sur le réseau, chaque machine possède ainsi un numéro IP personnel et unique qui se présente sous forme d'une combinaison de 10 chiffres. Chaque poste connecté à l'Internet peut ainsi être identifié par les autres postes, ce qui lui permet d'expédier comme de recevoir des données par paquets.

2- DÉFINITION JURIDIQUE DES INTERMÉDIAIRES TECHNIQUES

Sous ce terme d'intermédiaire technique, le droit tente de classer tous les métiers liés à l'Internet qui se caractérisent par **l'accomplissement d'une tâche technique entre l'envoi de données et la réception finale des informations.** Le trait commun de tous ces intermédiaires est de ne pas exercer de droit de regard sur l'information qui transite grâce à eux. C'est pour cette raison qu'ils sont en principe exonérés de responsabilité.

2.1- Le fournisseur d'accès à l'Internet

Le fournisseur d'accès est le premier des intermédiaires techniques qui intervient obligatoirement dans un projet d'utilisation de l'Internet en milieu scolaire. Sa fonction purement technique est de relier le matériel informatique à la disposition d'un établissement scolaire à l'Internet.
Le fournisseur d'accès en paramétrant le matériel informatique de l'établissement scolaire et en le connectant à son serveur permet ainsi aux élèves et aux enseignants de communiquer potentiellement avec des millions de postes informatiques à travers le monde.
Sa fonction se limitant à une prestation strictement technique – connecter des machines à un serveur sous TCP/IP -, le fournisseur d'accès est juridiquement rattaché au concept **d'intermédiaire technique.**
Dans le large spectre des métiers de l'intermédiation, le fournisseur d'accès offre la première et la dernière prestation technique aux internautes, lors de la transmission d'information par le réseau. Autrement dit, nous concernant, cela signifie que le fournisseur d'accès a techniquement la maîtrise de l'envoi et de la réception de données pour ou par les postes informatiques de l'établissement scolaire connectés à son serveur, sans pouvoir en connaître le contenu.

2.2- Le fournisseur d'hébergement

Les métiers de l'intermédiation ne s'arrêtent pas à la fourniture d'accès à l'Internet. D'autres prestations sont fournies par les intermédiaires techniques pour permettre l'utilisation de l'Internet en milieu scolaire. Il est fait ici référence aux activités d'hébergement ou plus largement de stockage d'informations. A titre d'exemple, les sites Web conçus par les écoles sont ensuite hébergés ou «stockés » chez des fournisseurs d'hébergement, permettant ainsi la consultation en ligne par l'ensemble des internautes. Il en est de même pour les serveurs qui hébergent les activités de messagerie électronique (courriel, forum, liste de discussion ou chat) Il existe également les services de référencement. C'est ainsi que des sociétés informatiques élaborent pour les écoles des sites portails qui référencent tous les liens utiles ou facilitent la recherche d'information par la mise à disposition de moteurs de recherche.

L'article 14 de la Directive n° 2000/31 du 8 juin 2000 dite commerce électronique définit ces services comme ceux qui consistent à « stocker des informations fournies par un destinataire de service ».

L'article 43-8 de la Loi du 30 septembre 1986 modifiée relative à la liberté de communication définit les fournisseurs d'hébergement comme «les personnes physiques ou morales qui assurent, à titre gratuit ou

onéreux, le stockage direct et permanent pour mise à disposition du public des signaux, écrits, images, sons ou messages de toute nature accessibles par ces services».

2.3- Le cas particulier de la forme de stockage dite caching

La forme de stockage dite caching est la conséquence pratique du mode de transmission des données sur l'Internet (TCP/IP) qui fait transiter les données envoyées sur plusieurs serveurs avant d'arriver à leurs destinations finales. Ce type de stockage sur les serveurs qui permet l'acheminement des données est automatique (aucune intervention humaine) et temporaire (quelques secondes).

L'article 13 de la Directive n° 2000/31 du 8 juin 2000 dite commerce électronique définit le caching comme «le stockage automatique, intermédiaire et temporaire de l'information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service»

3- LES DIFFÉRENTS RÉGIMES DE RESPONSABILITÉ DES INTERMÉDIAIRES TECHNIQUES

Type de services offerts par l'intermédiaire technique	Principe	Exceptions	Obligations
Accès à l'Internet (Art 43-7 et 43-9 de la loi du 30 septembre 1986)	Irresponsabilité	Aucune	**1** -Informer les abonnés de l'exist de moyens techniques permettan restreindre l'accès à certains serv ou de les sélectionner **2** - Proposer un moyen de filtrage **3** – Conserver les données de na permettre l'identification de toute personne ayant utilisé son service
Caching	Irresponsabilité	Aucune	Aucune
Hébergement (Art 43-8 et 43-9 de la loi du 30 septembre 1986)	Irresponsabilité	**Intermédiaire responsable** si n'a pas agi promptement pour empêcher l'accès au contenu hébergé suite à la saisie par une autorité judiciaire **Projet de loi LEN:** si n'a pas agi promptement pour empêcher l'accès au contenu hébergé **dès la connaissance effective du caractère illicite**	**1** - Fournir aux responsables de contenus hébergés le moyen tech de s'identifier **2** – Conserver les données de na permettre l'identification de toute personne ayant utilisé son service

Remarque :

Plus que la responsabilité juridique qu'ils encourent et au delà de l'obligation principale de nature technique, il est important de noter que les fournisseurs d'hébergement sont également tenus d'**informer les établissements scolaires des risques inhérents à leurs services de stockag**e. Cette information sera très utile lors de l'élaboration des chartes d'utilisation de l'Internet.

La responsabilité des parents

Le droit fait peser sur les parents une responsabilité du fait de leurs enfants. Tous les parents sont concernés, qu'ils soient légitimes, naturels ou adoptifs. En vertu de l'article 1384 alinéa 4 du Code civil, « le père et la mère, en tant qu'ils exercent le droit de garde, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux ».

1- Minorité de l'enfant

Tout d'abord, la responsabilité des parents ne joue que si l'enfant, auteur du dommage est mineur. A contrario, leur responsabilité cesse dès que l'élève atteint l'âge de 18 ans ou est émancipé dès l'âge de 16 ans révolu. En effet, comme le stipule l'article 482 du code civil, « le mineur émancipé cesse d'être sous l'autorité de ses père et mère ». De même, selon l'article 476 du code civil, « le mineur est émancipé de plein droit par le mariage ». Il faut préciser que la femme peut contracter mariage dès l'âge de 15 ans révolus.
Ensuite, le père ou la mère sont responsables des faits dommageables de leurs enfants uniquement s'ils cohabitent avec eux. Plus que l'autorité parentale, il est exigé une condition de cohabitation.

2- Cohabitation avec l'enfant

Pour les parents vivant ensemble, la cohabitation avec leurs enfants n'est qu'un des éléments de leur autorité parentale qui leur octroie un droit de garde, de surveillance et d'éducation. En contrepartie, les parents sont solidairement responsables des faits de leur enfant.
Par contre, pour les parents séparés, même s'ils exercent conjointement l'autorité parentale, le parent responsable est celui qui exerce le droit de garde au moment du dommage. Ainsi, à titre d'exemple, en cas de garde alternée, le parent responsable sera celui chez qui l'enfant habitait le jour où survient le dommage.

3- Une responsabilité de nature objective

Expression de la solidarité familiale, la responsabilité des parents découle d'une obligation de garantie. Comme le rappelle clairement la Cour de cassation (Assemblée Plénière, 9 mai 1984, Fullenwarth c/ Felten, D. 1984.525), l'article 1384, alinéa 4 exige seulement que le mineur « ait commis un acte qui soit la cause directe du dommage invoqué par la victime ». La faute de l'enfant n'est pas une condition d'application de l'article 1384. Cela signifie que la responsabilité des père et mère est **une responsabilité objective**. L'enfant commettant un fait non fautif, ses parents deviennent responsables en dehors de toute faute, simplement parce qu'il existe un fait dommageable dont l'enfant est l'auteur. Il n'est donc plus possible aux parents de s'exonérer en établissant l'absence d'une faute d'éducation ou de surveillance. « Seule la force majeure ou la faute de la victime peut exonérer le père ou la mère civilement responsable du fait de leur enfant » (Civ. 2ème, 19 févr. 1997, gaz. Pal. 19972.572).
C'est pourquoi « la présence d'un enfant dans un établissement scolaire ne suffit pas par elle-même à écarter la responsabilité des parents » (Civ. 2ème, 16 mai 1988, Gaz. Pal. 1989, 2 somm. 371).

La responsabilité des élèves

Mineur, l'élève n'encourt aucune responsabilité légale pour les actes dommageables dont il est l'auteur. Une responsabilité du fait personnel ou des choses en tant que gardien ne pèsera sur lui seulement s'il est âgé de plus de 18 ans ou émancipé après 16 ans. Comme nous l'avons vu précédemment, la réparation des dommages causés par l'élève incombera soit à l'instituteur fautif, soit aux parents. En contrepartie, le droit leurs reconnaît une certaine autorité sur l'élève qui doit suivre leurs instructions quant à son éducation.

1- Une autorité modulable

Concernant plus particulièrement le milieu scolaire, en vertu de l'article L 511-1 du Code de l'éducation, « les obligations des élèves consistent dans l'accomplissement des tâches inhérentes à leurs études ; elles incluent l'assiduité et le respect des règles de fonctionnement et de la vie collective des établissements ». A cela, l'article L 511-2 du Code de l'éducation ajoute que « dans les collèges et les lycées, les élèves disposent, dans le respect du pluralisme et du principe de neutralité, de la liberté d'information et de la liberté d'expression. L'exercice de ces libertés ne peut porter atteinte aux activités d'enseignement ».
C'est pourquoi, il est indispensable de tenir compte de l'âge et de la maturité, ainsi que la nécessité d'éducation à la responsabilité et à l'autonomie des élèves pour déterminer les règles d'utilisation de l'Internet au sein des établissements scolaires. Le contrôle des agissements des élèves sera à la mesure de leur discernement à évaluer les risques et les dommages éventuels causés par leurs actes. Autrement dit, on reconnaîtra à un lycéen une plus grande liberté d'utilisation des services en ligne qu'un élève en école primaire ; mais en contrepartie, on attendra de lui une conduite responsable ou tout du moins d'assumer plus largement ses actes fautifs.

2- Conseil

Lors de l'élaboration des règles de conduite, il s'agit donc **d'adapter les normes de comportement au public visé**. Les règles d'utilisation de l'Internet en lycée sont différentes de celles en collège ou en école primaire.

La responsabilité de partenaires étrangers

Est envisagée ici la situation de coopération entre établissements scolaires participants à des projets pédagogiques internationaux. Il est souhaitable que l'utilisation de l'Internet en milieu scolaire permette un plus grand rapprochement des cultures, à l'instar des échanges linguistiques.
Ceci dit, cela pose la question du droit applicable aux activités en ligne. L'enjeu est de savoir **quelles règles s'appliquent aux activités en ligne**.
A titre d'exemple, les élèves d'un collège français et d'une école américaine échangent des propos sur un forum de discussion ou créent un site Web commun. Des propos négationnistes sont diffusés. Aux Etats-Unis, cet acte n'est pas répréhensible, alors qu'en France son auteur sera poursuivi pénalement. Il est donc important de connaître le droit applicable.

1- RÈGLES D'ORDRE PUBLIC

Pour les règles d'ordre public, le droit français s'applique de droit (**exception d'ordre public**). Les établissements français ne peuvent pas transiger avec leurs partenaires étrangers. Leurs activités menées en coopération doivent obligatoirement respecter les règles d'ordre public françaises. Ainsi, le régime protecteur des données personnelles de la loi française du 6 janvier 1978 ne peut pas être écarté même si le pays du partenaire étranger ne connaît aucune législation à ce propos. Au minimum, des garanties équivalentes doivent être fournies par l'établissement étranger.

2- RÈGLES SUPPLÉTIVES

Pour le reste, le choix est laissé aux parties qui peuvent contractuellement prévoir l'application de la loi du partenaire étranger, mais il est conseillé aux établissements scolaires de préférer le droit français qui souvent est plus protecteur envers les élèves et les enseignants.

3- CONSEIL

Il est conseillé aux établissements d'enseignement français envisageant des activités en ligne avec des partenaires étrangers de déterminer clairement lors de l'élaboration des chartes d'utilisation de l'Internet les conditions de compétence du droit français ou étranger, et le cas échéant de rappeler les dispositions légales obligatoires pour les activités qui se déroulent avec des partenaires étrangers. Il s'agit encore d'**adapter les normes de comportement au public visé** selon sa plus ou moins grande autonomie lors de l'activité avec des partenaires étrangers eux-mêmes plus ou moins contrôlés. Les règles d'utilisation de l'Internet en lycée sont ici différentes de celles en collège ou en école primaire.

Le courrier électronique

1- DÉFINITION TECHNIQUE ET JURIDIQUE

Le courrier électronique est le premier des services en ligne **interpersonnel**. Grâce au protocole SMTP (Simple Mail Transfer Protocol), il est ainsi possible à deux internautes possédant une adresse électronique d'échanger personnellement des fichiers textuels, graphiques ou sonores. Du fait de sa simplicité d'usage, il est le moyen le plus utilisé dans le milieu scolaire pour échanger, discuter ou transmettre des informations entre deux personnes.
Le courrier électronique allie les avantages du courrier postal et du téléphone.
Comme la conversation téléphonique, le courrier électronique ou courriel est transmis au destinataire en quelques secondes quelque soit le lieu où il se trouve. Mais à la différence du téléphone, compte tenu d'une technique neutre, le coût de l'envoi d'un message électronique à son voisin ou à un correspondant aux antipodes est identique. Le protocole de transmission ignore les frontières et ne distingue pas les transmissions nationales ou internationales.
Comme le courrier postal, le courrier électronique opère un échange **en temps différé**. Il apparaît ainsi moins intrusif pour le destinataire qui garde le choix de consulter les messages souvent textuels quand bon lui semble. Une correspondance peut ainsi être entretenue sans qu'obligatoirement le destinataire soit présent devant son poste lorsque l'expéditeur envoie le message. Cela est particulièrement appréciable lorsque le correspondant vit en décalage horaire ou ne partage pas le même rythme d'activités. La communication est donc **asynchrone**. Mais à la différence du courrier postal, l'envoi de messages est potentiellement continu et non pas limité à un unique service de distribution quotidien.
Les risques concernant le courrier électronique sont directement liés aux caractères asynchrone et interpersonnel des communications, traits dominants du courrier électronique, mais leurs étendues se mesurent aux diverses fonctionnalités offertes par le courrier électronique.
Le message électronique comprend deux parties distinctes. Le corps du message où l'expéditeur rédige le texte qu'il souhaite communiquer à son destinataire. A cela s'ajoute l'en-tête qui fournit des informations

utiles à la transmission du message.

A (to) : Ce champ précise l'adresse du destinataire. Y figure l'adresse d'un seul ou de plusieurs destinataires
De (from) : l'expéditeur indique son adresse pour que le destinataire puisse lui répondre le cas échéant.
Sujet (subjet) : L'expéditeur précise par un titre le sujet de son message.
Cc (Copie conforme ou carbon copy) : Ce champ permet l'envoi d'une copie identique du message à une ou plusieurs personnes, autres que le destinataire principal (A/to). Sont fournies les adresses de ces destinataires secondaires qui ne sont pas visés directement par le contenu du message mais qui ont un intérêt à en être informés (ex : la hiérarchie de l'enseignant).
Cci (Copie conforme invisible, Blind Carbon Copy) : dénommée également copie conforme discrète, cette fonction est identique à « Cc », à la différence que le destinataire principal ne voit pas apparaître sur l'en-tête du message qui lui est transmis les noms des destinataires secondaires.

Aux informations fournies par l'en-tête du message, s'ajoutent les différentes fonctions liées à la transmission du message électronique.

Fichier joint (attachment) : Ce champ permet de joindre tous types de fichiers au message (documents textuels, visuels ou musicaux).
Répondre à un message (reply) : Cette fonction est utile pour répondre à un message préalablement reçu. Activée par le destinataire du premier message , cette fonction inscrit automatiquement l'adresse de l'expéditeur du premier message dans le champ « A/to » et recopie le titre du premier message précédé de « Re/ » pour bien indiquer qu'il s'agit d'une réponse. De plus le corps du texte du premier est intégralement recopié, permettant à la personne de répondre en complétant le premier message. Par convention le texte original est précédé des symboles « > ».
Faire suivre un message (forward) : cette commande permet au destinataire initial d'un message de le réexpédier à un ou des tiers. Ce nouveau courrier reprend l'adresse du premier expéditeur et reproduit intégralement le corps du texte du premier message, précédé des symboles « > », complété ou modifié le cas échéant par le premier destinataire du message réexpédié.
Le carnet d'adresses : Le carnet d'adresses est un fichier préalablement constitué par l'internaute grâce à son logiciel de courrier électronique. Il comprend la liste de tous les correspondants avec leurs adresses électroniques. Activée à partir de la barre d'outils, cette fonction évite à l'expéditeur de taper l'adresse du destinataire.

2- LES POINTS DE VIGILANCE

Les fonctions comme le protocole de transmission du courrier électronique le dédient naturellement à un usage interpersonnel qui favorise la correspondance privée. C'est pourquoi les principaux risques liés à ce contexte de communication concernent avant tout les atteintes aux droits des personnes, et plus particulièrement à leur vie privée et incidemment au droit d'auteur.
Dans une moindre mesure et comme tout service de communication, l'usage du courrier électronique peut également entraîner des risques pour la collectivité. Nous pensons ici aux atteintes à l'ordre public.

2.1- Les atteintes aux droits des personnes

La diffusion de certaines informations par le biais du courrier électronique peut causer un préjudice aux personnes.
Les principales situations préjudiciables aux personnes sont les atteintes à la vie privée ou à la réputation, l'usage non autorisé de l'image, le harcèlement ou les menaces et la réception de messages non sollicités (pourriels ou spam).

2.1.1- Les atteintes à la vie privée

Les courriers électroniques peuvent contenir des précisions sur l'intimité de l'expéditeur ou d'un tiers. La correspondance privée peut être l'occasion de divulguer des informations sur soi-même ou sur des tierces personnes. Deux situations sont à distinguer.
Dans le premier cas, l'expéditeur du message consent volontairement à révéler au seul destinataire un élément de sa vie intime. Ici, le destinataire doit être considéré comme un confident qui est tenu de garder secret l'information révélée, sauf autorisation de l'expéditeur. La vie privée de l'expéditeur du message est ici sauvegardée.
Dans le second cas, des informations intimes sont divulguées à des tiers sans le consentement de l'intéressé. Un message destiné à une personne déterminée est retransmis à d'autres par celle-ci. Ici, il y a atteinte à la vie privée et cela tombe sous le coup de la loi pénale.

Article 226-1 du Code pénal :

"Est puni d'un an d'emprisonnement et de 45000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement, de porter atteinte à l'intimité de la vie privée d'autrui :

1- En captant, enregistrant ou transmettant sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2- En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.
- Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé."

Attention : un mauvais usage de la fonction "**faire suivre un message**" peut conduire à commettre un délit. Un contenu confidentiel envoyé à une personne déterminée peut ainsi être réexpédié à d'autres personnes. Le destinataire du message confidentiel doit prendre garde de ne pas le diffuser. Il doit respecter la confidentialité de la correspondance. Le conseil vaut également pour les fonctions « **fichier joint** » ou « **copie conforme** ».

2.1.2- Les atteintes à la réputation

Le contenu d'un courrier électronique peut nuire à la réputation d'une personne. Le message sera jugé diffamatoire uniquement s'il est diffusé auprès d'au moins une tierce personne et qu'il donne sur la victime qui doit être identifiable une perception négative qui l'expose à la haine ou au mépris au risque de lui faire perdre l'estime ou la confiance du public.
Selon l'article 226-22 du Code pénal :
"Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces informations à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni d'un an d'emprisonnement et de 15000 euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de 7500 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit."
Les correspondances entretenues par les élèves ou les enseignants doivent respecter la réputation et la dignité des personnes.

2.1.3 - Les atteintes à l'image

Comme la diffusion d'informations intimes, en vertu de l'alinéa 3 de l'article 226-1 du code pénal, l'image d'une personne dans un lieu privé peut être diffusée uniquement si celle-ci autorise le destinataire du message à faire suivre l'image.
Attention : La fonction « fichier joint » ne doit transmettre des photos privées d'une personne à des tiers qu'avec le consentement de la personne photographiée.

2.1.4- Le harcèlement et les menaces

Comme toute communication interpersonnelle telle que le téléphone, le courrier électronique peut également être le moyen de harceler une personne. Autrement dit, un internaute peut recevoir sur sa boîte de courrier de manière répétitive plusieurs messages désobligeants, agressifs ou menaçants axés souvent sur le sexe, la religion ou la race. Ce type de comportement est pénalement réprimé (article 222-17 du Code pénal).

2.1.5- Les messages non sollicités

Méfait de la "marchandisation" de l'Internet, les messages non sollicités appelés également pourriel ou spamming sont une utilisation abusive du courrier électronique. Cela consiste en l'envoi massif de messages souvent publicitaires ou à caractère commercial dans les boîtes électroniques d'internautes qui ont la malchance de voir leur adresse électronique vendue par un acteur du commerce électronique. Cette pratique est partiellement condamnée par la législation européenne (art. 13 de la directive n° 2002/58/CE du 12 juillet 2002).

2.2- Atteintes au droit d'auteur

Par le biais de la fonction "pièce jointe ou attachment", le courrier électronique peut transmettre des fichiers textuels, visuels ou musicaux sans l'autorisation de leur auteur. Dans ce cas, il y a atteinte au droit d'auteur ou plus précisément non respect du droit de reproduction (voir fiche n°16).

2.3- Les risques pour la collectivité

2.3.1- Les atteintes à l'intégrité des ressources informatiques

Par le biais des outils Internet et du courrier électronique en particulier, les utilisateurs peuvent propager des virus pouvant altérer le fonctionnement du matériel informatique, voire le rendre inutilisable. La loi pénale punit ce type d'agissement.
En vertu de l'article 323-2 du Code pénal :
« le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 € d'amende ». L'article 323-3 du Code pénal ajoute que « le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 € d'amende ».

2.3.2- La surveillance du courrier électronique

Compte tenu du caractère privé reconnu au courrier électronique, il est risqué pour le responsable du serveur de contrôler les échanges. Tout d'abord, la loi protège le secret des correspondances.
En vertu de l'article 226-15 du Code pénal :
« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »
De plus, il est certain qu'un contrôle systématique des contenus des messages est techniquement très lourd et illégal. Toute la difficulté est de trouver un équilibre entre la protection de l'intimité des internautes et l'intégrité du réseau. Lorsqu'un internaute est suspecté du fait d'agissements anormaux, celui-ci doit être prévenu de la surveillance dont il fait l'objet. La surveillance du courrier se justifie uniquement afin de prévenir toutes activités déloyales ou illégales commises par les enseignants ou les élèves pouvant compromettre l'intégrité du réseau.
Dans un arrêt du 17 décembre 2001, la Cour d'appel de Paris reconnaît qu'il était dans la fonction des administrateurs d'assurer le fonctionnement normal des réseaux et de veiller à leur sécurité. Cela implique qu'ils aient un accès à l'ensemble des données du réseau afin de régler les problèmes techniques, notamment ceux relatifs à la sécurité informatique.
Le Forum de l'Internet recommande que soit reconnue une obligation de confidentialité au bénéfice des administrateurs qui pourraient « surveiller » le courrier sans lire son contenu seulement pour sauvegarder la sécurité du réseau (ex : intrusion de virus).

3- LES RÉFÉRENCES LÉGALES ET JURISPRUDENTIELLES

- Article 9 du Code civil (droit à la vie privée).
- Article 222-17 du Code pénal (menaces)
- Article 226- 1 du Code pénal (atteinte à la vie privée)
- Article 226 -10 du Code pénal (dénonciation calomnieuse)
- Article 226- 15 du Code pénal (atteinte au secret des correspondances)
- Cour d'appel de Paris, Arrêt du 17 décembre 2001

4- LIENS UTILES

- Recommandations du Forum de l'Internet « relations du travail et internet » sur la surveillance des courriers

http://www.legifrance.gouv.fr/
http://www.foruminternet.org

Le chat ou clavardage

1- DÉFINITION TECHNIQUE ET PRATIQUE

Internet Relay Chat (IRC) est un service de l'Internet qui autorise l'échange interactif de messages écrits, sonores ou visuels entre plusieurs utilisateurs du réseau. Par postes d'ordinateur interposés, plusieurs internautes peuvent ainsi dialoguer simultanément. Le clavardage ou chat est la première activité en ligne à permettre une communication interactive en temps réel.

Comment cela fonctionne-t-il ?

Au préalable, l'internaute installe un logiciel client IRC tel que mIRC, Pirch ou Msn Messenger. Il lui est alors possible de se connecter sur un serveur IRC qui offre une multitude de canaux où sont présentes des chambres de discussion (chat-room) sur de nombreux thèmes.

Différents modes d'utilisation sont possibles. Les discussions sont alors publiques, semi-publiques ou privées.
L'utilisation la plus courante de l'IRC est **publique**. Dans ce cas, l'internaute choisit un canal dédié à un thème, puis prend un nom d'utilisateur ou un pseudonyme afin d'être identifié lors de la conversation. Le dialogue se noue, une fois que l'internaute écrit un message qui apparaît simultanément et en temps réel sur tous les écrans des ordinateurs connectés au même canal. Le message lu, tous les autres internautes présents dans la même chambre de discussion (chat-room) peuvent répondre et à leur tour être lus par l'ensemble des internautes connectés. Voir par exemple le réseau Epiknet.
La seconde utilisation possible est **semi-publique**. Dans ce cas, le dialogue en ligne ou le clavardage ne se déroule pas dans des chambres de discussion ouvertes à tous. Les logiciels IRC peuvent être paramétrés pour limiter l'échange de messages à une liste de contacts ou d'interlocuteurs préalablement déterminés. Il s'agit dans ces conditions de chambres de discussion **privées**, protégées par des mots de passe et réservées à l'usage de quelques utilisateurs.
La dernière utilisation possible est **strictement privée**. Bien que dialoguant dans une chambre de discussion publique, certaines fonctionnalités des logiciels IRC permettent d'envoyer des messages à un seul internaute, sans que les autres utilisateurs connectés ne soupçonnent l'existence des messages. Il s'agit des whispers (ex : Lotus, Quick).

2- LES POINTS DE VIGILANCE

Selon l'utilisation de l'IRC, la mesure des risques courus est différente, mais comme pour le courrier électronique, deux grands types de risques demeurent : ceux d'atteinte aux droits des personnes et ceux d'atteinte à l'ordre public.

2.1- Les atteintes aux droits des personnes

2.1.1- Les atteintes à l'intimité

Le clavardage (chat) est souvent l'occasion de confier des informations intimes. Cela relève du libre choix de l'auteur des confidences dans deux situations :

- Soit l'auteur s'exprime sur sa propre vie privée.

- Soit les confidences sont révélées au public avec le consentement préalable de l'intéressé.

Dans ces deux cas, la vie privée des personnes ne subit pas d'atteintes.

En revanche, tombent sous le coup de la loi (art. 226-1 al. 1 du Code pénal), les révélations faites à l'insu d'autrui sur sa vie privée dans des chambres de discussions publiques ou semi-publiques auxquelles, par nature, participent plusieurs internautes. Dans ces deux situations il y a rupture de la confidentialité des propos intimes et par conséquent atteinte à la vie privée.

2.1.2- Les atteintes au droit à l'image

Le droit à l'image est le deuxième volet de la protection légale de la vie privée. Nul ne peut communiquer à autrui une image de soi dans un lieu privé, sauf si nous accordons notre consentement (art. 226-1 al. 2 du Code pénal). Ceci dit, jusqu'à aujourd'hui les fonctionnalités des logiciels IRC ne facilitaient pas l'échange de fichiers images. A l'avenir, cela risque de devenir beaucoup plus aisé et à la portée d'un nombre plus important d'internautes.

2.1.3- Les atteintes à la réputation

Le clavardage ne nuit pas seulement à la vie privée des personnes. Il peut également nuire à la réputation des personnes. Deux types d'agissements sont pénalement répréhensibles : la diffamation et l'injure.

Survenant au cours d'échanges dans des chambres de discussions publiques, il s'agit de délits de presse, car le message est communiqué à un public de personnes non identifiables et non déterminées. La diffamation est l'allégation ou l'imputation d'un fait déterminé de nature à porter atteinte à l'honneur et à la considération d'une personne déterminée (articles 29 et s. de la loi du 29 juillet 1881). Sauf preuve contraire, la diffamation est présumée de mauvaise foi. Enfin même si elle prend une forme dubitative ou ne nomme pas expressément la personne, la diffamation est tout de même constituée si les faits permettent indirectement une identification.

Par contre l'injure publique se définit comme toute expression outrageante, termes de mépris ou invective qui ne referment l'imputation d'aucun fait (article 29 de la loi du 29 juillet 1881). Dans le cadre d'une chambre de discussion semi-publique, l'injure devient non publique et n'est plus punie que par une contravention. Dans ce cas, il s'agit d'une correspondance privée car le message est exclusivement

destiné à une ou plusieurs personnes déterminées et individualisées (La liste des participants). (Art. R 621-2 du Code pénal).

Attention : Le clavardage est malheureusement un moyen propice pour nuire à l'intimité ou à la réputation des personnes. La participation à des chambres de discussion publiques se fait souvent de manière anonyme. Le pseudonyme choisi librement par les participants peut ne révéler aucun élément sur leur réelle identité. Ils sont alors enclins à s'exprimer dans les chambres de discussion plus librement. Se sentant protégés par l'anonymat et la fugacité de la conversation, des participants peuvent tenir des propos qu'ils ne tiendraient jamais en présence des victimes des révélations ou des personnes participantes au clavardage. Tenir des propos déplacés est d'autant plus aisé que l'on a le sentiment de ne pas avoir à les assumer. Tout l'enjeu des règles à élaborer est de faire cesser ce sentiment d'impunité.

2.2- Les atteintes au droit d'auteur

L'utilisation courante des logiciels IRC conduit rarement à enfreindre les lois protectrices du droit d'auteur. Les communications par clavardage s'effectuent en temps réel et se limitent souvent à l'échange de phrases courtes, entrecoupées de signes (smileys). Cela s'apparente plus à un dialogue oral entre internautes. L'objet premier du clavardage n'est pas la diffusion d'œuvres protégées. A ce propos, une commande automatique (refresh) efface les lignes de dialogue après quelques minutes.

Ceci dit, le rapide développement des logiciels IRC tend à offrir plus de fonctionnalités. C'est ainsi que les logiciels intègrent désormais des commandes permettant l'échange d'images. Il existe également, comme pour le courrier électronique, la commande "envoyer un fichier". Il est donc possible de violer le droit de diffusion d'auteur dont on communique l'œuvre sans son consentement.

2.3- Les risques pour la collectivité

Comme tout service de communication, le chat peut être le moyen de propager des messages à caractère raciste ou antisémite contraires à l'ordre public (articles 24 et 26 bis de la loi du 29 juillet 1881). Pour l'échange de tels contenus, leurs auteurs peuvent être poursuivis pénalement.

L'ordre public protège également les mineurs contre les contenus à caractère violent, pornographique ou pédophile.

Autre risque pour un public mineur, le chat est aussi un des moyens privilégiés par les réseaux pédophiles pour atteindre leurs victimes. Grâce à l'anonymat, des internautes adultes peuvent emprunter des fausses identités en prétendant avoir un âge, une apparence, une personnalité ou un sexe différent en vue de pouvoir correspondre avec des enfants. Mis en confiance par de nombreux échanges, par le clavardage, les enfants peuvent fournir des informations qui les identifient ou les localisent (nom, adresse, numéro de téléphone, école fréquentée, etc.…) ou recevoir des images indécentes.

Sur ce point, selon l'article 227-24 du code pénal :

« Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.
Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables ».

Enfin la diffusion d'images à caractère pédophile est également réprimée par l'article 227-23 du Code pénal : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de trois ans d'emprisonnement et de 45000 euros d'amende.
Le fait de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.
Les peines sont portées à cinq ans d'emprisonnement et à 75000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunications.
Le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30000 euros d'amende.
Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image ».

Conseils :

Il est recommandé aux enseignants d'**informer leurs élèves des risques courus lors de clavardage avec des tiers inconnus**, en particulier des dérives possibles en matière de pédophilie.

3- Les références légales.

- Article 226- 1 du Code pénal (atteinte à la vie privée)

- Article 227-23 du Code pénal (diffusion d'images à caractère pédophile)

- Article 227-24 du Code pénal (protection des mineurs contre les contenus violents ou pornographiques)

- Article R 621-2 du Code pénal (injure non publique)

- Articles 24 et 26 bis de la loi du 29 juillet 1881 (diffusion de contenus à caractère raciste ou antisémite).

- Article 29 de la loi du 29 juillet 1881 (diffamation)

- Article L 332-1 du Code de propriété intellectuelle (saisie-contrefaçon)

Les forums et listes de discussion

1- Définition technique et pratique

Les forums comme les listes de discussion partagent le même protocole de transmission que le courrier électronique, à savoir le SMTP. L'échange est donc en temps différé, mais à la différence du courrier électronique, la communication est en principe de nature publique pour les deux types de services.
Ceci dit, le forum et la liste fonctionnent différemment, influençant la mesure des risques courus.

Dans le cas du **forum de discussion (Usenet)**, le message est adressé à un forum dédié à un thème particulier qui répertorie sur une base de données l'ensemble des messages qui lui sont adressés. Des sites tels que Google groups [http://groups.google.com] proposent des moteurs de recherche permettant aux internautes de facilement accéder par mots-clefs aux articles postés et archivés sur des bases de données (Usenet database). A titre d'exemple, les forums dont les thèmes concernent la littérature, les beaux-arts ou la philosophie voient leurs adresses commencer par [humanities.] (ex : humanities.philosophy.objectivism), ceux concernant les sciences sociales se repèrent par le préfixe [sci.], Pour la culture ou les problèmes sociaux [soc.], pour les groupes de discussion en français [fr.]. Il faut en effet préciser que la majorité de ces forums sont en langue anglaise.

Intéressé par un thème, tout internaute peut donc librement accéder aux archives et envoyer un nouveau message afin de participer au débat ou à la discussion.Techniquement plus restrictive, **la liste de diffusion (mailing list)** réunit toujours un groupe de personnes autour d'un thème commun. En revanche, la participation à la discussion publique nécessite un abonnement préalable à la liste par courrier électronique. A la différence du forum, les messages adressés à la liste ne sont pas archivés sur une base librement accessible, mais expédiés simultanément à l'adresse électronique personnelle de chaque internaute, abonné à la liste. Certaines listes sont ouvertes à tous, d'autre réservent leur abonnement qu'à une certaine catégorie d'internautes.

Les risques liés à la participation à des forums ou des listes de discussion ressemblent à ceux courus lors de clavardage (chat). A cela s'ajoute le risque de courriers non sollicités comme pour le courrier électronique. Ceci dit, le rôle central joué par un éventuel modérateur influe directement sur l'étendue des risques. Cernons sommairement les risques déjà étudiés plus haut (voir fiches n° 12 et 13) pour mieux décrire l'influence de la fonction de modération dans ces services de communication.

2- Les points de vigilance

2.1- Les atteintes aux droits des personnes

2.1.1- Les atteintes à l'intimité

Diffusés facilement auprès d'un grand nombre possible d'internautes, les messages postés sur les forums ou les listes peuvent porter un grave préjudice à la vie privée des personnes. L'atteinte à l'intimité de

victimes de messages indiscrets est certaine si la divulgation est faîte sans leur consentement. C'est pourquoi une réparation civile au bénéfice des victimes (dommages et intérêts) est possible en vertu du droit à la vie privée reconnu par l'article 9 du Code civil. De plus, le ou les auteurs des messages indiscrets sont également condamnables pénalement (article 226-1 du Code pénal).

2.1.2- Les atteintes au droit à l'image

Joints aux messages postés, des fichiers images peuvent ainsi être expédiés à l'ensemble des internautes, abonnés à des listes de discussion. Un risque d'atteinte au droit à l'image existe si par ce biais sont diffusées des images de personnes prises dans des lieux privés sans leur consentement. Cette seconde forme de violation du droit à la vie privée est civilement dédommageable (art. 9 du Code civil) et pénalement réprimable (art. 226-1 al.2 du Code pénal).

2.1.3- Les atteintes à la réputation

Les forums ou les listes peuvent voir leur thème ou sujet de discussion débordé par des messages dont le contenu a un caractère offensant, injurieux, diffamatoire ou haineux. Plutôt que de tenter d'alimenter un dialogue quelquefois contradictoire, certains internautes préfèrent s'attaquer à la réputation des participants au forum ou des abonnés de la liste.
Dans le cas du forum où les messages archivés sont libres d'accès, l'atteinte à la réputation est toujours publique et est réprimée comme délit de presse : diffamation et injure publique (art. 29 et s. de la loi du 29 juillet 1881).
Le cas est identique pour les listes de discussions dont l'abonnement est ouvert à tous et dont le fonctionnement est souvent assuré par un automate.
En revanche pour les listes de discussion dont l'abonnement est restreint, les abonnés à la liste sont déterminés et individualisés. Bien qu'étant plusieurs à recevoir le message, il s'agit de correspondance privée. Dans ce cas, seule l'injure non publique est puni (art. R 621-2 et 621-4 du Code pénal).

2.2- Les atteintes au droit d'auteur

Joints aux messages expédiés dans des listes, si des fichiers contenant des œuvres littéraires, musicales ou audiovisuelles s'échangent entre internautes sans l'accord des auteurs des œuvres, il y a atteinte au droit d'auteur et plus précisément au droit de reproduction lorsque le fichier est copié sur les postes des internautes. Comme pour le courrier électronique, la fonction « joindre un fichier » peut être un moyen de violer facilement la protection légale des « œuvres de l'esprit ».

2.3- Les risques pour la collectivité

Comme pour les atteintes aux droits des personnes, les forums ou les listes de discussion sont également le moyen de diffuser des messages dont le contenu nuit à l'ordre public. En particulier en milieu scolaire où est requis un cadre protecteur des mineurs, doit être proscrite toute discussion conduisant à des messages à caractère haineux, racistes ou antisémites ou pornographiques. Le Code pénal punit de telles dérives contraires à l'ordre public (articles 24 et 26 bis de la loi du 29 juillet 1881). Pour l'échange de tels contenus, leurs auteurs peuvent être poursuivis pénalement.
L'ordre public protège également les mineurs contre les contenus à caractère violent, pornographique ou pédophile.
Autre risque pour un public mineur, les forums ou les listes de discussion sont aussi un des moyens privilégiés par les réseaux pédophiles pour atteindre leurs victimes (Voir fiche n° 13).

Conseils :

Il est recommandé aux enseignants d'informer leurs élèves des risques courus lors de discussions sur des listes ou forums avec des tiers inconnus, en particulier des dérives possibles en matière de pédophilie.

2.4- Le rôle primordial du modérateur

L'archivage des messages pour les forums , comme l'expédition des messages aux abonnés pour les listes, est souvent exécuté automatiquement par des serveurs. Ceci dit, l'intervention humaine est techniquement possible. Dans ce cas, un modérateur contrôle le fonctionnement de la liste ou du forum qui sont alors qualifiés de **« modérés ».** Concrètement, avant l'archivage dans la base de données pour le forum ou l'expédition aux abonnés pour la liste, les messages transitent sur la boîte aux lettres électronique d'un modérateur qui vérifie la conformité des messages tant avec le thème que les règles du forum ou de la liste.
Lorsque est crée une liste ou un forum de discussion en milieu scolaire, l'avantage de mettre en place un modérateur est l'assurance que les messages postés sont conformes aux exigences de protection des enfants, une vérification effective des messages permettant d'écarter tout contenu préjudiciable. Le rôle du modérateur permet ainsi à l'établissement scolaire comme aux enseignants de mieux assumer leurs responsabilités. En effet, le milieu scolaire peut se soustraire de sa responsabilité qu'en démontrant qu'il a

joué un rôle passif et purement technique analogue au fournisseur d'accès. Cela concerne très peu de situations. **La modération des forums ou des listes est donc vivement conseillée** afin de minimiser les risques de ce type de services de messagerie.

2.5- L'obligation de filtrage

Il faut savoir que pour ce type de services de messagerie, l'utilisation de moyens de filtrages ou de firewalls (logiciel assurant la sécurité du réseau)est imposé aux établissements scolaires.
Enfin, l'emploi de listes blanches de listes ou forums recommandé par l'Éducation nationale se développe.

3- Les références légales.

- Article 226- 1 du Code pénal (atteinte à la vie privée)
- Article 227-23 du Code pénal (diffusion d'images à caractère pédophile)
- Article 227-24 du Code pénal (protection des mineurs contre les contenus violents ou pornographiques)
- Article R 621-2 du Code pénal (injure non publique)
- Articles 24 et 26 bis de la loi du 29 juillet 1881 (diffusion de contenus à caractère raciste ou antisémite).
- Article 29 de la loi du 29 juillet 1881 (diffamation)
- Article L 332-1 du Code de propriété intellectuelle (saisie-contrefaçon).

La navigation et la recherche documentaire sur la toile

1- Définition technique et pratique

Pour l'élève ou l'enseignant, la navigation constitue le premier pas dans le World Wide Web (WWW, Web ou toile). Il s'agit du contexte de communication le plus connu par le Pour l'élève ou l'enseignant, la navigation constitue le premier pas dans le World Wide Web (WWW, Web ou toile). Il s'agit du contexte de communication le plus connu par le grand public au point d'être confondu avec l'Internet. Pourtant, la toile (Web) est uniquement un service d'information. D'autres services de messagerie comme le courrier électronique ou le forum de discussion par exemple existent également sur l'Internet (Voir fiches précédentes.)
Techniquement parlant, il s'agit d'un protocole d'échange hypertexte d'information (HTTP) utilisé sur l'Internet. Le trait dominant de la toile est donc le lien hypertexte qui lie tout document « Web » au réseau.
Le protocole de communication HTTP (Hyper Text Transport Protocol) permet à tout internaute, de son poste connecté à l'Internet, d'accéder à tout document textuel, visuel ou sonore hébergé sur un serveur « Web ». Complétant ce protocole de communication hypertexte, le langage HTML (Hypertext Text Markup Language) permet la mise en forme et le balisage hypertexte de fichiers afin de les rendre accessibles sur les serveurs Web puis lisibles ou écoutables du poste de l'internaute. Toute information communiquée sur le Web se présente donc toujours sous la forme d'un fichier codé en HTML.
Sur la toile (Web), les informations contenues dans des fichiers HTML se présentent sous la forme de pages écran comprenant un contenu (texte, image, son) et des liens hypertextes (hyperlink) affichés sous forme de boutons ou d'icônes ou insérés dans un mot qui une fois activés renvoie à une autre page Web. Sous une même adresse URL, les pages Web liées entre elles constituent des sites Web. Les hyperliens renvoient donc soit aux pages d'un même site, soit à un autre site Web qui de nouveau lie un ensemble de pages ou renvoie à d'autres sites.
C'est pour cette raison que l'on parle de navigation (furetage ou browsing). Consulter des informations mises en ligne sur le Web, cela signifie accéder à des pages qui renvoient à d'autres pages ou à d'autres sites et cela jusqu'à l'information que l'on souhaite trouver. L'internaute doit donc nécessairement naviguer de pages en pages, voire de sites en sites en activant des liens hypertextes pour accéder à l'information. A la différence du livre, l'organisation du contenu n'est donc pas linéaire.
Seul avec leur logiciel de navigation qui permet l'affichage de fichiers HTML (Internet Explorer, Netscape ou Opera), l'élève ou l'enseignant sont perdus face à la masse d'informations présentes sur le WEB. Elle double chaque année. En 2003, le Web compte 10 à 30 millions de sites, 500 millions d'images, 8 à 10 milliards de pages indépendantes et accessibles (seules 3% sont en langue française).
La consultation ne se conçoit donc pas sans la recherche documentaire. En milieu scolaire, la consultation du Web s'avère utile en tant que soutien aux activités d'apprentissage par l'apport considérable des informations présentes sur la toile. Il s'agit donc pour l'enseignant et sa classe de rassembler, d'étudier, d'analyser, d'interpréter voire de résumer les documents relatifs au sujet recherché et trouvés sur la toile. Cela signifie que les élèves doivent être formés aux rudiments de la recherche de contenus numériques, en particulier à l'utilisation d'outils de recherche sur l'Internet tels que les moteurs de recherche ou les répertoires thématiques présents dans des sites documentaires ou des bibliothèques en ligne.
Les moteurs de recherche comme Google [www.google.fr] sont des outils logiciels mis en ligne qui suite à une requête à partir de mots clés sont capables d'indexer tous les sites se rapportant aux mots clés.
Par l'acquisition d'une méthodologie de travail de recherche et l'apprentissage des fonctionnalités avancée des outils de recherche, la consultation peut devenir très enrichissante tout en minimisant les risques possibles.

2- Les points de vigilance

Les risques restent limités, bien que la sécurité de la consultation demeure un enjeu d'autant plus important que l'âge des élèves est bas.
Variant selon les contextes d'apprentissage (seul dans une recherche, pendant un cours ou en groupe lors d'un travail dirigé), le risque principal découle de la possibilité d'accéder à des documents, des images ou des films préjudiciables ou choquants compte tenu de l'âge des élèves. En classe, il est de la responsabilité de l'enseignant de s'assurer que les enfants ne sont pas confrontés à des contenus haineux, violents ou pornographiques. Ceci dit, le degré d'exigence de préservation des élèves n'est pas identique selon qu'il s'agit d'un enseignement en école primaire, au collège ou au lycée. Dans ce dernier cas, la plus grande maturité et le sens critique plus développé des lycéens permet d'accepter que leurs enseignants les confrontent à des documents plus violents ou haineux (ex : documents de propagande), car certains que ces élèves sauront prendre du recul et analyseront ainsi mieux des phénomènes tels que la montée du raciste ou de l'antisémitisme en Europe.

2.1- Le filtrage comme réponse

Avant tout développées pour un usage de l'Internet dans des lieux publics, il existe des solutions techniques ou logicielles pour bloquer l'accès des machines à certaines adresses ou certains types d'informations.
Le filtrage logiciel repose sur une base de données qui liste l'ensemble des sites ou des mots-clés jugés indésirables. Si l'Internaute essaie d'accéder à un site listé ou classé sous un mot-clé interdit, son logiciel de navigation est bloqué par le filtre. Il est donc en principe impossible d'accéder à des sites jugés indésirables.
Le blocage de l'accès à des contenus indésirable peut aussi être effectué de manière technique grâce à un Proxy qui permet aux postes connectés au serveur de n'accéder qu'à un nombre limité de site.

2.2- Les cookies

En accédant à certains sites, les enfants peuvent à leur insu recueillir des fichiers témoins dit cookies qui s'enregistrent sur le disque dur de l'ordinateur. C'est ainsi que les sites visités peuvent identifier l'ordinateur de l'internaute. Cela est sans danger sauf si c'est recoupé avec des renseignements personnels qui peuvent être glanés grâce à la naïveté des enfants à qui l'on propose un jeu concours auquel il faut s'inscrire.
Cela est désormais réglementé par des dispositions communautaires.

3- Les références légales

- Article 227-23 du Code pénal (diffusion d'images à caractère pédophile)
- Article 227-24 du Code pénal (protection des mineurs contre les contenus violents ou pornographiques)
- Article 9 de la Directive 2002/58/CE du 12 juillet 2002 dite « vie privée et communications électroniques » (**cookies**)

Les collections de signets

1- Définition technique et pratique

Une consultation régulière du Web conduit souvent les enseignants ou les élèves à constituer une collection de signets. Il s'agit d'une fonctionnalité offerte par les logiciels « navigateurs » pour faciliter la navigation des internautes. Lorsqu'une personne trouve une page qui l'intéresse et souhaite pouvoir la consulter encore dans l'avenir, en activant la commande « signets », elle peut conserver sur son poste l'adresse URL de la page. Listé sur un répertoire du navigateur, un simple « clic » sur le signet permet alors de revenir sur la page Web.
Souvent, avant même que leurs élèves ne débutent leur navigation, les enseignants ont préalablement installé sur les postes une collection de signets des meilleurs sites relatifs à leur matière.
Cela n'empêche pas les élèves aguerris à la recherche documentaire de constituer eux-mêmes une collection de signets vers leurs sites préférés.

2- Les points de vigilance

Le principal risque lié à la constitution d'une collection de signets se résume à la situation où l'un des signets conduit à un site non conforme aux règles de protection des enfants. Il peut s'agir de contenus à caractère violent, haineux, raciste ou pornographique. Il est donc de la responsabilité de l'enseignant ou de l'assistant « Internet » de vérifier périodiquement les sites listés par les signets et le cas échéant de remettre à jour la collection de signets, que celle-ci ait été initialement constituée par l'élève ou par l'enseignant.
Plus généralement, une information préventive des élèves sur les sites jugés « indésirables » compte tenu des règles d'utilisation de l'Internet en milieu scolaire est un moyen simple et efficace de minimiser les risques, surtout si ce sont les élèves eux-mêmes qui créent la collection de signets.

La collecte et le partage d'information

1- DÉFINITION TECHNIQUE ET PRATIQUE

Une nouvelle étape est ici franchie dans l'utilisation de l'Internet. Il ne s'agit plus pour les élèves de consulter individuellement le Web, mais au contraire de travailler collectivement.
Sous la tutelle de l'enseignant, la collecte et le partage d'information deviennent des activités éducatives structurées. Utilisant toutes les ressources du Web, mais aussi des forums ou du courrier électronique, les élèves collaborent dans la recherche, l'analyse et le traitement de l'information en vue de constituer un fond commun. L'accent est mis sur l'échange à tous les niveaux, de la recherche à la diffusion.
Il existe donc une grande variété de projets collaboratifs.

1.1- L'échange d'informations

Différentes classes (dans le cadre d'un jumelage par ex.) peuvent faire une recherche sur une même question et partager les données recueillies (Information exchanges).

1.2- La constitution d'une banque de données commune

Plus que le partage des résultats d'une recherche, le projet interclasse peut être la constitution d'une banque de données (database creation). Outre la collecte, la collaboration concerne dans ce cas l'organisation et la diffusion des données trouvées sur le Web.

1.3- L'analyse commune des données collectées

Enfin, le dernier stade de la collaboration est l'analyse des données collectées. Suite à la saisie dans une base commune des données recueillis en différents lieux, les classes peuvent aussi échanger les résultats de leurs analyses respectives des « données primaires » (pooled data analysis).

1.4- La téléconférence avec des experts

Des contacts avec des observateurs sur le terrain (experts ou scientifiques en mission) peuvent enrichir ce travail collaboratif an sein des classes. On parle alors de téléprésence (telefieldtrips), les élèves pouvant recueillir des informations directement auprès de spécialistes via les outils de communication offerts par l'Internet.

1.5- La cyberenquête

Présentée sous forme d'une mission ou d'une investigation, la cyberenquête (Webquest) est une démarche pédagogique nouvelle et originale qui intègre pleinement l'usage des technologies dans le processus d'apprentissage. Devant trouver en partie les informations sur le Web, la cyberenquête conduit des élèves en groupe de 2 ou plus à élaborer un dossier ou un exposé « numérique ».
Par exemple, La cyberenquête « Deviens architecte » fixe comme mission aux élèves de construire un pont. Ce projet oblige les élèves à rechercher sur l'Internet les différentes techniques de construction de pont, puis de réfléchir, compte tenu de leur connaissance en matière de géométrie et de physique à la technique la plus adaptée aux conditions imposées par la mission. A l'issue de la réalisation des différents travaux sous forme numérique, la classe élit le meilleur projet de pont.
Autre exemple avec la cyberenquête « A la découverte des êtres vivants » où la mission consiste à exposer les particularités d'une des familles du règne animal en usant de textes, mais aussi de tableaux ou d'images. L'exposé « virtuel» devient ainsi beaucoup plus vivant.

2- CONSEIL

Pour que le travail en collaboration soit un succès, il faut nécessairement des règles pour gérer le partage d'information. Il faut s'accorder sur les conditions de traitement de l'information, voire de sa diffusion.
Mais au-delà du caractère collectif des travaux, cela renvoie ensuite plus spécialement aux risques inhérents à la recherche documentaire, à la création de bases de données ou à la publication sur le Web.

Les bases de données

1- DÉFINITION TECHNIQUE ET PRATIQUE

L'information mis en ligne sur le Web est organisée sous des formes diverses. L'une des plus élaborées est la base de données (database). On entend légalement par « **base de données** » « un recueil

d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière » (article 2 de la Directive n°96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, JOCE 27 mars 1996, n°L77, p.20 et s).
La base de données comprend donc un ensemble d'informations ou de données (des références bibliographiques par exemple) numérisées et gérées par des logiciels spécifiques, appelés « **système de gestion de base de données** » (SGBD) (Database management systems - DBMS) dont l'avantage est de permettre une recherche automatisée, mais aussi une mise à jour ou un enrichissement du fond par l'effacement ou l'introduction de nouvelles informations. Il s'agit d'un système de recherche documentaire automatisé. L'internaute peut ainsi en ligne « interroger» la base par mots-clés. A la suite de la requête, les résultats s'afficheront, c'est-à-dire les documents archivés dans la base correspondant aux critères recherchés.
Compte tenu des fonctionnalités avancées d'organisation et de traitement des données numérisées que permet la base de données, elle constitue donc en particulier dans le milieu scolaire une véritable richesse informationnelle. C'est pourquoi la loi la protége.
Il faut distinguer deux situations juridiques :
Soit l'enseignant et ses élèves utilisent des bases de données pour leur recherche documentaire. Ils sont **utilisateurs**.
Soit les enseignants, leurs élèves, voire l'établissement scolaire ont pour projet de constituer une base de données. Ils sont alors **producteurs**.
Selon que l'on est utilisateur ou producteur, l'étendue des risques et, plus largement, l'importance de l'enjeu des règles relatives aux bases de données varient.

2- Les points de vigilance

2.1- Les risques liés à l'utilisation d'une base de données

Lorsque l'on est simple utilisateur, il faut se limiter à une utilisation légitime des ressources de la base de données, c'est-à-dire ne pas porter atteinte aux droits du producteur de la base de données.
En vertu de l'article L 342-1 du Code de la propriété intellectuelle, « le producteur de bases de données a le droit d'interdire :
1° L'extraction, par transfert permanent et ou temporaire de la totalité ou d'une partie qualitativement ou quantativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;
2° La réutilisation, par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme ».
Il s'agit donc d'utiliser normalement la base et non pas de l'extraire ou de réutiliser abusivement.

Conseil :
Il est conseillé aux utilisateurs de lire attentivement la licence d'utilisation afin de connaître l'étendue licite de leur utilisation de la base de données.

2.2- Les risques liés à la production d'une base de données

Lorsque l'établissement scolaire est producteur d'une base de données, il doit bien informer le public utilisateur des conditions d'utilisation de la base, en particulier de l'interdiction d'extraction et de réutilisation abusive. Mais dès la constitution de la base, s'il y a compilation d'œuvres protégés (textes, images, photos, etc.) au-delà d'une simple citation et pas seulement des notices bibliographiques ou des références, il ne faut pas oublier de demander aux auteurs leur autorisation pour l'utilisation de leurs œuvres.
Comme le rappelle la directive européenne, « la protection des bases de données par le droit d'auteur prévue par la présente directive ne couvre pas leur contenu et elle est sans préjudice des droits subsistants sur ledit contenu » (art. 3 alinéa 2 de la directive du 11 mars 1996)
Enfin, lorsque la base de données comporte des données nominatives, la loi du 6 janvier 1978 dite informatique et liberté impose au producteur de déclarer le traitement auprès de la Commission Nationale Informatiques et Libertés (CNIL) et d'informer les personnes fichés (voir www.cnil.fr).

3- Références légales

- Directive n°96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données.
- Loi n°78-17 du 6 janvier 1978 dite informatique et libertés.

L'édition et la publication sur le Web

1- Définition technique et pratique

Grâce au développement de logiciels d'édition simples et conviviaux, l'édition et la publication sur le Web sont devenues des activités à la portée du large public de l'éducation. La création d'un site Web offre aux enseignants et à leurs élèves de multiples possibilités de valorisation des activités d'apprentissage. Prolongeant **la navigation et la recherche documentaire sur le Web** [voir fiche n° 17], **voire la collecte et le partage d'information** [fiche n°18], l'édition et la publication de pages Web présentent l'intérêt de fédérer toute une classe à travers la rédaction de brèves, de nouvelles, d'éditoriaux, de reportages ou la création d'images, de photographies, de séquences vidéo et de graphismes. Il peut ainsi être envisagé l'élaboration d'un journal ou d'un magazine en ligne (Web zine) ou la diffusion d'une émission radiophonique ou télévisuelle sous la forme d'un cyber-reportage. Ces activités très formatrices ont un intérêt pédagogique certain. Les travaux des élèves sont mis en valeur et leur publication en ligne offre aux enseignants un outil et du matériel utiles pour l'apprentissage des nouveaux élèves. Ceci explique que de nombreuses écoles possèdent dès à présent leur propre site Web .
La publication sur le Web ouvre ainsi de nombreuses perspectives dans l'éducation, mais confronte en même temps les acteurs du milieu scolaire à des risques inédits.

2- LES RISQUES

Lorsqu'on édite et publie sur le Web, la vigilance est à la mesure de la complexité potentielle d'un site Web qui ne se résume pas toujours à un texte mis en ligne. Un site Web peut comprendre du texte mais aussi des images, des photographies, des vidéos, des bases de données, des logiciels de recherche, des hyperliens. A ces différents types de contenu correspondent autant d'obligations différentes.

2.1- Les informations obligatoires

Considéré légalement comme un « service de communication publique en ligne », le site Web doit obligatoirement afficher des informations sur les personnes qui l'éditent, l'élaborent et l'hébergent et dans notre cas :
- nom et adresse de l'établissement scolaire.
- Nom du directeur ou du codirecteur de la publication (souvent le chef d'établissement) et le cas échéant, celui du responsable de la rédaction (souvent un enseignant en charge du suivi du site).
- Nom, dénomination ou raison sociale et adresse du fournisseur d'hébergement.

L'intérêt de ces mentions obligatoires est de faciliter la mise en œuvre de la responsabilité en cas de préjudice suite à la publication d'informations sur le site Web , compte tenu des nombreuses atteintes possibles aux droits des personnes et à l'ordre public qui nous restent à étudier.

2.2- Les atteintes à l'honneur et à la réputation

Comme pour les forums ou les listes de discussion, le site Web peut être le moyen de diffuser des propos injurieux, diffamatoires, voire haineux ou racistes.
Pour l'injure publique ou la diffamation, il s'agit d'un délit de presse exposé plus haut (voir fiche n°14 sur le chat) qui peut être imputé à son auteur et à défaut, au responsable éditorial ou au directeur de publication (responsabilité en cascade).
Les propos racistes peuvent également être poursuivis (art. 32 loi du 29 juillet 1881), comme l'apologie des crimes contre l'humanité (art. 24 loi du 29 juillet 1881).

2.3- Les atteintes à la vie privée

L'intimité des personnes doit être respectée par les créateurs de sites Web qui ne doivent pas sous peine de poursuites publier ni des photos prises dans un lieu privé ni des informations sur la vie intime des personnes sans leur consentement (voir fiche n° 13 sur le courrier électronique).
L'atteinte à la vie privée peut également être le fait de diffuser des données personnelles. Le site peut ainsi avoir mis en ligne l'annuaire des enseignants ou des élèves. S'il y a collecte et traitement de données à caractère personnel, le responsable du site doit obtenir l'accord des personnes concernées et déclarer le traitement à la CNIL (déclaration simplifiée téléchargeable sur le site Web de la CNIL (www.cnil.fr).
Plus que les données à caractère personnel, certains sites en milieu scolaire peuvent utiliser les photos des élèves mineurs. Dans ce cas, l'autorisation des deux parents est toujours requise.

2.4- Les atteintes aux droits d'auteur

Un site Web est un ensemble de textes, d'images, de sons qui peuvent être autant « d'œuvres protégées » selon l'expression consacrée par le Code de la propriété intellectuelle.

2.4.1- La création d'œuvres originales par les acteurs de l'Internet scolaire

Le premier des conseils est de privilégier, lors de l'élaboration d'un site Web en milieu scolaire, les créations des élèves ou de leur enseignants. Il s'agit de la situation la plus simple à gérer car les personnes qui mettent en ligne sont également les personnes titulaires des droits d'auteur. Le conflit est ici, par nature, impossible.

Les sites en milieu scolaire se contentent souvent d'une diffusion à titre gratuit où seules les prérogatives d'ordre moral (art. L 121-1 à 9 du CPI) ont un enjeu. Il s'agit pour l'essentiel de respecter le droit à la paternité et au respect de l'œuvre. Concrètement, cela signifie que toute mise en ligne de texte ou de toute autre forme de création doit être réalisée sans modification, ajout ou retrait de l'œuvre initiale sauf accord de l'auteur (**droit au respect de l'œuvre**) et indiquer le nom de son auteur, élève ou enseignant (**droit à la paternité**). Ceci dit, le droit au respect de l'œuvre devra être strictement appliqué pour les créations originales des élèves et plus souplement apprécié avec des contenus de nature pratique ou technique (ex : rappel d'une règle grammaticale ou d'un principe scientifique) dont la moindre originalité ne souffre pas de mises à jour possibles.

2.4.2- L'intégration d'œuvres tierces

En revanche, lorsqu'un site « scolaire » souhaite intégrer une création d'un tiers au milieu scolaire, les enseignants s'exposent au risque d'être poursuivis pour contrefaçon s'il ne respecte pas les règles élémentaires du droit d'auteur.

Par principe, la loi protège toute création mais il faut distinguer différentes situations.

- La plus avantageuse pour le milieu scolaire est l'utilisation d'œuvres tombées dans le domaine public. Cela signifie que les élèves peuvent utiliser « librement » des œuvres littéraires, musicales, photographiques, etc., à la condition que leur auteur se soit éteint 70 ans plus tôt (ex : les écrits de Molière ou de Racine). Aucune autorisation n'est à demander car les prérogatives patrimoniales du droit d'auteur se sont éteintes. Par contre, il faut toujours respecter comme plus haut le droit à la paternité et au respect de l'œuvre.

- Un second cas de figure peut être des œuvres toujours sous le monopole d'exploitation de l'auteur qui est pourtant prêt à consentir aux projets de milieu scolaire une utilisation à titre gratuit. Le responsable du site doit donc obtenir l'autorisation écrite de l'auteur (un échange de courrier électronique peut suffire). Les droits moraux sont toujours à respecter.

A côté de ce cas classique, il existe également un mouvement plus global d'**open content** avec des licences d'utilisation spécifiques que nous étudions plus dans le détail (voir fiche sur open content)

- Dans le dernier cas de figure, l'auteur use de ses prérogatives patrimoniales et souhaite être rétribué pour l'utilisation de son œuvre sur le site. Il peut s'agir de photographies ou d'œuvres musicales par exemple. Souvent la rémunération est forfaitaire et faite auprès de la société de gestion collective.

En résumé, sauf pour les œuvres tombées dans le domaine public, l'autorisation de l'auteur est toujours requise.

2.5- Les conseils quant aux hyperliens

En principe l'établissement d'hyperliens est libre. Tel est le cas lorsqu'on pointe vers la page d'accueil d'un site dont le thème est en relation avec le sien. Par contre, la situation est toute différente avec l'établissement de liens dit profonds. Cette fois-ci, le lien pointe directement vers des pages Web déterminées sans avoir à naviguer dans le site tiers. Ce sont par exemple des articles de presse ou des fichiers téléchargeables comme des rapports en ligne. Dans ce cas il est recommandé de demander l'autorisation préalable du responsable du site avant de réaliser le lien afin d'éviter d'être poursuivi pour « parasitage ».

En ce sens, concernant l'établissement de liens hypertextes, le Forum des droits sur l'Internet fait les recommandations suivantes aux concepteurs de sites :

1- éviter d'établir des hyperliens vers les pages ou ressources des sites ayant clairement manifesté leur refus dans leurs conditions d'utilisation ou sur les pages web qu'ils refuseraient de voir liées ;
2- prévenir, en conformité avec la Netiquette, le titulaire du site vers lequel il tisse un ou plusieurs lien(s) et de lui demander s'il accepte l'établissement de ce(s) lien(s)
3- retirer le lien si tel est le souhait exprimé par le titulaire du site lié ;
4- respecter les conditions de présentation que le titulaire du site serait amené à lui demander.

FORUM DES DROITS SUR L'INTERNET, Groupe de travail « Liens hypertextes »,17/06/02, http://www.foruminternet.org/publications/lire.phtml?id=367

3- Les références légales

- Art. 43-10 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Art. 43-14

dans la modification de la loi par le projet de loi pour la confiance dans l'économie numérique)
- Art. L 111.1 du Code de propriété intellectuelle (reconnaissance du droit d'auteur)
- Art. L 121-1 du Code de propriété intellectuelle (prérogatives morales du droit d'auteur)
- Art. L 122-1 du Code de propriété intellectuelle (prérogatives patrimoniales).
- Art. L 123-2 du Code de propriété intellectuelle (durée de la protection, domaine public).
- Art. L 335-3 du Code de propriété intellectuelle (Délit de contrefaçon)
- Loi n° 78-17 du 6 janvier 1978 dite « informatiques et libertés » (protection des données nominatives).

4- LIENS UTILES

- [www.cnil.fr] Voir l'espace junior qui informe les enfants de leurs droits et des risques liées à l'usage de l'Internet et l'espace déclaration qui permet en ligne de déclarer le traitement de données nominatives sur le site Web.

Le portfolio numérique

1- DÉFINITION TECHNIQUE ET PRATIQUE

Le portfolio désigne la collection de travaux d'un élève qui fait foi de sa compétence en gardant des traces pertinentes de ses réalisations.
Allant plus loin que le simple relevé de notes, le portfolio est un outil dynamique qui permet de suivre l'évolution de la progression d'un élève dans ses apprentissages. Par son activité scolaire, l'élève est l'acteur principal dans l'élaboration du portfolio qui secondairement peut également contenir des commentaires et des réflexions des enseignants et des parents.
Le caractère numérique du portfolio a l'avantage de faciliter son accessibilité et sa consultation, sa modification par l'ajout ou la suppression de fichiers ou sa réorganisation par l'insertion d'hyperliens d'un document à l'autre.
En résumé, tout l'intérêt du portfolio numérique est d'être à la fois un lieu d'archivage des travaux de l'étudiant, un lieu de réflexion, de suivi et d'évaluation.
Spécifique à chaque élève, le portfolio comprend la copie originale ou numérisée de ses devoirs ou examens (textes, images, séquences sonores ou vidéos) accompagnés des commentaires de l'enseignant, voire des parents.
Plusieurs options s'offrent à l'établissement scolaire quant à l'accès au portfolio :
Toutes les informations peuvent être stockées dans une zone confidentielle dont l'accès est limité.
Tout ou partie du portfolio peut au contraire être mis en ligne pour une consultation publique des travaux en toute transparence.
Le portfolio en tant qu'outil de suivi de la progression des élèves a un intérêt pédagogique certain, mais par nature étroitement lié à chaque élève, il leur fait aussi courir des risques.2- Les points de vigilance

2.1- LES ATTEINTES À LA VIE PRIVÉE

La première des atteintes possibles concerne la vie privée des élèves. La nature du portfolio est de traiter des données à caractère personnel sur chaque élève d'une classe. Il s'y trouve toutes les informations permettant l'identification de l'enfant (son nom et ceux de ses parents, son adresse et sa situation familiale) accompagnées de sa photo, mais aussi de ses annotations personnelles sur son travail scolaire, les commentaires et l'évaluation de son enseignant sur sa production et son comportement et d'autres commentaires le cas échéant.
Le portfolio traite donc des données sensibles qui doivent être protégées afin de pas nuire à l'intimité des élèves.
Depuis la loi n° 78-17 du 6 janvier 1978 dite « informatique et libertés », des principes légaux président à la collecte et au traitement de données personnelles comme dans le cas du portfolio. La protection de la vie privée des élèves fichés dépend du respect de cette déontologie minimale des données.
Le principe majeur dont découle tous les autres est le principe de finalité. Selon ce principe défini par la Commission Nationale Informatique et Libertés (CNIL), « tout traitement d'informations nominatives est créé pour atteindre un certain but auquel il doit être adapté et donc ne pas servir à d'autres fins ». Autrement dit, de la finalité d'un traitement dépend son seuil de dangerosité pour les personnes fichées qui légitime l'existence de garanties adaptées pour prévenir de potentielles atteintes.
Dans notre cas, la finalité pédagogique du portfolio autorise l'encadrement enseignant à légitimement collecter des données personnelles sur leurs élèves. Ceci dit, le traitement de données sur les élèves ne se justifie qu'à des fins de suivi et d'évaluation. Toute autre finalité rend la collecte illégale, car injustifiable. De plus, cela n'exempt pas, d'une part, d'informer les élèves et leurs parents de leurs droits et, d'autre part de leur permettre d'exercer leur droits.

A la lumière du principe de finalité, le dispositif protégeant les élèves fichés s'articule autour de trois axes :

- la nature des informations
- le régime de la collecte des données
- les conditions de conservation des données

2.1.1- La nature des informations

Le portfolio ne rentrant pas dans le champ de l'exception d'intérêt public (art. 31 alinéa 3 de la loi du 6 janvier 1978), il est formellement interdit aux enseignants « de mettre ou de conserver en mémoire informatique, ..., des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses » des élèves ou de leurs parents (art. 31 alinéa 1).
Pour les autres données nominatives, l'établissement scolaire doit déclarer son traitement à la Commission Nationale Informatique et libertés (CNIL) [www.cnil.fr], en précisant les données collectées, la finalité de la collecte et les conditions de stockage des informations.

Précisions :

Le projet français de transposition de la directive européenne n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données abandonne la distinction entre les traitements publics et privés, ne retenant que le seul critère de finalité pour évaluer le seuil de dangerosité nécessitant soit une simple déclaration (pour les traitements sans risques), soit une demande d'avis (pour les traitements plus sensibles). [art. 4 du projet de loi AN n°3250, adoptée en première lecture le 30 janvier 2002).

2.1.2- Le régime de la collecte des données

La collecte des données doit respecter un principe général de loyauté (interprétation a contrario de l'article 25 de la loi du 6 janvier 1978). C'est pourquoi l'établissement scolaire où le portfolio s'élabore, en tant que « responsable du fichier » à la charge d'informer les enfants, mais surtout leurs parents « du caractère obligatoire ou facultatif des réponses, des conséquences à leur égard d'un défaut de réponse, des personnes physiques ou morales destinataires des informations, de l'existence d'un droit d'accès et de rectification », voire d'opposition « en cas de cession à des tiers envisagée» (art. 26 de la loi du 6 janvier 1978).
Les parents doivent être informés de la collecte de données personnelles sur leurs enfants. Certaines informations doivent obligatoirement être fournies par les élèves comme leur nom. Par contre, la profession des parents est facultative, car cette information n'est pas nécessaire à la finalité du portfolio.
Notre conseil est donc de limiter la demande d'informations nominatives au strict minimum afin de minimiser le risque d'atteinte à la vie privée des élèves pouvant conduire à des poursuites judiciaires.
Les parents, au nom de leurs enfants, doivent aussi connaître les modalités du droit d'accès au traitement automatisé des données à caractère personnel (art. 34 de la loi du 6 janvier 1978). Concrètement, les parents doivent pouvoir obtenir auprès de l'établissement scolaire communication du contenu du portfolio concernant leur enfant. Le cas échéant, constatant le caractère inexact, incomplet, équivoque, périmé ou illégal des données contenues dans le portfolio, les parents peuvent « exiger que les données soient rectifiées, complétées, clarifiées, mises à jour ou effacées » (art. 36 de la loi du 6 janvier 1978).
Enfin si l'utilisation des données nominatives du portfolio va au-delà de la finalité initiale de suivi et d'évaluation, les parents sont en droit de s'y opposer (art. 26 de la loi du 6 janvier 1978).

2.1.3- Les conditions de conservation des données

La loi exige une durée de conservation des données à caractère personnel adaptée à la finalité du traitement. Dans notre cas, cela signifie que les données nominatives sur l'élève peuvent être conservées par l'établissement scolaire tant que cela est nécessaire à son suivi et à son évaluation. Lorsque l'enfant cesse d'être dans l'établissement, la conservation des données ne se justifie plus.
Enfin une obligation de sécurité pèse sur le responsable du traitement des données qui doit prendre toutes les précautions possibles pour sauvegarder la confidentialité des données collectées auprès des élèves.
Cela pose indirectement la question de la responsabilité du serveur qui héberge les portfolios.
Plusieurs situations se présentent :
L'établissement possède le serveur qui héberge les portfolios et assume l'obligation de sécurité. L'accès aux portfolios se fait par le biais du réseau local de l'école protégé contre les intrusions extérieures. Seules les personnes habilitées peuvent accéder au portfolio (l'enseignant, l'élève et le cas échéant le responsable de l'établissement scolaire).
L'hébergement des portfolios est confié à un tiers (SSII par ex.). Dans ce cas l'accès aux portfolios se fait par le biais d'un intranet ou de l'Internet. Il revient à l'établissement scolaire de déterminer les conditions d'hébergement des données sur le serveur extérieur à l'établissement afin de garantir la confidentialité des informations. Dans ce cas, le tiers hébergeur pourra être poursuivi s'il ne respecte pas les modalités techniques garantissant la sécurité quant aux portfolios.

2.2- Les atteintes aux droits d'auteur

Ici encore tout dépend des conditions d'accès aux portfolios. La question du droit d'auteur ne se pose pas dans les mêmes termes selon que les travaux d'un élève sont strictement limités à un nombre restreint de personnes ou au contraire largement diffusés sur le réseau.
- Dans le premier cas, si l'accès au portfolio est protégé par un mot de passe et sa consultation restreinte

à un cercle de personnes déterminé (l'élève, ses parents et l'enseignant par ex.), la communication des travaux de l'élève garde un caractère privé qui évite toute atteinte au droit d'auteur de l'élève.
- Dans le second cas, si les travaux de l'élève sont plus largement diffusés, il s'agit d'une communication publique. Dans ces conditions, en vertu du droit de représentation reconnu à l'élève en tant qu'auteur (art. L122-2 du CPI), ce dernier (ou ses parents) doit autoriser la mise en ligne de ses travaux scolaires. Cela ne pause généralement pas de problème particulier dans la mesure ou la diffusion des portfolios ne conduit à aucune rémunération.
Enfin dans tous les cas, comme lors de la réalisation de page Web, si l'élève intègre dans ses propres réalisations une partie importante d'une œuvre tierce protégée par le droit d'auteur (ex : texte pris sur un site Web), il doit obtenir l'autorisation de l'auteur.

2.3- Conseils

Les conditions d'accès aux portfolios sont la question centrale pour évaluer les risques courus. Un hébergement en réseau local fermé a l'avantage de limiter les risques d'atteintes à la vie privée et aux droits d'auteur, mais n'a sans doute pas le même intérêt pédagogique.
La diffusion en ligne permet une meilleure valorisation des potentialités du portfolio. Il faut pourtant s'interroger sur la nature des documents à diffuser. Mis à part le nom, les données nominatives sont à exclure comme les commentaires trop personnels d'évaluation de l'élève.

Une diffusion partielle du portfolio est donc recommandée, se limitant aux travaux illustrant une acquisition d'un savoir utile pour d'autres élèves.

3- Les références légales

- Art. 26 de la loi n° 78-17 du 6 janvier 1978 (Droit d'opposition au traitement des données).
- Art. 27 de la loi n° 78-17 du 6 janvier 1978 (Obligation d'information des conditions de traitement).
- Art. 34 de la loi n° 78-17 du 6 janvier 1978 (Droit d'accès à ces données personnelles).
- Art. 36 de la loi n° 78-17 du 6 janvier 1978(Droit de rectification de ces données personnelles).
- Art. L 111.1 du Code de propriété intellectuelle (reconnaissance du droit d'auteur).
- Art. L 121-1 du Code de propriété intellectuelle (prérogatives morales du droit d'auteur).
- Art. L 122-1 du Code de propriété intellectuelle (prérogatives patrimoniales).
- Art. L 123-2 du Code de propriété intellectuelle (durée de la protection, domaine public).
- Art. L 335-3 du Code de propriété intellectuelle (Délit de contrefaçon)

4- Liens utiles

- [www.cnil.fr] Voir l'espace junior qui informe les enfants de leurs droits et des risques liés à l'usage de l'Internet et l'espace déclaration qui permet en ligne de déclarer le traitement de données nominatives sur le site Web.

Les sondages

1- Définition technique et pratique

Les sondages sont « des enquêtes visant à déterminer la répartition des opinions sur une question, dans une population donnée, en recueillant des réponses individuelles manifestant ces opinions ».
Plus que des sondages organisés par une classe, la situation la plus fréquente est le fait que les élèves soient amenés à répondre à des sondages afin de pouvoir accéder à certaines pages web utiles à leur recherche, lors d'utilisation de l'Internet. De nombreux sites web offrant une richesse d'informations régulièrement mises à jour sur des sujets variés ou très spécialisés désirent en échange collecter le plus d'informations possibles concernant les habitudes des internautes qui consultent leurs sites, soit pour mieux les satisfaire, soit pour vendre ces informations à des entreprises intéressées, soit les deux à la fois.

Pour les élèves, répondre à des sondages peut sembler relever du jeu. Participer à un sondage reste toujours une démarche volontaire qui pourtant est susceptible de réserver des écueils. Il est donc du devoir du personnel éducatif encadrant les élèves de les préserver du risque en prenant quelques précautions.

2- Les points de vigilance

Pour les sites web, l'intérêt de réaliser un sondage est souvent la possibilité de collecter, traiter et conserver des renseignements personnels sur les internautes qui les consultent.
Sur ce point il est utile de se reporter à l'étude des droits des personnes fichées reconnus par la loi du 6

janvier 1978 (voir fiche n°20).

Remarque

C'est pourquoi **le milieu scolaire doit s'assurer que les règles légales de protection des données personnelles sont respectées par les sites sur lesquels les élèves sont sondés.**

Les agendas

1- Définition technique et pratique

Sur le réseau local ou sur le site des établissements scolaires, les enseignants peuvent mettre en place un agenda qui affiche l'emploi du temps des différentes classes avec le nom de l'enseignant, la matière enseignée et le numéro de salle. De prime abord, cela paraît assez anodin. La mise en ligne de ce type d'informations n'est pourtant pas sans conséquence.

2- Les points de vigilance

Grâce à l'Internet, le partage d'information touche un nombre plus important que lorsque l'agenda reste sous un format papier. Cela signifie qu'au-delà du cercle scolaire strictement concerné par les horaires et les lieux affichés, des personnes peuvent être amenées à connaître l'emploi du temps d'enseignants.
Plus les informations seront facilement accessibles, plus les risques d'atteinte à la vie privée seront conséquents.
Il n'est pas certain qu'il soit très utile que quiconque sache le nom et l'emploi du temps des enseignants d'un établissement. En revanche, il est tout à fait intéressant que l'ensemble du personnel d'un établissement scolaire puisse savoir facilement les salles disponibles ou les enseignants en cours pour une meilleure coordination des différentes activités.

Conseils :

Au même titre que les annuaires mis en ligne, **il est recommandé d'informer les enseignants** concernés par le projet de mise en ligne, voire d'obtenir auprès d'eux l'autorisation de diffuser en ligne leur emploi du temps.
De plus, il est conseillé de limiter l'**accès à l'agenda**.

3- Les références légales

- Art. 26 de la loi n° 78-17 du 6 janvier 1978 (Droit d'opposition au traitement des données).
- Art. 27 de la loi n° 78-17 du 6 janvier 1978 (Obligation d'information des conditions de traitement).
- Art. 34 de la loi n° 78-17 du 6 janvier 1978 (Droit d'accès à ces données personnelles).
- Art. 36 de la loi n° 78-17 du 6 janvier 1978 (Droit de rectification de ces données personnelles).

La vidéoconférence

1- Définition technique et pratique

La vidéoconférence est « une conférence qui permet à ses participants de pouvoir se voir réciproquement, grâce à l'utilisation de caméras et d'écrans qu'on installe pour la transmission des images ». Bien qu'en des lieux distants, par le biais de la vidéoconférence, des personnes peuvent dialoguer en direct en se voyant. A la parole, s'ajoutent les gestes, les mimiques ou les expressions du visages des participants, ce qui accentue le contact humain.
Plus qu'une simple communication téléphonique, la vidéoconférence est donc un outil idéal pour les activités de télécollaboration de courte durée mais intenses. Peuvent ainsi être organisées des rencontres virtuelles où des classes ou des groupes d'élèves ont la possibilité de s'entretenir avec un invité dont les compétences reconnues peuvent être utiles à leur apprentissage. Dans des domaines les plus variés, des sciences exactes au sciences humaines, en passant par la littérature ou la musique, il peut s'agir de

professeurs, d'experts, de scientifiques, d'écrivains ou d'artistes qui peuvent ainsi apporter un éclairage nouveau à des notions ou des concepts abordés en classe précédemment. Bref, l'entretien avec le spécialiste est l'occasion unique pour les élèves d'approfondir leurs connaissances.
Sont désormais disponibles des outils logiciels permettant des vidéoconférences au moyen du protocole Internet (IP). Les coûts de communication sont ainsi devenus faibles rendant la vidéoconférence abordable à un plus large public. Plus que le son et l'image, le protocole Internet permet en même temps de transférer des fichiers, de partager des applications, de réaliser à distance des démonstrations sur un tableau électronique ou numérique et d'envoyer des messages.
Il existe plusieurs types de vidéoconférences :

1.1- Les vidéoconférences en mode point à point

Les premières sont point à point car elles ne mettent en liaison qu'un invité et une classe, par exemple, présents en deux lieux différents seulement.

1.2- Les vidéoconférences en mode multipoint

Les secondes sont en mode multipoint . Grâce à un serveur MCU (Multipoint Control Unit), plusieurs participants situés en différents lieux peuvent participer à une même vidéo conférence, par exemple des classes de plusieurs établissements scolaires qui communiquent en mode horizontal. La vidéoconférence crée ainsi une grande classe virtuelle. Pour information un mot de passe protège l'accès à ce type de vidéoconférence.

1.3- Les vidéoconférences de type Mbone

Les dernières sont de type Mbone. A la différence des deux premiers types de vidéoconférences, la communication n'est pas interactive. Il n'y a qu'un seul émetteur (l'invité) et une multitude de destinataires internautes qui captent la conférence par le réseau. Cela est idéal pour les cours donnés en ligne.
Selon les situations, les risques d'atteinte à l'image des personnes et de contrefaçon sont plus ou moins importants.

2- LES POINTS DE VIGILANCE

2.1- Les atteintes à l'image des personnes

Deux situations doivent être distinguées.

2.1.1- La diffusion en direct de la vidéoconférence

Si la vidéoconférence est seulement captée en direct par les différents participants, nous sommes dans un cadre comparable à celui d'un débat ou d'un dialogue. L''image des participants, en l'occurrence les élèves, leurs enseignants et l'invité, ne subit alors aucune atteinte.

2.1.2- L'enregistrement de la vidéoconférence

En revanche, si la vidéoconférence est enregistrée et diffusée en différé sur l'Internet, il y a communication au public. Dans ce cas, la diffusion sur l'Internet nécessite le consentement des participants dont l'image apparaît clairement dans la vidéoconférence.

2.2 - Les atteintes aux droits d'auteur

La vidéoconférence est diffusée en direct sur l'Internet ou en différé suite à un enregistrement sur un support numérique. La diffusion concerne souvent le cours ou la conférence d'un spécialiste, ou un débat animé et instructif. Dans ces deux cas, la vidéoconférence est une œuvre protégée dont il faut déterminer les auteurs avant de leur reconnaître des droits.
Dans le cadre des vidéoconférences point à point ou multipoint les auteurs sont représentés par l'ensemble des participants qui ont contribué à animer le débat tant par leurs questions que leurs réponses.
Par contre, dans la vidéoconférence de type Mbone, seul l'émetteur est l'auteur de la vidéoconférence (par hypothèse l'invité expert ou spécialiste).
Dans tous les cas, la diffusion sur l'Internet de la vidéoconférence suppose de la part du ou des auteur(s) l'exercice de leur droit de représentation (art. L 122-2 du CPI). Cela signifie qu'ils doivent préalablement autoriser la diffusion. Dans le cas contraire, les auteurs peuvent poursuivre en contrefaçon toute personne qui diffuse leur vidéoconférence sans leur autorisation écrite (art. L 335-3 du CPI).

3- LES RÉFÉRENCES LÉGALES

- Art. L 122-2 du Code de propriété intellectuelle (Droit de représentation)
- Art. L 131-2 du code de propriété intellectuelle (Autorisation par écrit).
- Art. L 335-3 du Code de propriété intellectuelle (Délit de contrefaçon)

L'échange et le partage de fichiers

1- Définition technique et pratique

L'Internet, par ces différents protocoles de communication, facilite l'échange et le partage de fichiers. De tels échanges sont un attrait majeur dans la constitution d'un réseau local au sein de l'établissement scolaire ou la connexion à un réseau ouvert. Dans l'intérêt des élèves, la circulation du savoir est ainsi facilitée.

Ceci dit, le partage de fichiers n'est pas sans risque. L'acte d'échange en lui-même n'est pas à remettre en cause. Au contraire, c'est par le partage que l'Internet, en particulier éducatif, a plus de chance de se développer. Mais seuls les contenus conformes aux principes du milieu scolaire sont à échanger sans risques.

2- Les points de vigilance

Tout dépend du contenu des fichiers échangés qui peuvent soit porter préjudice aux personnes, soit porter atteinte au droit d'auteur, voire à l'ordre public.

2.1- Les atteintes aux droits de la personne

Par le biais d'échange de fichiers, des contenus injurieux ou portant atteinte à l'intimité ou à la réputation des personnes peuvent être propagés. Nous sommes ici dans le même cas de figure que pour le courrier électronique ou le clavardage (chat) auxquels on peut utilement se reporter pour connaître le détail des risques identiques (voir fiches n° 12 et 13). Le respect des personnes exige des enseignants comme des élèves de ne pas divulguer d'informations intimes ou de ne pas rompre le secret de la correspondance privée, de ne pas injurier ou de tenir des propos racistes.

2.2- Les atteintes aux droits d'auteur

L'échange de fichiers est admis, voire incité pour des travaux d'élèves ou des contenus pédagogiques dont les auteurs ont autorisé l'utilisation. Par contre, il est interdit au sein du milieu scolaire d'utiliser le réseau pour échanger des œuvres musicales, audiovisuelles, littéraires ou logicielles sans l'autorisation de leur auteur. Le matériel informatique des établissements scolaires n'est pas à la disposition des élèves et des enseignants pour échanger et graver des copies pirates de logiciels, d'albums ou de films. De tels agissements peuvent être poursuivis pour contrefaçon (voir fiche n° 19).

2.3- Les atteintes à l'ordre public

Les règles d'ordre public interdisent la diffusion de contenus à caractère raciste, antisémite ou pédophile et protège les mineurs des contenus à caractère violent ou pornographique. De tels contenus sont donc prohibés dans le cadre d'échange ou de partage de fichiers.

3- Les références légales

- Article 226- 1 du Code pénal (Atteinte à la vie privée)
- Article 227-23 du Code pénal (Diffusion d'images à caractère pédophile)
- Article 227-24 du Code pénal (Protection des mineurs contre les contenus violents ou pornographiques)
- Article R 621-2 du Code pénal (injure non publique)
- Articles 24 et 26 bis de la loi du 29 juillet 1881 (Diffusion de contenus à caractère raciste ou antisémite).
- Article 29 de la loi du 29 juillet 1881 (Diffamation)
- Art. L 122-2 du Code de propriété intellectuelle (Droit de représentation)
- Art. L 131-2 du code de propriété intellectuelle (Autorisation par écrit).
- Art. L 335-3 du Code de propriété intellectuelle (Délit de contrefaçon)

Les outils poste à poste

1- DÉFINITION TECHNIQUE ET PRATIQUE

Jusqu'à maintenant, tous les services de messagerie ou d'information étudiés dans les fiches précédentes fonctionnent avec une architecture du réseau client / serveur. A titre d'illustration, le réseau local d'un établissement scolaire est organisé autour d'un ordinateur central (le serveur) auquel tous les autres ordinateurs de l'établissement (les clients) sont connectés. Cela signifie que sous une architecture **client / serveur**, toutes les requêtes envoyées sur le réseau par les élèves ou leurs enseignants sur leur ordinateur sont exécutées par le serveur qui centralise l'envoi et la réception de courrier électronique ou la réception de page web entre autres. Passage obligé entre les « clients » et l'Internet, le serveur distribue les données reçues et envoyées auprès de chaque ordinateur connecté à lui et destinataire ou expéditeur des données.

Les outils poste à poste ou « peer to peer » (P2P) bouleversent cette architecture centralisée du réseau, le rendant moins contrôlable par les administrateurs en charge du suivi technique des serveurs. Avec les outils poste à poste, il n'existe plus de hiérarchie entre les machines connectées. C'est pourquoi l'on parle d'architecture d'égal à égal ou d'échange de pair à pair. Cette fois-ci, les ordinateurs anciennement clients agissent à la fois comme clients et comme serveurs. Sans l'aide d'un serveur centralisé, les internautes communiquent entre eux ou transfèrent des fichiers directement de leurs postes respectifs.

On distingue deux modèles d'architecture poste à poste :

1.1- Le modèle poste à poste dit hybride ou assisté

Le premier est dit assisté ou hybride et a été popularisé par le site d'échange musical Napster. Equipés du même logiciel poste à poste (par ex. : Napster), tous les ordinateurs souhaitant partager directement leurs ressources se connectent à un serveur central. Mais à la différence du serveur « classique », ici le serveur n'exécute pas des commandes de transfert, mais se limite à un rôle d'indexation des ordinateurs connectés et des fichiers disponibles. Concrètement, sa machine connectée au serveur, l'internaute qui recherche un fichier particulier (un texte, une photographie, etc.) interroge la base de données du serveur qui lui transmet la liste des ordinateurs connectés au réseau qui possèdent le fichier recherché. L'internaute n'a plus qu'à activer l'hyperlien qui renvoie directement sur l'ordinateur sélectionné et le téléchargement se fait directement d'ordinateur à ordinateur sans transiter par le serveur. Ce dernier permet juste de centraliser l'information sur les ressources disponibles dans les disques durs des ordinateurs connectés au serveur.

1.2- Le modèle poste à poste dit pur ou natif

Le deuxième modèle d'architecture poste à poste est dit pur ou natif. Utilisant le même logiciel poste à poste (par ex : Gnutella ou Freenet), les internautes peuvent s'échanger directement des fichiers sans l'aide préalable d'un serveur. Ici, le poste informatique de l'internaute est totalement autonome et cumule les fonctions de client, serveur et moteur de recherche. Concrètement, lorsqu'une recherche est lancée par un internaute via le logiciel Gnutella par exemple, la requête est envoyée à tous les ordinateurs connectés sur l'Internet et possédant le même logiciel poste à poste. Chacun des ordinateurs laisse donc libre accès à son disque dur et lorsque le fichier recherché est localisé sur l'un d'eux, automatiquement ce dernier le transfère à celui qui le réclame. Ce modèle d'architecture du réseau est donc totalement décentralisée.

1.3- L'intérêt éducatif de l'architecture technique poste à poste

Plus que le simple échange d'images, de vidéos ou de musiques, le modèle poste à poste permet une véritable collaboration entre ordinateurs. Grâce à des logiciels poste à poste, plusieurs classes de différents établissements scolaires, sans l'aide d'un serveur, peuvent ainsi facilement partager leurs ressources, créer des espaces de travail virtuels basés sur des outils tels que le calendrier, le partage de fichiers, la messagerie instantanée ou vocale (V. GrooveNetwork par ex.).

Les outils poste à poste présentent donc de nombreux intérêts pour le milieu scolaire, mais leur utilisation doit être strictement encadrée afin d'empêcher une utilisation illicite de l'Internet ou de protéger les élèves de certains risques.

2- LES POINTS DE VIGILANCE

2.1- Les atteintes à la vie privée

Dans une architecture poste à poste, par hypothèse, les ordinateurs connectés laissent libre accès à leurs

ressources. Il existe donc des risques plus importants d'intrusion sur les postes où des données personnelles contenues dans certains fichiers peuvent être détournées. Les enseignants, ou plus largement l'encadrement éducatif, doivent mettre en garde leurs élèves contre ce type de risques.

2.2- L'accès à des contenus pornographiques

Plus encore que par la navigation sur le Web, les outils poste à poste tels que Gnutella permettent aux enfants ou aux adolescents de accéder facilement à du matériel à caractère pornographique. Pour information, bien avant le piratage musical, des outils comme Gnutella ou Freenet ont pour principale finalité l'échange de milliers d'images ou de vidéos à caractère pornographique.
Effectuant une simple recherche avec des mots-clés basiques, le mineur peut facilement accéder à de nombreux fichiers téléchargeables librement. A la différence de certains sites web, aucune restriction d'accès ou vérification de l'âge par l'intermédiaire de la carte bancaire n'est effectuée. Les filtres parentaux les plus utilisés ne bloquent ce type de téléchargement de poste à poste.
Enfin même involontairement, un mineur peut également accéder à du contenu pornographique en effectuant une recherche sur un tout autre domaine. L'exemple donné par une étude de la chambre des représentants des Etats-Unis est éloquent. 70 % des résultats à la recherche concernant « Britney Spears » correspondent à des fichiers à caractère pornographique.

2.3- Les atteintes aux droits d'auteur

Objet de poursuites judiciaires par l'industrie du disque, les utilisateurs d'outils poste à poste, tels que Napster par exemple, étaient connus pour reproduire des œuvres musicales sans l'autorisation des artistes. Napster a d'ailleurs été condamné par la justice américaine. Racheté par la société d'édition Berstelmann, le site Napster propose désormais un abonnement. Mais d'autres sites proposent l'échange gratuit et illégal de fichiers musicaux.
Ces pratiques illicites posent **le problème du délit de contrefaçon** et plus généralement de l'obligation de respecter les règles de droit d'auteur (voir fiche n°19).

Conseils :

Face à tant de risques, il est recommandé aux établissements scolaires d'interdire l'usage de logiciels tels que Gnutella ou Freenet, car les risques d'usage illicite effectué par les élèves sont trop importants. De plus, la majorité des contenus échangés par ce type d'outils poste à poste ne sont pas très utiles d'un point de vue pédagogique.

3- Références légales

- Art. L 111.1 du Code de propriété intellectuelle (reconnaissance du droit d'auteur).
- Art. L 121-1 du Code de propriété intellectuelle (prérogatives morales du droit d'auteur).
- Art. L 122-1 du Code de propriété intellectuelle (prérogatives patrimoniales).
- Art. L 123-2 du Code de propriété intellectuelle (durée de la protection, domaine public).
- Art. L 131-2 du code de propriété intellectuelle (Autorisation par écrit).
- Art. L 335-3 du Code de propriété intellectuelle (Délit de contrefaçon)
- Art. L 323- 1 et s. du Code pénal (Délits informatiques, intrusion, virus…)
- Article 227-23 du Code pénal (diffusion prohibée d'images à caractère pédophile)
- Article 227-24 du Code pénal (protection des mineurs contre les contenus violents ou pornographiques)

Le développement d'outils logiciels

1- Définition technique et pratique

Au sein des établissements scolaires, cette activité n'est certes pas courante. Ceci dit, elle est envisageable et utile dans les classes spécialisées (Baccalauréat technique par ex.). Mettant en pratique leurs connaissances en matière de langage informatique, des élèves peuvent programmer des logiciels, créer des moteurs de recherche ou des bases de données. Le cas échéant, les meilleurs travaux peuvent être sélectionnés et utilisés par les lycées ou les collèges...
Les établissements scolaires peuvent aussi faire développer des outils spécifiques par des sociétés informatiques (SSII), afin de mieux répondre aux besoins spécifiques du milieu éducatif.

2- Les points de vigilance

Le développement d'outils logiciels ne pose que des questions de protection de la création.
Sauf exceptions dans l'enseignement supérieur, les projets de développement d'outils logiciels menés par les élèves et encadrés par leurs enseignants restent d'un enjeu limité. Cela n'a pas la même portée économique ou financière que le développement de logiciels par des SSII.

2.1- Le développement de logiciels au sein des établissements scolaires

La question de la protection se pose avec moins d' acuité dans le premier cas que dans le second. Ceci dit, quelque soit l'enjeu économique, les créations logicielles sont toujours protégées ; les élèves, leurs enseignants comme l'établissement scolaire doivent tout mettre en œuvre pour assurer cette protection.

Depuis la loi du 3 juillet 1985, le logiciel connaît un régime dérogatoire du droit commun. Confirmant la position de 1985, la loi du 10 mai 1994 transposant la directive n° 91/250/CE du 14 mai 1994 concernant la protection juridique des programmes d'ordinateur pose le principe de la dévolution des droits patrimoniaux au bénéfice de l'employeur (l'Etat). Autrement dit, sauf clauses contraires, grâce au mécanisme de la présomption légale de cession, l'Etat représenté par l'établissement scolaire est titulaire des droits d'exploitation sur les programmes d'ordinateur créés par les enseignants et leurs classes dans le cadre de l'activité scolaire avec les moyens informatiques de l'établissement scolaire. Par contre les droits moraux restent sur la tête des auteurs. Les noms des élèves ou de l'enseignant qui ont créé le logiciel doivent être mentionnés.

L'article L113-9 du CPI est très clair :

Son alinéa 1 dispose que « sauf dispositions statutaires ou stipulations contraires, les droits patrimoniaux sur les logiciels et leur documentation créés par un ou plusieurs employés dans l'exercice de ses fonctions ou d'après les instructions de leur employeur sont dévolus à l'employeur qui est seul habilité à les exercer ».
L'alinéa 3 précise que ses dispositions s'étendent « aux agents de l'Etat, des collectivités publiques et des établissements publics à caractère administratif ».
A titre d'information, le décret du 2 octobre 1996 prévoit au bénéfice de certains fonctionnaires et agents de l'Etat et ses établissements publics ayant participé à la création d'un logiciel un complément de rémunération égal à 25% des produits tirés de la création, après déduction des frais supportés par la personne publique.

2.2- Le développement de logiciels par une société de services et d'ingénierie informatique (SSII)

Selon l'importance «stratégique » du logiciel, l'établissement scolaire peut opter pour une simple licence d'utilisation du logiciel ou au contraire négocier une totale maîtrise du logiciel en demandant les codes sources et la titularité des droits patrimoniaux.

3- Références légales.

- Art. L 113-9 du Code de propriété intellectuelle (Dévolution des droits patrimoniaux à l'employeur).

L'utilisation et le développement de logiciels issus de l'Open Source

1- Définition technique et pratique

L'Open Source est le nom donné à leur mouvement en 1998 par les acteurs du logiciel libre. Fruit de la mouvance libertaire de l'Internet, les bases de l'Open Source ont été jetées en 1984 par Richard Stallman avec son projet GNU (GNU's not Unix). Ce projet consistait à créer un système d'exploitation aussi performant qu'Unix et complètement compatible avec lui. Est ainsi né le premier système d'exploitation dit « libre », car son utilisation, sa copie, sa redistribution voire sa modification étaient laissées au libre arbitre de l'utilisateur.
Sous le nom d'Open Source, sont fédérées **toutes les expériences d'accès libre au code source des logiciels**.

1.1- Les principes de l'Open Source

En réaction au monopole d'exploitation reconnu par le droit d'auteur ou le Copyright, la finalité de l'Open source est la promotion du savoir et sa diffusion auprès d'un public le large possible. Il est proposé aux

internautes utilisant et développant les logiciels issus de l'Open Source de créer un fonds commun de logiciels en ligne. Concrètement, l'utilisation de logiciels issus de l'Open Source permet le libre accès au code source du logiciel, sa copie et sa libre redistribution.

1.2- Les conditions d'utilisation

Afin de développer à un moindre coût un projet informatique, des élèves et leur enseignant peuvent utiliser des logiciels « Open Source », les modifier ou les améliorer afin de les adapter à leurs besoins. En revanche, les améliorations effectuées sur le logiciel initial doivent être versées dans le fond commun mis en ligne. Il est possible de puiser gratuitement dans le fond des logiciels libres, à condition qu'à son tour on enrichisse le fond de ses améliorations en permettant à d'autres de les exploiter gratuitement...

2- Les points de vigilance

En utilisant des logiciels issus de l'Open source, les élèves comme leurs enseignants doivent avoir conscience des conditions d'utilisation particulières de ce type de logiciel. Cela permet d'avoir des outils logiciels performants à moindre coût, mais son apport dans l'amélioration du logiciel n'est nullement protégé. Il faut au contraire le mettre en libre accès en rappelant sur le site de téléchargement du logiciel les principes de l'Open Source.

Conseils :

Il est donc **déconseillé** d'utiliser ce type de logiciel si les élèves, leurs enseignants, voire l'établissement scolaire
souhaitent **garder un monopole d'utilisation** des travaux de développement du logiciel libre. Les principes de l'Open Source obligent les développeurs à garantir un accès libre aux améliorations du code source du logiciel libre.

L'utilisation de contenus issus de l'Open Content

1- Définition technique et pratique

Dans le prolongement du mouvement Open Source qui concernait que les logiciels, l'Open Content reprend les mêmes principes de libre accès à la connaissance en l'appliquant cette fois à tout type de contenus en ligne (content). Sur l'Internet, des auteurs mettent en libre accès leurs créations musicales, photographiques, littéraires, etc. ...
Ils choisissent ainsi de contribuer à l'enrichissement d'un fonds commun de savoir mis en ligne.
Lors de l'élaboration d'un site web ou de tout autre travail, les élèves ou les enseignants peuvent utilement puiser dans ce fonds et intégrer ces contenus issus de l'Open Content dans leurs propres travaux. Enfin, à leur tour, les élèves et leurs enseignants peuvent aussi verser leurs propres travaux dans le fonds commun de l'Open Content. Il faut pourtant garder à l'esprit quelques règles à respecter.

2- Les points de vigilance

L'Open Content est un choix conscient et maîtrisé par l'auteur, comme le démontrent les licences d'utilisation de ce type de «contenus libres». Les conditions d'utilisation sont claires.

2.1- Les prérogatives morales

Tout d'abord, les licences sont l'occasion de rappeler aux futurs utilisateurs, élèves et enseignants les prérogatives morales de l'auteur : le respect de la paternité et de l'intégrité de l'œuvre. En utilisant ces contenus, le nom de l'auteur doit être mentionné et aucune modification à l'œuvre originale doit être apportée sauf si elle est mentionnée avec l'accord de l'auteur.

2.2- Les prérogatives patrimoniales

De même, la licence précise les conditions d'exercice des prérogatives patrimoniales de l'auteur : les droits de reproduction et de représentation. Sur ces points, selon le principe de libre accès, la licence permet la copie et la redistribution de l'œuvre à condition que les copies soient faites dans une finalité non commerciale. Il s'agit d'une cession à titre gratuit limitée. Les contenus issus de l'Open Content peuvent donc être utilisés sans restriction dans le cadre de l'activité scolaire à la condition de respecter les

prérogatives morales des auteurs initiaux et en rappelant sur les pages où se trouvent les contenus « libres » les conditions des licences « Open Content ».

Conseil :

Il est par contre **déconseillé** au milieu scolaire d'utiliser ce type de contenus si on envisage de valoriser ses travaux en s'associant avec un partenaire privé **pour une exploitation commerciale**.

La prise en charge des activités en ligne

Ni la connaissance des risques généraux liés aux différents services, ni celle des responsabilités des différents acteurs ne suffisent pour gérer pleinement l'Internet en milieu scolaire.
Les acteurs de l'Internet scolaire doivent être capables de combiner les différentes responsabilités en jeu aux véritables risques courus. Il s'agit donc d'élaborer une charte d'utilisation de l'Internet adaptée à l'établissement scolaire, c'est-à-dire aux contextes d'utilisation et aux véritables risques que les activités en ligne engagent.
Suite aux deux premières parties de ce guide qui présentent tant **les responsabilités des acteurs** (fiches n° 2 à 11) que **les caractéristiques des services en ligne et les points de vigilance** (fiches n° 12 à 28), cette troisième partie propose une démarche à suivre pour prendre en charge les activités en ligne en milieu scolaire.
Cette démarche comprend **trois étapes** qui seront l'objet des prochaines fiches :

1- Première étape : analyse

Premièrement l'analyse préliminaire de l'environnement à réguler. Dans ce but, le guide propose aux participants à l'utilisation de l'Internet en milieu scolaire de répondre à des grilles de questions (fiche n°30).

2- Seconde étape : élaboration et adoption

Deuxièmement, prise en charge des risques identifiés en élaborant une charte d'utilisation d'Internet. A cet effet, le guide donne des conseils quant à la mise en place du processus d'élaboration et offre des exemples de clauses et d'autorisations (fiches n°31, 32 et 33).

3- Dernière étape : sanction et révision

Troisièmement, la charte une fois adoptée, l'établissement scolaire doit s'assurer de son respect. Il s'agit donc de mettre en place un processus de sanction en cas de non-respect et de révision lorsque les règles deviennent obsolètes face à l'évolution des activités en ligne (fiche n° 34).

L'analyse préliminaire de l'environnement

Le guide propose des grilles de questions pour situer les caractéristiques des intervenants et des activités et déterminer les risques inhérents aux outils de communication. Cette première fiche se limite aux caractéristiques des personnes utilisant l'Internet en milieu scolaire et des activités en ligne. La détermination des risques d'atteintes aux droits des personnes, aux droits d'auteur ou à l'ordre public est l'objet de la fiche suivante.
Il s'agit de la première étape d'évaluation des risques qui doit conduire les acteurs, à la fin du processus, à élaborer des règles pour prendre en charge ces risques identifiés.

1- Profil des utilisateurs de l'Internet en milieu scolaire

Les risques liés à l'utilisation de l'Internet dans un établissement scolaire changent selon l'âge, le degré de maturité ou la familiarité avec les outils logiciels des utilisateurs. Les usages de l'Internet en école primaire, au collège ou au lycée conduisent à des situations de vulnérabilité ou de dérives diverses, appelant des règles différentes. C'est pourquoi il est important que des personnes responsables d'évaluent les risques selon les caractéristiques des participants par le biais des questions suivantes.
Evaluation des risques selon les caractéristiques des utilisateurs.

- A quelle tranche d'âge les activités en ligne sont-elles proposées ? A des enfants âgés de moins de 6 ans (préscolaire), de 6 ans à 10 ans (primaire), à des préadolescents de 11 à 14 ans (collège), à des adolescents de 15 à 17 ans (lycée), voire à des majeurs ?
- A âge identique, certains utilisateurs sont-ils plus vulnérables que d'autres ? De quelle manière ?
- Existent -ils des obstacles rendant plus difficile la participation de certains élèves à des activités en ligne (problèmes de niveau scolaire, de discipline...) ?
- A quel point les utilisateurs connaissent-ils le maniements des logiciels nécessaires aux activités en ligne ? Totalement ignorants, au début de l'apprentissage, autonomes, expérimentés, ... ?
- A quel point les utilisateurs sont-ils informés des enjeux et des risques liés aux activités en ligne ? Jamais informés auparavant ou suivent-ils la préparation en vue du B2i, ont-ils passé avec succès le B2i, suivent- ils des cours supplémentaires en complément du B2I ?
- Certains utilisateurs ont-ils déjà utilisé l'Internet chez eux ? Episodiquement ou régulièrement ?
- Dans le cadre des activités en ligne, les utilisateurs se connaissent-ils tous ?
- Est-ce que les activités en ligne conduiront les utilisateurs à communiquer au sein d'un même groupe ou avec des personnes étrangères, mineures ou majeures ?

2- Profil des activités en ligne présentes au sein de l'établissement scolaire

Certaines activités en ligne appellent plus de précautions que d'autres. Il existe des situations qui exigent toujours un encadrement normatif. En revanche, pour d'autres, il peut être possible de s'en remettre au libre arbitre des utilisateurs.

Évaluation des risques selon l'activité en ligne

- Quels sont les thèmes abordés lors des activités en ligne ? Certains sont-ils controversés ou impliquent-ils des révélations d'ordre personnel, familial ou intime de la part des participants ?
- Quelles sont les activités où les participants sont anonymes ?
- Quelles sont les activités où les participants sont identifiés ?
- Les participants ont-ils la possibilité de communiquer en temps réel ou sont-ils toujours en temps différé ?
- Existe-il une surveillance des activités en ligne ? Par qui et avec quels moyens ?
- Existe-il une modération des activités en ligne ? Pour quels types d'activités et par qui ?
- L'activité en ligne se déroule-t-elle toujours dans les locaux de l'établissement scolaire ou peut-elle être effectuée à l'extérieur (domicile de l'élève par ex.) ?
- Le serveur se trouve-t-il sous l'autorité de l'établissement scolaire, si non, auprès d'un organisme public ou privé sous contrat ?
- Lors des activités, les élèves peuvent-ils passer d'un contexte privé à un contexte public et inversement ?
- Un archivage est-il mis en place ? Pour quel type d'activités et de documents ?
- Qui accède aux activités en ligne et par quels moyens (mots de passe, ...) ?
- Certaines activités en ligne impliquent-elles la création de documents ? Quels types de matériel sont utilisés (domaine public, protégé par le droit d'auteur, open source, open content) ? Sous quelles formes (photos, vidéos, sons, textes, extraits) ?

Une fois le profil des participants et des activités en ligne réalisé, il est possible d'affiner l'analyse en déterminant quels risques fait courir l'Internet en milieu scolaire en matière d'atteintes aux droits des personnes, d'atteintes aux droits d'auteur ou d'atteintes à l'ordre public.

3- Les risques d'atteintes aux droits des personnes

L'utilisation de services de messagerie ou de diffusion d'informations comporte de nombreux risques pour les personnes. Déjà étudiés dans les fiches précédentes, il s'agit :

- des atteintes à l'intimité
- des atteintes au droit à l'image
- des atteintes à la réputation
- du non-respect des règles protectrices des données à caractère personnel
- du harcèlement et des menaces
- de l'envoi de messages non sollicités (spamming ou pourriel).

Questions à se poser pour évaluer les risques pour les personnes

- Les informations révélées portent-elles sur une matière habituellement considérée comme relevant de l'intimité ? Si oui, la personne concernée a-t-elle consenti ?
- La diffusion au public lors d'activités en ligne comporte-t-elle des images de personnes prises dans des lieux privés ? Si oui, ont-elles consenti à cette diffusion ?
- Les propos sont-ils une expression légitime de l'opinion que l'on a sur la personne ?

- Les faits mentionnés sont-ils vérifiables ?
- Les activités en ligne donnent-elles lieu à la collecte et au traitement de données à caractère personnel ? Si oui, quelles autorisations ont été obtenues à l'égard de ces renseignements ? Quelles sont les conditions d'exercice du droit d'accès et de rectification des personnes concernées ?
- Un même auteur peut-il envoyer une multiplicité de messages à une même personne ? Si oui, ces messages ont-ils toujours la même teneur (commentaires relatifs au sexe, à la race, à la nationalité, à un produit à acheter ?
- Quelle réaction a la personne qui reçoit les messages ? Consent-elle à la réception de ces messages ou souhaite-t-elle que cela cesse ?

4- Les risques d'atteintes aux droits d'auteur

Lors d'activités d'échanges ou de diffusion en ligne, les élèves peuvent utiliser des œuvres sans l'autorisation du titulaire des droits d'auteur. Des risques de violation du droit d'auteur existent.

Les autorisations à obtenir

En principe pour diffuser une œuvre sur un site ou en pièce jointe à un message, il faut obtenir l'autorisation écrite de l'auteur de l'œuvre (art. L 131-2 du Code de propriété intellectuelle). Tel est le cas pour les créations d'élèves par exemple. Pour des œuvres exploitées commercialement, la situation est souvent différente. Pour que son œuvre connaisse un public, l'auteur a souvent cédé par contrat ses droits patrimoniaux à un éditeur (livres) ou à un producteur (films ou musiques). C'est donc auprès d'eux qu'il faut obtenir l'autorisation d'exploitation de l'œuvre, à la condition que le contrat de cession des droits conclu avec l'auteur ait prévu explicitement la diffusion sur l'Internet. Dans le cas contraire, il faut se retourner vers l'auteur ou les ayants droits (héritiers) si l'auteur est décédé.

Dernier cas de figure, l'auteur peut avoir confié la gestion de ses droits patrimoniaux à une société de gestion collective. Mandatée par l'auteur, elle peut autoriser l'exploitation de l'œuvre en milieu scolaire (voir fiche n° 32 pour les modèles de demande d'autorisation).

Les questions à se poser pour évaluer les risques pour le droit d'auteur

- Lors des activités en ligne, est-il envisagé d'utiliser des contenus protégés par le droit d'auteur ?
- Si non, l'œuvre est-elle tombée dans le domaine public ou issue de l'Open source ou de l'Open content ?
- Si oui, connaît-on le ou les auteur(s) ?
- Avons-nous obtenu une cession de droits ou une autorisation de diffusion de l'œuvre ?

5- Les risques d'atteinte à l'ordre public

Il s'agit ici de prévenir les risques de violation des règles d'ordre public visant à protéger tant la société que les mineurs en raison de leur vulnérabilité.

Il faut évaluer les possibles dérives dans les contenus échangés ou diffusés à travers les outils de communication sur l'Internet.

Plusieurs types de propos interdits légalement ne doivent pas se retrouver dans les activités en ligne en milieu scolaire.

- les contenus à **caractère raciste ou antisémite**, c'est-à-dire discriminatoire envers certaines personnes en vertu de leur seule appartenance ethnique ou religieuse ou de leur couleur de peau. Le respect de la personne humaine, valeur promue par l'école, condamne totalement le racisme et sa diffusion sur l'Internet.
- Pour assurer un épanouissement sain des mineurs dans la société, la loi les protège des messages « **à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine** » (voir fiche n° 13). Le milieu scolaire doit donc se prémunir contre ces dérives lors des activités en ligne, en particulier sur le Web et les messageries en temps réel (clavardage ou chat).
- Pour protéger l'intégrité physique et morale des mineurs, la loi condamne sévèrement **toute activité pédophile** d'adultes incitant les mineurs à la débauche, en particulier en vue « d'organiser des réunions comportant des exhibitions ou des relations sexuelles auxquelles un mineur assiste ou participe » (art. 227-22 du Code pénal). Le milieu scolaire doit évaluer les situations où les élèves risquent d'être confrontés à des messages ou à des images à caractère pédophile afin de tout mettre en œuvre ensuite pour éradiquer ce fléau de l'Internet scolaire.
- Toujours pour protéger les enfants, la loi condamne l'incitation à utiliser des matières dangereuses ou nuisibles à leur santé morale et physique. Elle punit pénalement les provocations directes

auprès des mineurs pour « **faire usage illicite de stupéfiants** » (art. 227-18 du Code pénal) ou pour « **consommer de manière habituelle et excessive des boissons alcooliques** » (art. 227-19 du Code pénal).

Questions à se poser pour évaluer les risques d'atteinte aux règles d'ordre public

- Le contenu que l'on souhaite utiliser lors des activités en ligne outrepasse-t-il les normes de tolérance telles qu'elles sont généralement admises dans la société ?
- Quel que soit l'outil de communication, les messages reçus par les élèves les incitent-t-ils ou leur proposent-ils des activités contraires à la loi ?
- Par le biais des activités en ligne envisagées, les élèves peuvent-ils être incités à la toxicomanie ou à l'alcoolisme ?
- Les activités en ligne envisagées peuvent-elles conduire les élèves à accéder à des contenus incitant à la haine ou à la violence ?
- Est-il envisageable d'établir une échelle de la violence des contenus permettant de fixer un âge minimum requis pour certains élèves plus matures ? Sur quels critères (Conseil d'état, CSA,...) ?
- Les activités en ligne envisagées peuvent-elles conduire les élèves à accéder à des contenus pornographiques ou plus gravement à caractère pédophile ? Quelle ligne de partage doit être établie avec l'information auprès des adolescents sur leur sexualité (identité sexuelle, relation à soi et à l'autre, sentiments et plaisir) et les précautions à prendre contre les maladies sexuellement transmissibles ?
- Quelles sont les situations où un message ou un contenu enfreignent les règles de la vie scolaire déterminées par le règlement intérieur ?

Le processus d'élaboration des règles

Cette fiche entend préciser les différentes étapes du processus d'élaboration des règles de conduite jusqu'à l'adoption finale. Inspiré de plusieurs études de cas, voici un processus type d'élaboration de règles en quatre étapes :

1. la collecte d'informations;
2. la discussion préliminaire avec les membres du conseil d'école ou du conseil d'administration;
3. la nomination d'un groupe de travail et l'élaboration d'un projet de charte;
4. l'adoption finale de la charte d'utilisation par le conseil d'école ou le conseil d'administration.

1- Collecte d'informations

L'objet primordial de cette première étape est de cerner le contexte de l'utilisation de l'Internet dans l'établissement d'enseignement et d'en dégager les spécificités.
Les initiateurs de la charte d'utilisation de l'Internet collecteront donc des informations sur la nature des activités en ligne et le public visé.
Il est nécessaire de consulter les personnes engagées dans les projets d'activités en ligne en milieu scolaire. Cette participation des acteurs du site est fort utile pour engranger des informations sur leurs préoccupations ou leurs craintes par rapport à l'utilisation de l'Internet. Il s'agit, ni plus ni moins d'une enquête d'opinion. Plus l'éventail des participants sera large, **plus les chances de succès de la charte seront importantes. Il faut permettre la participation concrète des principaux acteurs des activités en ligne.**
Mais d'autres informations plus factuelles peuvent aussi être collectées :

- les cas de conflits les plus souvent rencontrés dans le milieu scolaire
- le cas échéant, les types de problèmes vécus par d'autres établissements scolaires

2- Discussions préliminaires avec les membres du Conseil d'école ou du Conseil d'administration

Suite aux contacts et aux réactions des acteurs des activités en ligne, la discussion peut s'instaurer avec les membres du conseil d'école ou du conseil d'administration du collège ou du lycée. Ceux-ci ont alors pour mission de faire émerger les questions qui nécessitent un article dans la charte d'utilisation d'Internet. Concrètement, une feuille de travail doit être établie par le conseil avec les principaux problèmes que la future charte doit prendre en charge.

3- La création d'un groupe de travail et l'élaboration d'un projet de charte d'utilisation de l'Internet.

Désormais les initiateurs ont une idée des orientations de la charte. Mais pour que les choix deviennent des règles, un groupe de travail doit être nommé par le conseil d'école ou le conseil d'administration du collège ou du lycée.
Il est essentiel que les bonnes personnes siègent à ce groupe. Celles-ci doivent être compétentes, crédibles et bien renseignées, représentatives de leurs corps ou statuts, et disposer du temps et des ressources nécessaires. Les membres de ce groupe sont donc les personnes clés. Il est évident que, selon la nature des activités en ligne envisagées ou présentes et leur contexte, des personnes seront plus ou moins incontournables.

Conseils :

Le groupe de travail a tout avantage à être **le plus représentatif possible** de la variété des acteurs qui de près ou de loin sont touchés par l'activité Internet dans l'établissement scolaire.
Toute la collecte d'informations sur le site va, à présent, être mise à profit. Connaissant les préoccupations des acteurs des activités en ligne et les choix du conseil, le groupe de travail doit rédiger un projet de charte.
Il s'agit de préciser les droits et obligations des acteurs ou utilisateurs de l'Internet dans l'établissement scolaire.

Deux situations sont possibles :

1. ré-appropriation d'un texte préexistant,
2. création d'un nouveau texte.

3.1- Réappropriation d'un texte préexistant

Ici, la charte d'un autre établissement scolaire est prise comme modèle pour son efficacité reconnue. Elle sera alors une source d'inspiration pour le contenu de la charte en cours d'élaboration. Cette situation est possible seulement si l'on trouve d'autres établissements ayant les mêmes activités en ligne et des problèmes comparables. C'est pourquoi, quelquefois, le texte préexistant est modifié ou transformé afin de répondre aux besoins spécifiques de l'établissement qui élabore une nouvelle charte.

3.2- Création d'un texte nouveau

La réappropriation d'un texte préexistant peut vite s'avérer insuffisant pour des contextes plus élaborés où les participants aux activités en ligne ont un grand rôle créateur et/ou interactif. Nous pensons ici à la création de sites web, la mise en place de portfolios numériques…
Dans ces conditions, la spécificité des activités en ligne demande une charte "sur mesure". C'est pourquoi, doit être élaboré un énoncé des droits et obligations des acteurs propres aux activités en ligne de l'établissement scolaire.

Conseils :

le groupe de travail a tout avantage à élaborer d'une part une charte complète et précise qui sera annexée au règlement intérieur et d'autre part **une version plus succincte** qui sera très utile pour être affichée dans les locaux de l'établissement afin de rappeler aux élèves les principales règles d'utilisation du matériel informatique.

4- L'adoption finale de la charte d'utilisation

Une fois le projet de charte réalisé par le groupe de travail, il doit être soumis au Conseil d'école ou au Conseil d'administration pour être adopté définitivement lors d'un vote. Pour information, avant le vote final, le projet de charte doit être soumis à des autorités de tutelle (voir fiche n°3).

Exemples de clauses de charte

Quelques articles modèles sont présentés ici afin d'aider à la rédaction de chartes d'utilisation de l'Internet
Ces règles doivent pouvoir informer les utilisateurs sur les caractéristiques des outils de communication proposés et les risques courus. Elles doivent former et éduquer les utilisateurs, mais aussi les mettre face à leurs responsabilités le cas échéant.
Le code adopte la présentation des textes réglementaires déterminant les droits et obligations de chacun.

1- RAPPEL DE LA MISSION DES RESSOURCES INFORMATIQUES DE L'ÉTABLISSEMENT

« Les ressources du (...) (nom de l'établissement) sont dédiées prioritairement à l'enseignement. Toutefois elles peuvent être utilisées pour des travaux spécifiques d'administration liés à la l'enseignement, lorsque cela peut se faire sans pénaliser les tâches prioritaires d'enseignement ».
Art. 0.1 de la charte de bon usage des ressources informatiques du CICRP

2- DOMAINES D'APPLICATION

« Ce règlement s'applique à toute personne utilisant les systèmes informatiques situés sur le site de (...) (nom de l'établissement), les systèmes informatiques auxquels il est possible d'accéder à partir de l'école ainsi que les systèmes informatiques d'organismes extérieurs à l'école, mentionnés dans le contrat d'étude d'un élève ou ayant fait l'objet d'une convention avec l'école »
Art. 1 du règlement d'utilisation des moyens informatiques de l'Ecole normale supérieure.

3- CONDITIONS DU DROIT D'ACCÈS AU RÉSEAU INFORMATIQUE

« Tout utilisateur accédant aux ressources informatiques du (...) (nom de l'établissement) doit avoir au préalable approuvé la présente charte.
Tout utilisateur possède un « **user id** » auquel est associé un mot de passe. La remise de ces deux informations détermine un droit d'accès, éventuellement limité, aux ressources du (...) (nom de l'établissement) pour une durée déterminée. L'étendue des ressources auxquelles l'utilisateur a accès peut être limitée en fonction de ses besoins et des contraintes imposées par le partage de ces ressources avec les autres utilisateurs.
Ce droit d'accès aux ressources informatiques est personnel et incessible.
Ce droit d'accès est temporaire. Il est retiré dès lors que la fonction de l'utilisateur ne le justifie plus.
Il est retiré si le comportement d'un utilisateur est en désaccord avec les règles définies dans la présente charte. »
Art. I.a et III.b de la charte de bon usage des ressources informatiques du CNUSC.

4- RAPPEL DES PRINCIPES DE RESPECT DES DROITS DES PERSONNES

4.1- Droit à l'intimité

« Tout utilisateur a droit au respect de sa vie privée. Par conséquent, il est interdit d'utiliser les ressources informatiques de l'établissement en vue de révéler des éléments d'ordre intime d'une personne. Il est ici fait référence à la vie sentimentale, sexuelle ou familiale, l'état de santé, les opinions politiques, religieuses ou philosophiques.
De plus, les fichiers de chacun sont privés, même s'ils sont techniquement accessibles : la possibilité de lire un fichier n'implique pas l'autorisation de le lire. Toute tentative de lecture ou de copie de fichiers d'un autre utilisateur sans son autorisation est donc répréhensible. »

4.2- Droit au secret des correspondances privées

« Le respect du secret des correspondances interdit à tout utilisateur (des ressources de l'établissement) d'intercepter des communications privées qui ne lui sont pas destinées, de les utiliser ou de réexpédier un message qui lui était destiné à d'autres personnes sans l'autorisation de l'expéditeur initial ».

4.3- Droit à la réputation

« Toute personne a droit au respect de sa réputation. Par conséquent, il est interdit aux utilisateurs des ressources informatiques de l'établissement d'exposer toute personne à la haine ou au mépris en vue de nuire à l'estime ou la confiance que les autres lui portent. »

4.4- Droit à l'image des personnes

« Toute personne a droit au respect de son image. Par conséquent, il est interdit aux utilisateurs des ressources informatiques de l'établissement de capter et/ou de diffuser l'image ou la voix d'une personne lorsqu'elle se trouve dans un lieu privé sans son consentement. Lorsqu'une personne est identifiable dans un lieu public il est également recommandé d'obtenir son autorisation à la diffusion de son image. »

4.5- Consentement de la personne photographiée à la publication de son image sur un site web

« Je (nom) accepte que ma photo soit publiée sur le site (nom du site et URL).
J'ai été informé qu'une telle publication suppose que ma photo peut être vue et éventuellement reproduite par toute personne qui accède au site dans tout pays.
Le site s'engage à informer les usagers que les photos ne peuvent être reproduites (à des fins commerciales) ou (à n'importe quelles fins). »

4.6- Harcèlement et injures

« Tout utilisateur a droit de travailler sans être importuné. La liberté de parole n'autorise en rien le harcèlement ou les insultes via forum, courrier électronique ou autre moyen de communication. Par conséquent, il est interdit aux utilisateurs des ressources informatiques de l'établissement d'envoyer des messages de nature discriminatoire de façon répétée ou insultante ».

5- Rappel des principes de respect du droit d'auteur

« Le droit d'auteur reconnaît aux auteurs un monopole d'exploitation sur leurs œuvres ou créations, c'est-à-dire un droit exclusif sur les conditions de diffusion ou de reproduction via l'Internet.
Les élèves sont titulaires des droits d'auteur sur leurs œuvres originales créées au moyen des ressources informatiques de l'établissement. A ce titre, tout travail d'élève publié sur l'Internet doit mentionner le nom de son auteur et avoir obtenu l'autorisation des parents (si l'élève est mineur).
Sauf accord contraire, l'établissement est présumé titulaire des droits d'exploitation des travaux des enseignants créés lors de leur service d'enseignement et avec les ressources informatiques de l'établissement. Par contre, en tant qu'auteur, le nom des enseignants doit toujours être mentionné.
Sauf exceptions au droit d'auteur (domaine public, citation, copie privée), tout utilisateur des ressources informatiques de l'établissement doit au préalable obtenir l'autorisation de l'auteur avant d'utiliser tout contenu littéraire, audiovisuel ou musical, en vue par exemple d'une publication ou d'une diffusion en ligne. Sans autorisation, l'utilisateur peut être poursuivi pour contrefaçon. »

6- Rappel des règles d'ordre public de protection des personnes

Compte tenu des valeurs partagées par notre société et promues par l' Éducation nationale, il s'agit ici d'expliquer que des lois existent afin de sanctionner des agissements jugés contraires à l'ordre public. Il en est ainsi pour les informations à caractère pornographique ou violent perçues par les mineurs, la propagande raciste ou l'incitation à la haine raciale ou antisémite.

6.1- Propos raciste et antisémite

« La loi pénale condamne les propos raciste et antisémite. Par conséquent, il est interdit aux utilisateurs des ressources informatiques de l'établissement de tenir des propos de nature raciste ou antisémite ou de diffuser des messages ou des contenus de propagande haineuse via le courrier électronique, les forums de discussion ou tout autre moyen de communication. Cette interdiction ne concerne pas les propos exprimant des opinions légitimes à l'égard de groupes, de religions ou d'entités ethniques ».

6.2- Contenus à caractère violent et pornographique

«L'utilisation des ressources informatiques de l'établissement a une finalité strictement éducative et ne peut en aucun cas servir de moyen pour les utilisateurs, mineurs en particulier, de percevoir des contenus à caractère violent ou pornographique, quel que soit le support de diffusion, local ou distant. »

6.3- Lutte contre la pédophilie

« Au nom de la lutte contre la pédophilie, sont interdites toutes représentations graphiques, photographiques, filmées ou autres, de mineurs se livrant à des activités explicitement sexuelles réalisées ou non par des moyens mécaniques ou électroniques. L'établissement scolaire entend donc poursuivre avec la plus grande sévérité toute utilisation de l'Internet en général, et des ressources informatiques de l'établissement en particulier, pour transmettre, rendre accessible, exporter, accéder à des images à caractère pédophile ou correspondre avec un enfant en vue de commettre contre lui une infraction sexuelle.
La loi permet aux tribunaux d'ordonner la suppression des contenus à caractère pédophile stockés sur un ordinateur français et permet la confiscation de matériels ou d'équipements utilisés pour commettre l'infraction. »

Exemples d'autorisations

Quelques exemples de formules de cession de droits autorisant la publication en ligne d'œuvres ou d'images protégées conformément à la législation en vigueur (Art. L 131-2 du Code de propriété intellectuelle).

1- Autorisation de publier le travail d'un élève sur un site web

« Nous, soussignés (nom de l'élève) et (nom du parent) en tant que représentant légal, sommes d'accord pour que les photographies, dessins ou autres travaux (dûment identifiés et nécessairement décrits car l'engagement ne peut être global) de (nom de l'élève) puissent faire l'objet d'une publication sur Internet. Je comprends que mon nom de famille ne sera pas utilisé avec mes photographies, dessins ou autres travaux dans le but d'assurer le respect de ma vie privée.
(Suivie de la signature des parents et de l'élève mineur) »

Conseils :

Quelques précautions à prendre pour convaincre les parents réticents à autoriser la publication en ligne face au risque d'atteinte à la vie privée de leur enfant :

- Ne jamais écrire le nom de famille des élèves sur leurs travaux.
- Éviter de publier du matériel permettant d'identifier les élèves comme le numéro de téléphone, l'adresse ou une photo.
- Les photos de classe devraient représenter au minimum trois élèves
- Si vous êtes autorisés à afficher des photos individuelles, n'inscrivez pas le nom de l'étudiant apparaissant sur la photo.
- Éviter de publier les pages web personnelles de vos élèves. Si vous agissez de la sorte avec un seul de vos étudiants, vous allez devoir en faire de même pour chacun d'entre eux. Si un élève veut créer un site Internet, cela doit être fait dans le cadre des objectifs du cours. Lier la page personnelle d'un étudiant peut ne pas être approprié pour le site web de l'école.
- Expliquer les différents modèles de permission pour publier les travaux d'étudiants sur l'Internet durant les rencontres portes ouvertes. Informer les parents des différentes mesures que vous prenez pour assurer le respect de la vie privée de leurs enfants.

2- Autorisation d'utiliser les œuvres d'un tiers pour publication sur un site web

« J'autorise (_____nom de l'établissement _____) à publier (___inscrire le nom ou une description de l'œuvre__) sur le site web (_____nom du site et URL_____) ou de tout autre site qui pourra remplacer celui-ci.

Je garantis que je détiens effectivement les droits dans l'œuvre et m'engage à indemniser l'institution s'il s'avère que d'autres personnes revendiquent des droits sur l'œuvre.
Cette autorisation ne vaut que dans la mesure où le site conserve sa finalité d'enseignement.

Cette autorisation est valable pour (__inscrire la durée____). Elle oblige mes héritiers et ayants droit. »

3- Autorisation de publier une photographie par un titulaire du droit d'auteur

« Je consens à la publication de la photo (_____décrire la photo ou en annexer une copie_____) sur le site web de (__nom de l'établissement scolaire___). Cette autorisation donnée sans limite de temps et à titre non exclusif vaut pour tout le temps où l'établissement maintient un site Internet à finalité éducative. »

4- Autorisation d'établissement d'un lien hypertexte

« Je (nom) accepte que le site (nom du site et URL) établisse un lien hypertexte vers mon site (nom du site et URL).

Je garantis que je détiens effectivement les droits relatifs au nom de domaine et m'engage à indemniser l'institution s'il s'avère que d'autres personnes revendiquent des droits sur le site.

Cette autorisation donnée sans limites de temps vaut pour tout le temps où l'établissement (nom de l'établissement scolaire) maintient un site Internet à finalité éducative. ».

Sanction et révision

Une fois la charte rédigée, la démarche de régulation des activités en ligne de l'établissement scolaire ne cesse pas. La troisième et dernière étape est de s'assurer du respect des règles par un processus de sanction et de réviser régulièrement les règles afin de répondre aux évolutions des activités en ligne.

1- LE PROCESSUS DE SANCTION

Avant de sanctionner l'infraction aux règles, l'établissement doit s'assurer que l'ensemble des utilisateurs a bien eu connaissance des règles d'utilisation des ressources informatiques.
Quelle que soit la forme des règles, le plus sûr moyen de s'assurer de la connaissance des règles est de conditionner l'ouverture d'un compte utilisateur à la signature d'un engagement écrit.
L'exemple du campus de Jussieu avec la feuille d'inscription au Centre Interuniversitaire de Calcul de la région Parisienne (CICRP)

« Je soussigné (nom de l'utilisateur) enregistré sur les serveurs du CICRP sous le sigle (code le l'utilisateur), utilisateur des ressources du CICRP en qualité de (statut de l'utilisateur) déclare avoir pris connaissance de la charte des utilisateurs du CICRP et m'engage à respecter ses règles de bon usage.

Lu et approuvé à Paris le, ... (Signature) »

En annexe de l'engagement signé en double exemplaire se trouvent les règles d'utilisation.
Pour les élèves mineurs, la signature des parents ou du représentant légal est également requise.

La Charte d'utilisation de l'Internet peut également être commentée par le professeur principal et signée en début d'année scolaire en même temps que le règlement intérieur (pour le lycée) ou le contrat de vie scolaire (pour les collèges).

1.1- Sanction disciplinaire du non respect de la charte

Exemple d'échelle possible et minimale des conséquences d'un comportement indésirable :

1ère infraction

• Les parents de l'étudiant sont informés de la violation
À la discrétion des administrateurs :
• Interdiction d'accès à Internet pour l'élève pendant une semaine;
• Envoi de courrier électronique par l'élève limité aux professeurs pendant une semaine;
• Retenue.

2ème infraction

• Les parents sont informés de l'infraction et une réponse est requise de leur part
• Interdiction d'accès à Internet pour l'élève pendant deux semaines
• Envoi de courrier électronique par l'étudiant limité aux professeurs pendant deux semaines
• Retenue

3ème infraction

• Rencontre entre les parents et l'administrateur à l'école
• L'étudiant perd l'accès à son compte d'utilisateur pendant un mois

4ème infraction

• Suppression définitive d'accès au réseau

Pour les infractions plus graves, l'utilisateur peut passer devant le conseil de discipline qui peut selon la gravité de la situation prononcer un blâme, un avertissement en cas de récidive ou décider d'un renvoi de l'établissement.

L'enseignant-fonctionnaire encourt lui des sanctions administratives.

1.2- Sanction juridique du non respect de la charte

Il s'agit ici d'une charte, assimilée à un règlement disciplinaire, qui offre tout un éventail de sanctions d'ordres disciplinaire et juridique.
Pour les infractions les plus graves, les élèves comme le corps enseignant peuvent être poursuivis devant la justice.
Dans le cas de communications menaçantes, de destruction volontaire de la propriété ou d'autres violations graves, les auteurs d'infractions pourront encourir des condamnations pénales suite au signalement aux autorités de police ou de justice.

2- Le processus de révision

Pour éviter l'obsolescence de la charte, un processus de révision doit être prévu par l'établissement scolaire.
La charte peut prévoir sa propre révision par la mise en place d'un organisme d'évaluation et de révision qui chaque année peut remettre un rapport de bilan et de recommandations quant aux changements à apporter.

Les acteurs du site doivent toujours être vigilants quant à l'évolution des activités en ligne au sein de leur établissement et être prêts à s'investir de nouveau dans une nouvelle démarche de révision de la charte.

Conseils :
Il faut savoir que les choix de régulation d'une charte ne sont jamais figés. Un site et son contexte évoluent… Une règle qui pouvait être opportune au moment de son élaboration, peut s'avérer, quelque temps plus tard décalée et inefficace.

Conclusion

L'Internaute n'échappe pas aux droits nationaux ou internationaux. Lorsque le ministère de l' Éducation Nationale décide de connecter les établissements scolaires à l'Internet, le premier des devoirs est de favoriser des usages du réseau conformes aux valeurs de notre société.
Le véritable enjeu de la régulation de l'Internet en milieu scolaire est celui du développement de processus appropriés afin d'assurer l'encadrement nécessaire des activités en ligne dans le contexte spécifique de l'enseignement.
L'élaboration de chartes d'utilisation de l'Internet est nécessaire pour assurer une répartition des responsabilités entre les acteurs et essentielle afin d'assurer, de manière pratique, le respect des principes et des obligations légales. On ne peut pas se contenter de proclamer des généralités sans informer, de manière adéquate , les acteurs des risques et surtout des responsabilités qui leur incombent lorsqu'ils agissent sur l'Internet.
Dans ce guide, nous avons proposé une démarche pour la mise en place d'outils pertinents afin d'élaborer et appliquer des règles de conduite.
Comme le prouve la gestion des aspects juridiques liés à l'Internet en milieu scolaire, pour assurer la mise en œuvre et surtout, l'effectivité des règles dans des environnements aussi instables, il faut identifier les risques découlant du contexte précis dans lequel on se trouve. En définitive comme la démarche de ce guide le suggère, il n'est plus possible de se satisfaire de reconduire les règles qui prévalent dans l'espace physique sans s'interroger sur les mutations qui affectent les activités présentes sur l'Internet.

2- Bibliographie pour aller plus loin

2.1- Ouvrages sur la régulation de l'Internet

LUCAS (André), **DEVEZE (Jean)** et **FRAYSSINET (Jean)**, Droit de l'Informatique et de l'Internet, PUF, coll. Thémis Droit privé, Paris 2001
LUCAS (André), Droit d'auteur et numérique, Litec, Paris, 1998
TRUDEL (Pierre) et al., Droit du Cyberespace, Thémis, Montréal, 1997

2.2- Articles sur la régulation de l'Internet

TRUDEL (Pierre), « Quel droit et quelle régulation dans le cyberespace ? », Sociologie et sociétés, vol. XXXII.2, p. 189
VIVANT (Michel), « Internet et modes de régulations », in Internet face au droit, colloque du CRID, 21 et 22 novembre 1996, Cahiers du CRID n° 12, Story scienca, Namur, p 215

2.3- Lois françaises

Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, JO 13 juillet 1991, p. 9167 et 10 août 1991 (rectificatif), p. 10617.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 janvier 1978, p. 3

Loi n° 94-361 du 10 Mai 1994 portant mise en œuvre de la directive n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle ; JO 11 mai 1994, p. 6863.

Loi n° 98-536 du 1er juillet 1998 portant transposition dans le Code de la propriété intellectuelle de la directive n°96/9/CE du Parlement et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données, JO 2 juill. 1998, p. 75

Loi n° 2000-719 du 1 août 2000 modifiant l'article 43-8 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication ; JO 2 août 2000, p.11903.

2.4- Droit communautaire

Directive n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données, JOCE n° L 281, 23 nov. 1995, p. 31.

Directive n° 91/250/CE du Conseil, du 14 mai 1991, concernant la protection juridique des programmes d'ordinateur ; JOCE n° L122, 17 mai 1991, p.42.

Directive n° 1996/9/CE du Parlement européen et du Conseil concernant la protection juridique des bases de données, JOCE n° L 177, 27 mars 1996, p. 20.

Résolution du Conseil et des représentants des gouvernements des État s membres, réunis au sein du conseil du 17 février 1997 sur les messages à contenu illicite et préjudiciable diffusés sur Internet, JOCE n° C 70, 6 mars 1997, p.1.

Directive n° 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques ; JOCE n° L 013, 19 janv. 2000, p. 12.

Directive 2000/31/CE du parlement européen et du conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, JOCE L 178/1 du 17 juillet 2000.

Directive n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; JOCE n° L 201 31 juill. 2002, p. 37.

Directive n° 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, JOCE n° L 178 17 juill. 2000, p. 1.

Directive n°2001/29/CE du parlement européen et du conseil sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, JOCE n° L 167, 22 juin 2001, p. 10.

2.5- Documents – Rapports -Guides

Conseil d'État, Internet et les réseaux numériques, La Documentation française, Paris, 1998

CRDP, TRUDEL (Pierre) et ABRAN (France), Guide pour gérer les aspects juridiques d'Internet en milieu scolaire, Montréal, 2003, [www.crdp.umontreal.ca/guides]

PNER, de LAMBERTERIE (Isabelle) (ss la dir.), La numérisation pour l'enseignement et la recherche : aspects juridiques, Editions maison des sciences de l'homme, Paris, 2002, [www.pner.org].

COSTE (Pierre de la) et BENARD (Vincent), L'hyper-république : bâtir l'administration en réseau autour du citoyen, Rapport remis au secrétaire d'État à la réforme de l'État le 10 janvier 2003, La Documentation Française, 2003

Forum des droits sur l'Internet, Quelle responsabilité pour les organisateurs de forums de discussion sur le Web ?, [www.foruminternet.org], 2003.

KNOBEL (Marc), Haine raciale sur le réseau internet, rapport édité par la LICRA en avril 1999, [www.LICRA.com]

2.6- Documents non juridiques

LABERGE (Clément), Apprendre à penser autrement pour imaginer un monde différent, In « Les défis du Cybermonde » ss. la dir. de FISCHER Hervé, Presses de l'Université Laval, Laval, 2003.

KARNIK (Kiran), Perspectives et défis relatifs aux TCI et à la formation assistée par ordinateur ou en ligne, In « Les défis du Cybermonde » ss. la dir. de FISCHER Hervé, Presses de l'Université Laval, Laval, 2003.

AUMONT (Serge), Installer et Administrer des listes de diffusion, UREC, novembre 1997, [www.cru.fr/listes/atelier/ll/ll.html].

GRENIÉ (Michel), Dictionnaire de la micro-informatique, Larousse, Paris, 1997

LEVY (Pierre), Les technologies de l'intelligence, l'avenir de la pensée à l'ère informatique, Points, Paris 1990

LEVY (Pierre), Qu'est-ce que le virtuel ? La Découverte, Paris, 1995