aix-marseille

PROTECTION DES MINEURS DANS LE CADRE PÉDAGOGIQUE

référentiel de la sécurité informatique à l'école

// 2006-2007

ministère
éducation
nationale
enseignement
supérieur
recherche

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

sommaire

1. Objet et contenu du document

Le présent document constitue le **Référentiel de sécurité informatique en écoles** élaboré par l'Académie d'Aix-Marseille. Ce document aborde les thèmes suivants :

- Les enjeux et risques liés à l'usage des Technologie de l'Information et de la Communication (TIC),
- Les recommandations en terme d'usage de l'Internet dans le cadre pédagogique et de la protection des mineurs, La circulaire DARCOS,
- Les aspects législatifs et réglementaires (protection des données personnelles, code de la propriété intellectuelle,
- Les moyens à mettre en œuvre (filtrage, authentification, traçabilité, etc.),
- Les mesures d'accompagnement des utilisateurs (sensibilisation, formation, responsabilisation).

L'objectif de cette politique est de délimiter les rôles et responsabilités des différents intervenants de la communauté éducative et d'élaborer des recommandations en termes de moyens à mettre dans le cadre de l'usage de l'Internet et de la protection des mineurs.

2. Les enjeux et risques des TIC.

2.1 Le contexte.

Les Technologies de l'Information et de la Communication prennent une place essentielle dans le monde d'aujourd'hui. L'Internet, les réseaux de communication à haut débit, la convergence du traitement numérique des données, de la voix et des images ont pour conséquence le développement spectaculaire de nouveaux secteurs économiques et surtout de nouveaux rapports entre les hommes et dans le fonctionnement des organisations. La société de l'information est la nouvelle donne du développement économique et social mondial. Cette société introduit des bouleversements qui dépassent largement le seul enjeu économique et comme le souligne le PAGSI (Programme d'Action Gouvernemental pour la Société de l'Information) : *« L'essor des nouveaux réseaux d'information et de communication offre des promesses sociales, culturelles et en définitive politique ».*

Le développement soutenu des TIC impulsé par les pouvoirs publics constitue à l'évidence un des axes majeurs d'action pour l'enseignement et la recherche qui sont sans doute les domaines les plus en prise directe avec les évolutions de notre société. Au sein de l'Éducation Nationale, l'usage de l'Internet dans les pratiques pédagogiques est déjà largement développé et se banalise avec la généralisation des accès à l'Internet haut-débit dans les établissements scolaires et plus particulièrement dans les écoles.

L'école étant un levier stratégique fort pour l'appropriation de l'Internet par les enfants, l'Éducation Nationale s'est fixé comme objectif d'obtenir la maîtrise par tous les jeunes des nouvelles technologies d'où la généralisation au sein des écoles du Brevet Informatique et Internet (B2I).

2.2 Les enjeux et risques.

L'essor des TIC est un facteur de développement, d'intégration sociale et d'enrichissement individuel incontestable. Elles sont incontournables dans les enseignements et permettent notamment de mieux prendre en compte les publics à besoins spécifiques et de développer de nouvelles modalités d'enseignement (tutorat à travers les réseaux, ...). Le déploiement d'espaces numériques de travail, engagé par les Académies en partenariat avec les collectivités territoriales, permettra d'assurer un accès ergonomique et performant aux outils et aux services adaptés aux besoins des différentes catégories

Le développement de l'Internet constitue donc un enjeu majeur pour l'Éducation Nationale. A mesure que l'Internet intègre la vie quotidienne, sa maîtrise s'avère indispensable à l'ensemble des élèves. Face à ces nouveaux défis, l'École a un rôle crucial à jouer comme lieu d'apprentissage et de familiarisation à l'Internet. Elèves et enseignants doivent à la fois s'approprier ces technologies et leurs enjeux et en faire un véritable outil au service de la réussite scolaire.

La maîtrise des technologies de l'Internet devient cruciale à la fois pour les élèves et pour l'ensemble des personnels de l'Éducation Nationale. Au-delà d'une utilisation « passive », il convient de favoriser une meilleure maîtrise de la création et de la diffusion des informations sur le réseau. Les élèves ne peuvent plus se contenter d'être seulement des téléspectateurs/consommateurs.

L'accès à Internet, s'il n'est pas accompagné d'une démarche de sensibilisation et d'un travail d'analyse, peut mener à une forme de stagnation sur des usages « techno-ludiques » sans réelle portée pédagogique. Le risque de cette forme d'appropriation de l'Internet est qu'elle ne développe qu'une habileté technique et non un véritable sens critique. Or c'est précisément dans une démarche critique qu'enseignants et élèves doivent s'inscrire pour évaluer les informations qu'ils trouvent sur Internet.

En effet, ce nouveau média peut également se révéler être un important vecteur de danger notamment à l'égard des enfants. L'exposition d'adolescents et d'enfants à des contenus, images, photos et vidéos, peut constituer une forme nouvelle de violences.

Les effets négatifs de l'émergence de ce nouveau média au sein même des familles restent trop souvent méconnus des principaux intéressés, parents et enfants mineurs, qui à l'apprentissage de la technique doivent, dans un même temps, ajouter l'appréhension d'un environnement médiatique particulier et non policé.

C'est dans ce contexte que l'Académie d'Aix-Marseille a élaboré le présent **Référentiel de la sécurité informatique en écoles**. Il s'agit d'un outil qui permet d'offrir un cadre de référence cohérent à l'ensemble des acteurs et des activités d'une école. Il doit sensibiliser aux risques qui menacent les élèves ainsi qu'aux moyens disponibles pour s'en prémunir. Sa diffusion à l'ensemble de la communauté éducative mais également aux représentants des collectivités locales et territoriales contribue une prise de conscience et une implication de tous dans la protection des mineurs dans le cadre pédagogique.

3. Les Textes officiels et préconisations.

Le chapitre présente les principales circulaires, projets et recommandations nationales en termes de protection des mineurs à savoir :

- La **Circulaire « DARCOS »** n°2004-035 du 18 février 2004 (BO n° 9 du 26 février 2004), adressée aux Rectrices et Recteurs d'Académie, a vocation à organiser l'usage de l'Internet dans le cadre pédagogique et la protection des mineurs,
- Le **« Plan d'action national de sensibilisation aux enjeux et aux risques de l'Internet »** qui dresse un premier bilan des mesures prises au sein de l'Éducation Nationale.
- Les **guides pratiques** concernant la sensibilisation et d'autre part la protection des élèves mineurs face aux dangers de l'Internet,
- Le **Brevet Informatique et Internet** qui atteste de compétences développées par les élèves tout au long de leur cursus scolaire lors d'activités intégrant les nouvelles technologies d'information et de communication.

3.1 Circulaire DARCOS.

La circulaire DARCOS n°2004-035 du 18 février 2004 (BO n° 9 du 26 février 2004) vise à instaurer des mesures d'accompagnement adaptées, destinées à faciliter le travail des équipes pédagogiques, tout en prenant en compte les impératifs de sécurité, et notamment la protection des mineurs.

Pour ce faire, elle entend mettre en place :

- Des mesures d'aides aux écoles et équipes éducatives.
  Deux modes de contrôles sont possibles, modulables selon les situations rencontrées (selon l'équipement des écoles et le niveau d'enseignement) :
  - ⊙ un contrôle a priori des informations consultées, en interdisant l'accès à un ensemble de sites reconnus comme inappropriés (sites au contenu pornographique, raciste, violent…) par l'intermédiaire de « listes noires » (possibilité, pour des situations pédagogiques particulières, de limiter la consultation à un ensemble connu de sites, à partir de « listes blanches »),
  - ⊙ un contrôle a posteriori, par examen de la liste des sites consultés.
- Des mesures de formation, de sensibilisation et de responsabilisation des utilisateurs.
  Un accompagnement des dispositifs de filtrage est prévu, avec des mesures de formation, de sensibilisation et de responsabilisation de l'ensemble des acteurs concernés : usagers, personnels de l'Éducation Nationale et élèves doivent être informés des spécificités de l'Internet ; il convient pour cela de prévoir des actions d'information et de sensibilisation à destination des équipes éducatives et des élèves, en s'appuyant sur les ressources académiques les plus concernées (Conseillers aux Technologies de l'Information et de la Communication pour l'Enseignement scolaire et Responsables de la Sécurité des Systèmes d'Information) ; la responsabilisation, quant à elle, doit passer par la contractualisation de l'usage de l'Internet : chaque école devra établir une charte d'utilisation de l'Internet et l'annexer au règlement intérieur ; elle devra être signée par les élèves et leurs parents dans le cas des élèves mineurs ;
- Des mesures d'alertes.

  Etablissement de la chaîne d'alerte reposant sur l'Inspecteur d'Académie, la cellule académique organisée autour du Conseillers aux Technologies de l'Information et de la communication pour l'enseignement scolaire (CTICE) et du Responsable de la Sécurité des Systèmes d'Information (RSSI), et la cellule nationale de coordination;
- Des mesures d'accompagnement du dispositif lui-même ;

  Elles sont pour l'instant de plusieurs sortes :

  - ⊙ un formulaire en ligne qui devra être renseigné périodiquement par le directeur d'école (http://aiedu.orion.education.fr) ;
  - ⊙ un guide pratique de mise en œuvre du dispositif (www.educnet.education.fr/aiedu/guide1.htm). Ce guide est conçu pour prendre en compte à la fois l'évolution des technologies et le savoir-faire des utilisateurs. ;
  - ⊙ Enfin, le brevet informatique et Internet (B2i) doit permettre aux élèves de maîtriser, avec efficacité et civisme, ces nouveaux moyens de communication.

3.2 Plan CONFIANCE.

Le 18 mai 2005, François Fillon, ministre de l'Éducation Nationale, a dressé un premier bilan des mesures prises au sein de l'Éducation Nationale. Au cours de cette conférence de presse, Francois d'Aubert, ministre délégué à la Recherche, a annoncé le **plan « Confiance »** à destination du grand public et soutenu par la commission européenne qui vient compléter le dispositif gouvernemental. La Délégation aux usages de l'Internet doit en assurer la coordination à travers le développement du site mineurs.fr.

Le projet CONFIANCE « **Plan d'action national de sensibilisation aux enjeux et aux risques de l'Internet** » a été proposé par la Délégation aux usages de l'Internet (DUI) à la Commission européenne, qui l'a retenu en novembre 2004, dans le cadre de son plan d'action pour un Internet plus sûr (SIAP). Il vise à valoriser et conduire de manière concertée, des actions de sensibilisation des enfants et de leurs parents à la sécurité et à la civilité de l'Internet, en impliquant l'ensemble des acteurs de l'Internet, institutions publiques, associations et industriels, acteurs dans ce domaine

3.3 Guides et préconisations.

Deux guides pratiques concernant d'une part la sensibilisation et d'autre part la protection des élèves mineurs face aux dangers de l'Internet ont été réalisés par l'Éducation Nationale :

- **Guide « pratique » de mise en place de ces préconisations dans les établissements** disponible sur le site Educnet (http://www.educnet.education.fr/).

  Ce guide comporte notamment des précisions sur la liste « noire » nationale de sites inappropriés à filtrer, accessible auprès des missions TICE des Académies. Pour améliorer l'efficacité de la « liste noire », une adresse est disponible afin de transmettre les pages à ajouter à la liste ou à retirer : http://bd.educnet.education.fr/cgi-bin/squidguard_modify.cgi

  Une cellule nationale de coordination et de gestion des procédés de filtrage, une chaîne d'alerte et un contrôle de l'efficacité du dispositif ont été mis en place au Ministère. La cellule nationale est contactée pour toutes les opérations qui n'ont pu trouver de solutions au niveau académique.

- **Guide d'aide à l'élaboration des chartes d'utilisation des ressources Internet destiné à l'ensemble des établissements**

  Une charte d'utilisation des ressources TIC doit être établie dans chaque école et jointe au règlement intérieur. Afin d'avoir une valeur de contrat entre l'élève et l'école, elle devra être signée par les élèves et les parents, pour les élèves mineurs.

  La charte de l'école doit être expliquée et détaillée aux élèves par l'équipe pédagogique, au même titre que le règlement intérieur. Les discussions associées contribuent à la formation civique et citoyenne des élèves. Elles font donc partie intégrante du dispositif éducatif.

3.4 Brevet Informatique et Internet.

Après avoir été présentée comme l'une des priorités de la rentrée scolaire 2004, « la maîtrise des techniques usuelles de l'information et de la communication » est définie, dans la loi d'orientation et de programme, comme l'une des cinq composantes du socle commun de « connaissances et de compétences indispensables » qui doivent être acquises à la fin de la scolarité obligatoire. C'est dans ce cadre que l'attestation de compétences du Brevet Informatique et Internet (B2i), graduées tout au long du cursus scolaire, est validée. Conformément à la circulaire n°2005-135 du 9 septembre 2005 relative aux technologies d'information et de communication dans l'enseignement scolaire, la dénomination B2i niveau 1 est remplacée par B2i école, la dénomination B2i niveau 2 est remplacée par B2i collège(*), la dénomination B2i niveau 3 est remplacée par B2i lycée-CFA. »

(*) devrait être prochainement intégré dans l'évaluation du Brevet.

Le B2i école est intégré aux programmes de l'école primaire depuis la rentrée 2002. Il atteste des premières compétences acquises par l'enfant (de 6 à 10 ans) pour lire et produire des documents, rechercher des informations, communiquer au moyen d'une messagerie et, déjà, adopter une approche citoyenne face aux informations véhiculées par les outils informatiques.

4. Les aspects juridiques et réglementaires.

Le chapitre décrit les principaux textes de loi traitant de la sécurité informatique et plus particulièrement de la protection des mineurs.

4.1 La Commission Nationale de l'Informatique et des Libertés.

Face aux dangers que l'informatique peut faire peser sur les libertés, la Commission Nationale de l'Informatique et des Liberté (CNIL) a pour mission essentielle de protéger la vie privée et les libertés individuelles ou publiques. Elle est chargée de veiller au respect de la loi 'Informatique et liberté' qui lui confie six missions principales :

- Recenser les fichiers, en enregistrant les demandes d'avis du secteur publique et les déclarations du secteur privé, en tenant à jour et en mettant à la disposition du public le « fichier des fichiers » ;
- Contrôler, en procédant à des vérifications sur place ;
- Réglementer, en établissant des normes simplifiées, afin que les traitements les plus courants et les moins dangereux pour les libertés fassent l'objet de formalités allégées ;
- Garantir le droit d'accès, en exerçant les droits d'accès indirect, en particulier au fichier des Renseignements Généraux ;
- Instruire les plaintes, en procédant le plus souvent à une concertation entre les parties en vue d'un règlement à l'amiable ;
- Informer, les personnes de leurs droits et obligations , conseiller toutes les personnes qui le lui demande, de proposer au gouvernement les mesures législatives ou réglementaires qui lui paraissent utiles.

La CNIL n'est pas une instance de réglementation de l'informatique en général ni de protection de la vie privé ou des libertés en général (par exemple elle n'est pas compétente en matière de copie illicite, de violation de licences, ou de contrefaçon de logiciel). Son champ de compétence est strictement délimité par la loi du 6 janvier 1978 et concerne essentiellement les traitement des données nominatives, automatisés ou manuels.

La loi du 6 janvier 1978.

Le principe de base de la loi 'informatique et liberté' est qu'il est interdit de mettre ou de conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données **nominatives** qui, **directement ou indirectement**, font apparaître les **origines raciales ou les opinions politiques, philosophiques ou religieuse des personnes**.

La loi du 6 janvier 1978 reconnaît essentiellement 7 droits aux personnes :

- Le droit à l'information préalable ;
- Le droit de curiosité ;
- Le droit d'accès direct ;
- Le droit d'accès indirect ;
- Le droit de rectification ;
- Le droit d'opposition ;
- Le droit à l'oubli.

Ces droits ne sont pas des simples figures rhétoriques. On les retrouve dans la plupart des législations sur la protection des données personnels en Europe et dans le monde.

4.2 Principales lois liées à la sécurité informatique.

Il est rappelé que toute personne sur le sol français doit respecter l'ensemble de la législation applicable (nul n'est censé ignorer la loi), notamment dans le domaine de la sécurité informatique (liste non exhaustive) :

- la nouvelle loi Informatique et Libertés du 6 août 2004 qui modifie la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) ;

- la loi d'orientation pour la sécurité intérieure du 29 août 2002 (LOPSI) ;
- la loi de sécurité quotidienne du 15 novembre 2001 (LSQ) ;
- la législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal);
- la loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication ;
- la loi du 3 juillet 1985 relative au droits d'auteurs et celles relatives à la cryptologie ont été insérées dans la loi n°92-597 du 1er juillet 1992 relative au code de propriété intellectuelle.

4.2.1 La nouvelle loi informatique et libertés.

La nouvelle loi Informatique et libertés du 6 août 2004, publiée au JO le 7 août 2004, transpose la directive communautaire 95/46/CE d'octobre 1995 et modifie la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La nouvelle loi remplace la notion de « données nominatives » par celle de « données à caractère personnel » et introduit des concepts juridiques adaptés aux nouvelles formes de traitements issus de la société de l'information et de l'économie numérique. **Elle renforce aussi les droits et protections reconnus aux personnes physiques, et augmente le niveau d'obligations incombant aux responsables de traitements.**

En premier lieu, le nouveau texte réforme profondément les formalités de déclaration. Huit catégories génériques de traitements, considérés comme générateurs de risques pour les droits et libertés, sont désormais soumis à l'autorisation préalable de la Commission Nationale de l'Informatique et des Liberté (CNIL) du fait de la nature des données concernées et de leur finalité. En pratique, les traitements suivants sont être concernés : segmentation de la clientèle de type CRM (Customer Relationship Management ou gestion de la relation client), profiling (cookies et données de connexion...), scoring (utilisé par les organismes de financement afin de qualifier l'éligibilité au financement)(fournisseur de systèmes de crédit), lutte contre la fraude et listes noires, cybersurveillance des salariés, biométrie, géolocalisation. En parallèle, la loi instaure un régime déclaratif réservé aux traitements les plus courants, permettant de recourir à des déclarations extrêmement simplifiées. Elle innove également en proposant aux entreprises de nommer un correspondant à la protection des données à caractère personnel permettant à ces dernières d'être exonérées des obligations déclaratives dès lors qu'elles tiennent un registre interne et garantissent la conformité des traitements à la loi.

En second lieu, l'allégement des formalités trouve sa contrepartie dans l'augmentation des pouvoirs de la CNIL. La loi précise les modalités de cette action, maintient l'existence du délit d'entrave, renforce la coopération de la CNIL avec la justice. En cas d'urgence, la CNIL pourra recourir au référé sous astreinte, ordonner le verrouillage de bases de données et l'interruption de traitements ou encore retirer une autorisation.

Enfin, autre grande nouveauté, la CNIL rejoint le club très fermé des autorités administratives dotées d'un pouvoir de sanction financière. La sanction pourra être proportionnée à la gravité des manquements commis et aux avantages qui en sont tirés. Pouvant se situer entre 150 000 et 300 000 euros elle pourra être rendue publique. Les sanctions pénales existant dans la loi de 1978 sont alourdies et demeurent applicables aux personnes physiques et morales.

4.2.2 Loi de Confiance dans l'Economie Numérique.

La loi dite Loi de Confiance dans l'Economie Numérique (LCEN) est née du souhait du législateur de fonder à la fois l'Internet et le commerce électronique dans la législation française. Elleprocède à une refonte de l'architecture du droit des médias, clarifiant le droit applicable aux services de l'Internet. L'article 1er de la LCEN crée dorénavant une nouvelle catégorie générique : la « communication au public par voie électronique » qui se subdivise en « communication audiovisuelle » et en « communication au public en ligne ». Chacune de ces deux catégories est dorénavant soumise à un régime propre : loi du 30 septembre 1986 sur la liberté de communication pour la communication audiovisuelle et loi du 21 juin 2004 pour la confiance dans l'économie numérique pour la communication au public en ligne.

La LCEN a pour but de renforcer la confiance dans les échanges sur Internet en établissant clairement la responsabilité de chacun des acteurs. En effet, elle permet de mieux protéger les internautes contre la présence de sites illicites (racistes ou pédophiles), le démarchage, la publicité en ligne, et la cybercriminalité dont ils sont parfois victimes. Le droit des contrats électroniques (en particulier des commandes en ligne) est également régi par ce texte. Cette loi transpose en droit français la directive européenne de juin 2000 sur le commerce électronique. La responsabilité des intermédiaires techniques a été clairement définie et plusieurs jugements ont d'ores et déjà été rendus en 2004 en s'appuyant sur cette loi pour exonérer des hébergeurs de responsabilité vis à vis des contenus.

La LCEN s'articule ainsi :

- les hébergeurs et les fournisseurs d'accès à Internet ne peuvent voir leur responsabilité engagée que de manière limitée ;
- en revanche, les éditeurs de contenus sont responsables, puisqu'ils sont à la source de l'information ;
- enfin, les opérateurs de télécoms, qui ne font que transmettre le signal sur le réseau, ne sont pas responsables, à moins d'avoir manipulé le contenu transporté.

Toutefois, la LCEN impose au fournisseur d'accès à l'Internet d'informer ses abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et doit leur proposer au moins l'un de ces moyens.

4.2.3 Loi d'Orientation et de Programmation sur Sécurité Intérieure.

La Loi d'Orientation et de Programmation sur la Sécurité Intérieure (LOPSI), adoptée le 29 août 2002 et promulguée le 9 septembre 2002, complète la Loi sur la Sécurité Quotidienne (LSQ). La LOPSI n'est pas un texte technique, mais comme son nom l'indique, une loi d'orientation et de programmation dans un domaine, celui de la sécurité, qui relève du domaine législatif.

En annexe du projet de LOPSI, le gouvernement établit l'inventaire des innovations à mener. Pour faciliter le travail des enquêteurs, des données de connexion peuvent être stockées sans passer par l'intermédiaire des opérateurs de télécommunications ou des fournisseurs d'accès. En effet, les officiers de police judiciaire sont autorisés, par un magistrat juge d'instruction, à accéder à des fichiers informatiques et à saisir les renseignements qui paraissent nécessaires à la manifestation de la vérité.

4.2.4 Loi sur la Sécurité Quotidienne.

La loi relative à la sécurité quotidienne du 15 novembre 2001, tout d'abord, a introduit dans le droit positif français certaines mesures sécuritaires spécifiques à Internet, dont notamment la conservation, pendant une **période d'un an**, des **données relatives à une communication** et ce « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales » (art.29). Ces données, précise la loi, ne peuvent « en aucun cas, porter sur le contenu des correspondances échangées ou des informations consultées sous quelque forme que ce soit » , mais concernent seulement l'identité des utilisateurs et les caractéristiques techniques des services fournis par les prestataires de communication (comme par exemple les adresses IP, les adresses de messagerie électronique envoyées ou reçues, ainsi que les adresses des sites visités).

L'article 30 de cette loi a, par ailleurs, modifié le code de procédure pénale en y insérant un chapitre concernant la mise en clair des données chiffrées nécessaires à la manifestation de la vérité. Ainsi, lorsque les données obtenues au cours d'une enquête ou d'une instruction ont été chiffrées, « le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire » .

4.2.5 La loi du 3 juillet 1985.

Toute reproduction autre que l'établissement d'un copie de sauvegarde par l'utilisateur ainsi que toute utilisation d'un logiciel non expressément autorisée par l'auteur ou ses ayant droit est passible des sanctions prévues dans la dite loi.

Donc, les articles du code pénal sur la contrefaçon en matière de droits d'auteur (écrits, peinture, musique, etc.) s'appliquent à la contrefaçon de logiciels.

4.3 Les textes règlementaires liés à la protection des mineurs.

Il existe des dispositions pénales relatives à la mise en péril des mineurs notamment :

- L'article 227-22 du Code pénal qui prévoit que le fait de favoriser ou de tenter de favoriser la corruption d'un

mineur est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé d'un réseau de télécommunication ou que les faits sont commis à l'intérieur d'un établissement scolaire.

- L'article 227-24 du Code pénal qui reprend pour partie l'incrimination de l'outrage aux bonnes mœurs des articles 283 et suivants du même Code mais la limite aux cas où le message présentant un caractère immoral serait susceptible d'être vu ou perçu par un mineur.

La LCEN renforce également les aspects liés à la protection de l'enfance comme suit :

- Maintien de l'obligation d'information en matière de logiciel de filtrage (article 6).

  L'article 6 maintient l'obligation , créée par la loi du 1er août 2000, imposée aux fournisseurs d'accès à l'Internet et aux fournisseurs d'accès mobile à l'Internet d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et de leur proposer au moins un de ces moyens.

- Modification du régime de responsabilité en matière d'exposition des mineurs à des contenus préjudiciables.

  En remaniant les articles 1er et 2 de l'architecture du droit de la communication, la LCEN a impliqué une modification dans l'application de l'article 227-24 du Code Pénal. En effet, l'article 1er crée une catégorie générique (la « communication au public par voie électronique ») qui se subdivise en « communication audiovisuelle » et en « communication au public en ligne ». Ainsi, pour qu'un texte vise explicitement l'Internet, il doit faire référence soit à la communication au public en ligne, soit à la communication au public par voie électronique. A l'inverse, dès lors que le texte ne fait référence qu'à la notion de « communication audiovisuelle », l'Internet n'est plus implicitement visé.

  En l'absence de modification de la référence à la communication audiovisuelle à l'article 227-24 du Code pénal (responsabilité du directeur de la publication), le schéma de responsabilité en cascade n'est plus susceptible de s'appliquer, en la matière, pour les contenus sur l'Internet (en pratique les responsables de sites ne pourront être poursuivis qu'à deux titres : d'une part, au titre de leur qualité d'éditeur du site et au titre de leur qualité d'hébergeur, d'autre part.

- Modification de l'incrimination concernant la pornographie infantile (article 44).

  Cet article a été inséré dans l'article 227-23 du code pénal qui prévoit : « Les peines sont portées à cinq ans d'emprisonnement et à 75 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de 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'emprissonnement et de 3000 euros d'amende ».

5. Les recommandations.

5.1 L'organisation des dispositifs.

La mise en oeuvre opérationnelle des dispositifs de sécurité en écoles nécessite des décideurs, un engagement fort et un travail en étroite coordination avec les responsables techniques dans la mesure où il leur revient d'impulser des actions de natures différentes qui recouvrent aussi bien la sensibilisation aux risques et enjeux de la sécurité que la détermination des moyens techniques et des technologies susceptibles de répondre à l'évolution de ces risques.

Différentes actions ont déjà été entreprises en ce sens, que ce soit par le biais d'une mise en place d'un réseau de compétences permettant de créer des chaînes d'alertes ou par l'élaboration d'un cadre de référence pour la mise en réseaux des écoles (S2I2E).

Ces actions doivent s'inscrire dans la durée et être complétées notamment par des dispositifs techniques renforcés décrits dans les paragraphes ci-après afin que les élèves puissent accéder aux ressources de l'Internet sans se mettre en danger ou menacer l'intégrité du réseau de l'école.

Aussi, la mise en oeuvre de ces quelques actions tend à prouver que la sécurité des mineurs est déjà pour partie prise en compte dans les services de l'Éducation Nationale mais qu'elle doit se développer davantage, notamment au travers des actions précisées ci-dessous.

5.2 Les compétences et moyens techniques nécessaires.

Afin d'aider les enseignants et d'accompagner les élèves dans leur utilisation de l'Internet, un contrôle des documents consultés et des informations fournies est nécessaire :

- **Pour la pédagogie** : Lors d'une séquence pédagogique, l'enseignant peut souhaiter développer l'exploration des ressources de l'Internet par ses élèves en autonomie. La personne responsable de l'activité ne peut pas accompagner chacun des élèves en permanence, il faut donc que cette pratique soit encadrée afin de permettre une utilisation la plus enrichissante possible.

  Ce cadrage de l'activité repose sur deux aspects : une formation et une sensibilisation à la spécificité de l'Internet pour tous les acteurs de l'école, et sur un contrôle des informations consultées

- **Pour la protection des mineurs** : Un certain nombre de sites peuvent présenter un contenu préjudiciable voire illégal, pour les élèves mineurs ou l'ensemble de la communauté éducative. La navigation libre sur l'Internet est un processus de passage d'un site à un autre, parfois sans liens entre eux. Afin d'éviter l'accès à des sites inappropriés (par exemple pornographiques, pédophile, xénophobes, racistes, antisémites, violents, …), la navigation sur l'Internet doit être contrôlée. Il est donc indispensable de mettre en place une politique d'accompagnement sur Internet.

  Toute mise à disposition de documents suppose un choix et donc une sélection dans le fond comme dans la forme vers l'intérêt de l'élève. Il semble donc naturel et indispensable que les écoles disposent de moyens d'accompagnement et de contrôle de l'usage de l'Internet dans le cadre pédagogique.

Conformément à la législation en vigueur, c'est au maire, en collaboration avec de l'Inspection Académique, à qui il appartient de prendre les mesures nécessaires (obligation de moyens). Il doit identifier les besoins, définis et validés par l'institution, exprimés par l'ensemble des acteurs, et choisir un dispositif qui permette de répondre aux impératifs de sécurité tout en prenant en compte les besoins des acteurs et des usagers.

5.3 La sensibilisation et la formation.

Les dispositifs de sécurité ne peuvent être efficients que s'ils sont perçus comme des bénéfices et non vécus comme des contraintes. Pour cela, un apprentissage minimal de la sécurité d'ensemble est nécessaire. Divers moyens doivent être utilisés pour y parvenir :

- Séminaires de sensibilisation et formation des équipes éducatives : Cette sensibilisation et responsabilisation, qui est déjà largement engagée dans l'Académie d'Aix-Marseille, est une étape indispensable à une utilisation

citoyenne de l'Internet. Elle demeure une nécessité et le fondement d'une véritable prise de conscience des problèmes éventuels.

- Formation des élèves au travers du Brevet Informatique et Internet (B2I) : Le Brevet Informatique Internet (B2I) constitue à cet égard une sensibilisation de premier niveau des élèves à la notion de sécurité des systèmes d'information.
- Mise en place de points d'informations dans toutes les écoles.

Parallèlement à ces actions, la charte d'utilisation des ressources et de bon usage des systèmes d'information doit être diffusée aux personnels, aux élèves et à leurs parents pour leur signifier leurs droits et devoirs en la matière. En effet, chaque école doit établir une charte d'utilisation de l'Internet et l'annexer au règlement intérieur. Elle doit être impérativement signée par les élèves et leurs parents dans le cas des élèves mineurs. Une charte école, est disponible sur le portail Pédagogie de l'Académie d'Aix-marseille (http://pedagogie.ac-aix-marseille.fr).

5.4 Les acteurs de la sécurité et leur responsabilité.

Le Schéma Directeur de la Sécurité des Système d'information (SDS SI) définit précisément les responsabilités de chacun des acteurs. Il définit en particulier la notion de **Personne Juridiquement Responsable** (PJR). La PJR doit être particulièrement sensibilisée sur la responsabilité juridique qui lui incombe en matière de sécurité du système d'information. Elle joue un rôle moteur dans la mise en place de l'organisation dédiée à l'application des mesures de sécurité définies dans le SDS SI et précisées dans par le présent document.

5.4.1 Les élèves et parents.

La sécurité des systèmes d'information de l'institution et des écoles repose avant tout sur l'adhésion de l'ensemble des acteurs du dispositif, usagers et représentants légaux. Principale catégorie d'usagers de par leur nombre, les élèves se doivent de respecter les lois en vigueur, les règles de sécurité et de déontologie édictées par l'entité, au travers d'une charte de bon usage des ressources utilisées.

La responsabilité des parents d'élèves mineurs, peut être envisagée, dans certains cas, sous deux angles:

- En tant que gardiens de l'autorité parentale,
- En tant que cosignataires ou signataires de la charte informatique et/ou du règlement intérieur (sanctions relevant de la violation d'obligations contractuelles – droit commun des contrats).

5.4.2 Les personnels de l'Éducation Nationale.

Exerçant une activité professionnelle au sein d'une entité relevant de la responsabilité d'une PJR, les personnels et autres intervenants (professionnels, associatifs...) se doivent de respecter la réglementation en général et tout particulièrement les règles de déontologie et de sécurité consignées dans la charte d'utilisation des ressources informatiques dont les PJR doivent assurer la diffusion (obligation de moyens).

En tant qu'utilisateur et/ou personnel de l'Etat, chaque individu est responsable en tout lieu et tout temps de l'usage qu'il fait des ressources informatiques, des réseaux ou des systèmes qui sont mis à sa disposition.

Dans le cas des enseignants, on se retrouve en présence :

- D'une **responsabilité civile** : article 1384 du Code Civil, principe de substitution (loi du 5 avril 1937), action récursoire.
- D'une **responsabilité pénale** : commission d'une infraction pénale (loi du 13 mai 1996 imprudence ou négligence, loi du 10 juillet 2000 diligence normale – violation délibérée de la loi et création d'une situation de risque), principe de protection dû aux fonctionnaires conformément aux dispositions de l'article 11 de la loi n°83-634 du 13 juillet portant droits et obligations des fonctionnaires).

D'autre part, lorsque le site est hébergé au sein d'une école ou d'un fournisseur d'accès à Internet, l'enseignant, qui en a assuré son élaboration, sera alors considéré comme le directeur de publication et assujetti aux responsabilités associées.

5.4.3 Le directeur d'école.

Le directeur d'école se doit de veiller à la bonne organisation générale du service de surveillance conformément à la circulaire n° 97-178 du 18 septembre 1997 (surveillance et sécurité des élèves dans les écoles maternelles et élémentaires publiques). Celle-ci est définie en conseil des maîtres qui a compétence pour émettre des avis et présenter des suggestions en matière de protection et de sécurité des enfants dans le cadre scolaire (décret n° 90-788 du 6 septembre 1990).

5.4.4 Le maire.

Les modalités de mise en œuvre du dispositif de filtrage sont définies sous la direction du maire en concertation avec les services de l'Inspection Académique. Il prend la décision de retenir une solution technique adaptée à ses écoles (obligation de moyens), sous les conseils des ressources académiques.

Si sa responsabilité ne peut être engagée en tant qu'**hébergeur** dans le cas de sites Web hébergés hors des services académiques, il en va autrement lors la commune offre un service d'hébergement Web à une école.

5.4.5 L'Inspecteur d'Académie.

L'Inspecteur d'Académie a en charge la mise en place d'un dispositif de formation et de sensibilisation à destination de l'équipe pédagogique et des élèves.

Les responsabilités de l'Inspecteur d'Académie sont des responsabilités afférentes au **directeur de la publication** pour les sites Web hébergés par les services académiques et notamment le Rectorat avec cependant une exception civile : usage hors service ou usage personnel.

5.4.6 Le Recteur.

Le Recteur, en tant que « Personne Juridiquement Responsable » est personnellement responsable de la définition et de l'application de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'Académie.

Ces responsabilités sont les suivantes :

- La responsabilité administrative générique ;
- Une obligation d'agir et de réagir ;
- Une responsabilité propre aux systèmes d'information (protection des systèmes, accès/hébergement, directeur de la publication).

5.5 Organisation de la sécurité au sein de l'Académie.

Un fonctionnement sans faille de l'accès à l'Internet ne peut être garanti par les seules mesures précédentes. Un certain nombre d'incidents peuvent survenir, notamment liés à l'accessibilité de pages inappropriées non filtrées. Une chaîne d'alerte a ainsi été définie permettant d'engager les mesures adaptées dans les meilleurs délais et d'assurer la circulation de l'information utile afin de maintenir un niveau de protection optimal.

Cette chaîne repose sur l'Inspecteur d'Académie, une cellule académique organisée autour du CTICE et du RSSI et une cellule nationale de coordination dont le rôle est précisé en annexe. L'Inspecteur d'Académie alerté par ses équipes pédagogiques de tout incident lié à la sécurité survenant dans son école, doit se mettre en contact avec la cellule académique qui contactera au besoin la cellule nationale de coordination.

5.5.1 Le Recteur.

Le Recteur est chargé au niveau académique de la coordination de l'action des Inspecteurs d'Académie.

5.5.2 Le RSSI coordinateur et correspondant académique.

Le Responsable de la Sécurité des Systèmes d'information académique centralise les remontées d'informations, en estime la gravité, effectue une remontée au niveau nationale si besoin, grâce à la chaîne de gestion d'urgences via une chaîne d'alerte (Cf. paragraphe 6.4 La Chaîne d'alerte).

6. Les moyens à mettre en oeuvre.

6.1 Le filtrage

Conformément à la circulaire DARCOS, il est obligatoire de mettre en place un contrôle automatique des pages consultées (filtrage) dans les écoles afin de rendre possible le travail en autonomie. Ces dispositifs techniques permettent de restreindre les accès à l'Internet et de présenter les documents intéressants selon le profil de l'utilisateur connecté. Plusieurs possibilités existent :

- Pour ceux qui bénéficient d'une architecture multiposte ou mutualisée, le filtrage au niveau du serveur mandataire ou « **proxy** » qui centralise l'ensemble des accès aux ressources web de l'Internet en provenance des postes clients,
- Pour les autres, l'emploi de logiciels de **filtrage autonomes**, au niveau du poste de l'utilisateur, qui ne se basent pas sur le système PICS (*) (Platform for Internet Content Selection - Plateforme de Sélection du Contenu sur Internet).

Dans les deux cas, le principe repose sur des listes de sites à filtrer, et des critères de filtrage par mots clés. Ces listes peuvent être des listes de sites interdits (listes noires), des listes de sites autorisés (listes blanches) ou une combinaison des deux. Les procédés de filtrage par mots clés permettent de se passer d'une classification des pages a priori en utilisant une analyse du site à la volée. Il n'y a donc pas besoin de répertorier les sites.

(*) L'efficacité de PICS dépend très fortement de l'adhésion des concepteurs de sites ou des organismes d'évaluation externes. A l'heure actuelle, ce n'est pas le cas, peu de sites sont classifiés. Si le choix est fait de refuser tous les sites non classifiés, l'utilisation de l'Internet se trouve fortement limitée : de nombreux sites, non classifiés, vont être bloqués lors de la navigation alors qu'ils peuvent correspondre au profil de l'utilisateur. Par conséquent, ce système ne peut pas remplir le rôle de filtrage et ne répond donc pas aux objectifs de l'Éducation Nationale.

6.1.1 Le serveur mandataire ou proxy.

L'architecture type proposée est de choisir un serveur mandataire qui propose déjà des fonctionnalités de filtrage. Le logiciel Squidgard, par exemple, est un logiciel libre intégré dans plusieurs projets soutenus par l'Éducation Nationale : EOLE, SLIS, pingoo, linuxedu, certains S2i2e, etc. Il s'agit d'un greffon (plug-in) destiné à Squid (serveur mandataire libre très utilisé) qui apporte les fonctionnalités de filtrage. Il permet entre autres fonctionnalités de :

- Bloquer l'accès à un ensemble de sites définis par une liste noire pour certaines catégories d'utilisateurs,
- Rediriger un accès à une page interdite vers une autre page,
- Limiter l'accès à l'Internet dans le temps,
- Autoriser l'accès à un nombre limité de pages web,
- Journaliser les accès à l'Internet (logs).

6.1.2 Les filtres autonomes.

Il existe sur le marché des logiciels de filtrage autonomes, au niveau du poste de l'utilisateur et qui ne se basent pas sur le système PICS.

Ces produits de filtrage reposent sur des listes de sites à filtrer, et des critères de filtrage par mots clés. Ces listes peuvent être des listes de sites interdits (« liste noire »), des listes de sites autorisés (« liste blanche ») ou une combinaison des deux.

Ce type de logiciel ne demande donc pas d'évaluation du site par le concepteur, mais ce sont directement les éditeurs du logiciel de filtrage qui peuvent fournir une liste de sites à interdire. Ce sont aussi les administrateurs du poste de travail qui peuvent sélectionner cette liste.

Le procédé de filtrage par mots clés permet de se passer d'une classification des pages a priori en utilisant une analyse du site à la volée. Il n'y a donc pas besoin de répertorier les sites.

Listes noires.

Pour bloquer l'accès aux contenus inadaptés, les logiciels de contrôle parental utilisent deux méthodes principales : le filtrage par liste d'URL et le filtrage par mot clés.

Méthode la plus répandue, le filtrage par liste fonctionne avec une base de données de sites déconseillés. Appelées aussi « listes noires », ces bases contiennent des adresses de sites classés selon différents thèmes. Ainsi, quand l'enfant souhaite visiter une page web, l'URL du site est d'abord comparée aux URL interdites entrées dans la liste noire du logiciel. Si l'adresse en question fait partie des sites déconseillés, l'enfant ne peut pas y accéder.

L'inconvénient de ce type de système réside dans la nécessité de réaliser des mises à jour très régulières.

En outre, la langue utilisée est un critère important dans le choix du logiciel car si celui-ci bloque le mot en français il ne le bloquera pas forcément s'il est entré en anglais, la protection peut de fait être aisément contournée.

Une liste noire nationale de sites inappropriés est mise à disposition des communautés éducatives. Les documents d'accompagnement et leurs évolutions sont tenus à jour sur un site de référence. La Personne Juridiquement Responsable (PJR) est chargée de veiller à la mise en oeuvre du dispositif.

Listes blanches.

Une liste blanche contient l'ensemble des sites sur lesquels la navigation peut avoir lieu. C'est donc un ensemble de sites autorisés.

Dans le cas d'une école, une liste blanche, est un ensemble d'URL dont l'intérêt pédagogique ou pratique a été clairement identifié et pour lesquelles une autorisation d'accès a été explicitement exprimée. Les listes blanches sont parfois opposées aux listes noires constituées d'un ensemble d'URL dont la consultation est explicitement interdite.

Par exemple, une liste blanche s'adressera à un public d'élèves pour la matière Histoire. Elle sera constituée de l'ensemble des signets relatifs à l'Histoire et déclarés comme accessibles aux élèves de terminale. La liste blanche peut s'apparenter à l'ensemble des signets contenus dans un répertoire thématique d'un navigateur Internet.

6.2 L'authentification.

Pour pouvoir ouvrir l'accès d'un site ou d'une zone de confiance à des mineurs, la reconnaissance des individus en tant que tels devient impérative. D'autre part, toutes les sessions doivent être authentifiées, besoin nécessaire vers une authentification unique en cohérence avec les directives nationales.

L'accès authentifié par un service d'annuaire doit pouvoir associer l'identification de l'utilisateur avec un type de profil (mineurs, enseignants, éducateurs, ...) pour permettre un filtrage par type d'utilisateur. L'accès Internet depuis les zones administratives et élèves doit pouvoir être défini selon des plages horaires qui peuvent être différentes selon le profil et la zone concernée.

L'authentification constitue le facteur clé de la reconnaissance d'un individu et des contrôles d'accès associés. De sa qualité et de sa robustesse dépendent la protection des mineurs.

6.3 La traçabilité.

L'ouverture des systèmes d'information de l'Éducation Nationale aux élèves (et plus particulièrement des mineurs), personnels et partenaires au travers de réseaux publics comme l'Internet implique une politique de contrôle des accès au niveau utilisateur afin de se prémunir contre les actes malveillants.

Dans ce cadre, la loi prévoit des mécanismes de « journalisation » des accès, afin de pouvoir engager la responsabilité d'un utilisateur dérogeant à la charte. La durée de conservation de ces données est également définie dans la loi (décret du 26 mars 2006).

La mise en place de tels mécanismes doit être signalée dans le règlement intérieur du site (charte de bon usage des réseaux, de l'Internet et des ressources multimédias) afin d'en informer les usagers. De même, un projet de déclaration de gestion

des traces sera établi et soumis à la CNIL.

6.4 La chaîne d'alerte.

La chaîne d'alerte doit être utilisée afin d'informer l'ensemble des acteurs. La circulation de l'information est primordiale afin d'assurer une réponse optimale à chaque problème posé. La chaîne d'alerte doit être utilisée dans les cas suivants :

- Découverte d'un site Internet inapproprié accessible : la cellule de gestion de la liste noire doit être prévenue ;
- Découverte d'un site Internet injustement filtré : la cellule de gestion de la liste noire doit être prévenue ;
- Besoin d'une assistance psychologique suite à la consultation de sites inappropriés ;
- Demande des médias en cas de crise.

Organisation de la chaîne d'alerte

La chaîne d'alerte s'organise comme suit :

- Au sein de chaque école, les membres de l'équipe pédagogique informent l'Inspection Académique des incidents constatés.
- La cellule académique constituée autour du RSSI et du CTICE est informée des incidents se produisant dans les écoles par l'Inspecteur d'Académie. Si localement l'incident n'a pu être résolu, les ressources académiques telles que les psychologues, les techniciens sécurité, conseillers juridiques des rectorats et des inspections académiques pourront être sollicités. Ces structures devraient pouvoir traiter la plupart des incidents.
- Cette cellule académique informe la cellule nationale de coordination par l'intermédiaire des dispositifs d'assistance mis à disposition. Au besoin, le haut fonctionnaire de défense est informé par la chaîne d'alerte définie dans le schéma directeur de la sécurité. Si l'incident n'a pu être résolu au niveau académique, des ressources spécialisées, notamment dans les domaines psychologique, judiciaire et liés à la sécurité seront sollicitées.

La circulation de l'information par cette chaîne d'alerte est le moyen le plus efficace d'améliorer la liste noire nationale. En effet le site (site web de remontée d'informations sur la liste) permet d'indiquer à la cellule responsable de la gestion de la liste noire, des sites inappropriés pour l'instant non répertoriés par la liste noire. La contribution de tous les acteurs permettra d'obtenir une liste de plus en plus complète et qui remplira d'autant mieux son rôle.

Procédure d'alerte

Dans chaque département, les écoles sont informées des procédures d'alertes, par l'intermédiaire d'affichettes qui sont apposées dans chacune d'entre elles.

7. Conclusion.

Les usages de l'Internet posent des questions de responsabilité, de comportements, de connaissance d'un environnement difficile complexe et évolutif. C'est pourquoi, il convient de définir les outils et les conditions nécessaires à une pratique sécurisée de l'Internet par les enfants (et notamment les mineurs) et à l'exercice des responsabilités afférentes.

La direction de la technologie (SDTICE), sensible aux questions de sécurité sur Internet, a engagé un certain nombre d'actions pour le respect de la loi et des personnes dans l'enceinte des écoles. Ce plan national systématique de protection des élèves, paru au BOEN (Bulletin officiel de l'éducation nationale) du 26 février 2004, s'articule autour de deux axes prioritaires :

- d'une part la formation, la sensibilisation et la responsabilisation des élèves, enseignants et équipes éducatives aux spécificités de l'Internet (chartes d'utilisation de l'Internet) ;
- d'autre part une aide aux équipes éducatives par la mise à disposition d'outils leur permettant de sélectionner ou de contrôler l'information mise à disposition des élèves par exemple à partir de systèmes de filtrage (mise à disposition d'une liste « noire » nationale des sites délictueux).

C'est dans cette perspective que l'Académie d'Aix-Marseille a élaboré le présent **Référentiel de la sécurité informatique en écoles**. Il s'agit d'un outil qui permet d'offrir un cadre de référence cohérent à l'ensemble des acteurs et des activités d'une école. Il doit sensibiliser aux risques qui menacent les élèves ainsi qu'aux moyens disponibles pour s'en prémunir. Sa diffusion à l'ensemble de la communauté éducative mais également aux représentants des collectivités locales et territoriales contribue une prise de conscience et une implication de tous dans la protection des mineurs dans le cadre pédagogique.

8. Annexes.

8.1 La charte d'usage des TIC et de l'Internet

Chaque école doit établir une charte d'utilisation de l'Internet et l'annexer au règlement intérieur. Cette charte, à laquelle adhèrent les membres des équipes éducatives, doit être signée par les élèves ou par les parents dans le cas des enfants mineurs.

Une charte école est annexée au présent document.

8.2 Les blogs.

L'un des objectifs de l'adhésion de tous, et des élèves en particulier, à la « Charte d'usage des TIC et de l'Internet » est de faire prendre conscience des risques inhérents au « surf » sur l'Internet, aux échanges sur les « chats » et à la pratique des « blogs ». Le terme « blog » est une abréviation de « weblog » qui signifie journal sur Internet. Bien souvent, il s'agit d'une sorte de journal intime publié Internet et pouvant contenir des textes, des photos, des vidéos.

On peut créer un blog de manière très simple, sans aucune connaissance particulier, en utilisant des sies de blogs (le plus utilisé par les jeunes est http://www.skyblog.com/).

Comme des incidents ont eu lieu récemment dans plusieurs collèges et lycées à cause du contenu de certains blogs d'élèves, une lettre a été adressée aux Recteurs d'Académie, le 26 avril 2005 (DUI n° 2005-045), pour les alerter sur cette question et leur rappeler les mesures à prendre.

Si les « blogs », comme les « chats », interviennent dans le développement personnel des enfants, en leur permettant de communiquer et d'échanger sur les loisirs, le sport, les sorties, l'amitié, les amours, les difficultés de la vie, les questions existentielles, etc.. Ce qui, avant l'Internet, ne sortait pas de la discussion dans le cercle restreint des « copains » est désormais accessible à la terre entière. Or, le « blogueur » en est, la plupart du temps, inconscient, tout comme il ignore qu'il risque une punition disciplinaire et une sanction judiciaire :

- s'il reproduit et diffuse des productions intellectuelles sans l'accord des personnes qui en détiennent le droit d'exploitation ;
- s'il enregistre, adapte ou modifie des informations révélant la vie privée des personnes ou permettant leur identification ;
- s'il diffuse des informations à caractère diffamatoire, injurieux, obscène, offensant, violent, pornographique, portant atteinte au respect et à la dignité de la personne humaine ou incitant à la violence politique, raciste ou xénophobe ;
- s'il communique des messages présentant sous un jour favorable le banditisme, le vol, la haine ou inspirant des préjugés ethniques ou discriminatoires.

Le travail à mener par l'équipe éducative (et par les parents) est donc, avant toute chose, d'informer et de sensibiliser sur les enjeux et les risques de l'Internet en général et des « blogs » en particulier. Prévenir les possibilités de « dérapage » en privilégiant l'acquisition d'une démarche citoyenne et critique, tel est le rôle de la « charte d'usage » mais aussi l'une des composantes des compétences sanctionnées par le Brevet informatique et Internet (B2i).

9. Terminologie.

Sigle,Terme.	Définition
B2I	Brevet Informatique et Internet
BO	Bulletin Officiel
BOEN	Bulletin Officiel de l'Éducation Nationale
CE	Communauté Européenne
C2I	Certificat Informatique et Internet
CNIL	Commission Nationale de l'Informatique et des Libertés
CRM	Customer Relationship Management ou gestion de la relation client
CTICE	Conseillers aux Technologies de l'Information et de la communication pour l'enseignement scolaire
DATSI	Direction Académique des Technologies et des Systèmes d'Information
DUI	Délégation aux Usages de l'Internet
EOLE	Ensemble Ouvert Libre Evolutif
EPLE	Établissement Public Local d'Enseignement
HTML	Hypertext Transfer Markup Language
HTTP	HyperText Transfer Protocol
IEN	Inspecteur de l'Éducation Nationale
IP	Internet Protocol
IA	Inspection Académique
JO	Journal Officiel
IUFM	Institut Universitaire de Formation des Maîtres
LCEN	Loi de Confiance dans l'Economie Numérique
LDAP	Lightweight Directory Access Protocol
LOPSI	Loi d'Orientation Pour la Sécurité Intérieure
LSQ	Loi sur la Sécurité Quotidienne
PAGSI	Programme d'Action Gouvernemental pour la Société de l'Information
PICS	Plateforme de Sélection du Contenu sur Internet
PROXY	Serveur mandataire
PJR	Personne Juridiquement Responsable
RACINE	Réseau d'Accès et de Consolidation des Intranets Éducation
RENATER	REseau NATional de rechERche en télécommunications
RSSI	Responsable de la Sécurité des Systèmes d'Information
S2I2E	Services Intranet/Internet d'Etablissements scolaires et d'Ecoles
S3IT	Schéma Stratégique des Systèmes d'Information et des Télécommunications
SDI	Schéma Directeur des Infrastructures
SDS SI	Schéma Directeur de la Sécurité des Système d'information
SIAP	Système d'Information et d'Aide pour les Promotions
TIC	Technologies de l'Information et de la Communication
TICE	TIC pour l'Éducation
URL	Uniform Ressource Location

Documents de référence.

Les documents cités en référence ont servi de base de travail pour rédiger ce document.

Nom du document	Propriétés
Circulaire DARCOS : Usage de l'Internet dans le cadre pédagogique et protection des mineurs	Ministère de l'Éducation Nationale, de l'Enseignement Supérieur et de la Recherche
Schéma directeur de la sécurité des systèmes d'information - organisation et orientation de la sécurité des systèmes d'information pour les communautés éducatives	Ministère de l'Éducation Nationale, de l'Enseignement Supérieur et de la Recherche
Rapport sur la Protection de l'enfant et usages de l'Internet	Ministère des Solidarités, de la santé et de la famille
Présentation Sécurité des Systèmes d'Information dans les EPLE : aspects techniques et juridiques	Académie d'Aix-Marseille
Séminaire Eole - Sécurité Réseau Informatique dans l'EPLE	Académie d'Aix-Marseille
Portail Juridi-tice. Ces document sont consultables sur http://www.pedagogie.ac-aix-marseille.fr/tice/juridique/index.php	Académie d'Aix-Marseille
OASI: observatoire académique des systèmes d'information. Ces document sont consultables sur http://oasi.ac-aix-marseille.fr	Académie d'Aix-Marseille

aix-marseille

rectorat
place Lucien Paye
13621 Aix-en-Provence, cedex 1

responsables de la publication
direction **a**cadémique des **t**echnologies et des **s**ystèmes d'**i**nformation **(datsi)**
téléphone **04 42 91 74 55**
télécopie **04 42 91 70 10**
ce.datsi@ac-aix-marseille.fr
conseiller pour les **t**echnologies de l'**i**nformation et de la **c**ommunication pour l'**e**nseignement **(ctice)**
téléphone **04 42 91 75 91**
télécopie **04 42 91 70 10**
pole.tice@ac-aix-marseille.fr

date de parution
novembre 2006
photographies
licences computers art
& stéfane guilbaud
impression
spi imprimerie septèmes