Gouvernance des contenus audiovisuels sur Internet et protection de la jeunesse

État de la situation et pistes de solution

présentée à :

Régie du cinéma Québec

par

ISOC QUÉBEC

2007-01-31

Table des matières

Table des figures

Table des tableaux

Sommaire

Depuis la création de la Régie du cinéma du Québec en juin 1983, rares sont les films projetés au Québec, documentaires ou fictions, vidéos ou bobines, qui ne soient pas passés entre ses mains.

La Régie cote chaque film suivant son contenu et détermine l'âge du public qui devrait y avoir accès. Les distributeurs, exploitants de salles de cinéma ou de clubs vidéos et autres commerçants s'assurent ainsi que les jeunes qui visionnent ou louent ces produits sont informés des recommandations de la Régie du cinéma. Les stations de télévision sont également tenues d'informer le public de la cote attribuée par la Régie du cinéma du Québec aux contenus qu'elles proposent à leur auditoire.

Avec la venue d'Internet, le rôle de tous ces acteurs se trouve bouleversé par la transformation qui s'opère avec ce nouveau média : les canaux de distribution explosent. Désormais, dans le monde d'Internet, toute personne, jeune et adulte, peut accéder à tout contenu audiovisuel, quelle que soit sa nature. Si bien qu'un jeune peut fréquemment se retrouver devant des images blessantes ou traumatisantes (racisme, violence, pornographie voire pédopornographie), sans mécanismes de protection ou d'alerte.

Le classement des documents audiovisuels devient une notion vague ou carrément absente dans les sites Internet. Cette situation interpelle la Régie du cinéma dans l'accomplissement de sa mission, soit la sensibilisation des auditoires aux contenus mis à leur disposition et, partant, la protection de la jeunesse.

C'est pourquoi la Régie, de concert avec ISOC Québec, a initié la présente étude sur la gouvernance des contenus audiovisuels sur Internet afin :

- de dresser un état de situation dans les autres gouvernements et organismes de classement face à la question de cette gouvernance;
- d'établir l'inventaire des stratégies de codification et de classement du contenu sur Internet;
- d'évaluer leur portée et les mécanismes ou outils nés avec l'Internet qui offrent des moyens de les mettre en application.

D'entrée de jeu, distinguons dans Internet la gouvernance qui se rapporte aux contenus de celle qui se rapporte aux technologies de l'information et aux communications qui leur donnent vie.

La gouvernance des contenus audiovisuels sur Internet s'exerce tantôt sur le plan local, tantôt sur les plans national, régional ou mondial. On résume en trois modes de régulation cette gouvernance des contenus : par l'autorégulation (sans aucune intervention de l'État), par corégulation (délégation au secteur privé tout en conservant le pouvoir de réviser cette délégation) ou par régulation classique (loi ou directive de l'État).

Des travaux de réflexion et d'orientation ont été réalisés au niveau mondial ces dernières années entourant la gouvernance d'Internet. Ces travaux peuvent se classer ainsi : gouvernance technique d'Internet, gouvernance des services et gouvernance des contenus.

La gouvernance technique se caractérise principalement par un ensemble de normes et de pratiques élaborées et mises en place par des organismes internationaux qui permettent à Internet de communiquer d'un réseau national de télécommunications à un autre de façon rapide et transparente. Un organisme important est l'Organisation internationale de normalisation (ISO) qui gère quelque 15 000 normes dont certaines en matière d'audiovisuel numérique.

La gouvernance technique touche aussi le système de gestion des noms de domaines et d'adresses correspondantes, appelé Domain Name System (DNS), géré par l'organisation Internet Corporation for Assigned Names and Numbers (ICANN). Ainsi, le nom de domaine de la Régie du cinéma www.RCQ.qc.ca correspond à une adresse numérique unique (exemple : 199.84.128.1) qui lui permet d'être retrouvé sur Internet. Pour que tout fonctionne bien, l'ICANN a déployé une organisation répartie à l'échelle mondiale. Cette gouvernance technique s'appuie sur un ensemble de normes définies, notamment par l'Internet Engineering Task Force (IETF) rattaché à l'organisation ISOC (Internet Society à laquelle ISOC Québec est reliée) et par le World Wide Web Consortium (W3C - Organisme de normalisation du Web).

La gouvernance des services et des contenus d'Internet est plus jeune et moins riche en organisations et en normes. Lors des événements du Sommet mondial sur la société de l'information (SMSI), les pays ont convenu d'établir un « cadre de référence de la régulation du contenu visant à protéger les utilisateurs d'Internet de contenu nuisible et d'abus en ligne, mais uniquement en relation avec les enfants et les adolescents. » Ce cadre reste à structurer, même si l'Europe et d'autres pays ont commencé à sérieusement s'y mettre, appuyés par l'Organisation des Nations Unies pour la Science, l'Éducation et la Culture (UNESCO).

Une organisation vouée à la gouvernance du contenu, soit l'Internet Content Rating Association (ICRA), a établi une structure de codification du contenu sur Internet qui permet à chaque site Web d'offrir son contenu codifié, un peu comme un film porte son classement. L'initiative de l'ICRA fait école à ce chapitre.

Voyons à ce sujet le portrait que fait l'étude de trois provinces canadiennes, du gouvernement fédéral canadien ainsi que de neuf autres pays, incluant l'Europe comme pays. Les résultats de cette comparaison sont les suivants, pour les pays étudiés :

- Un seul des gouvernements, celui du Danemark, a intégré en un seul organisme la responsabilité du classement des films, vidéo et DVD ainsi que la gouvernance sur le contenu audiovisuel véhiculé par les jeux et Internet;
- Un seul gouvernement, soit l'Australie, maintient le même système de classement pour les films et pour Internet, mais le contenu sur Internet est classé par l'industrie en mode volontaire (autorégulation) et il est difficile d'évaluer jusqu'à quel point c'est fait;
- Tous les gouvernements étudiés sauf ceux des provinces canadiennes, ont attribué à un organisme gouvernemental un rôle de gouvernance du contenu sur Internet à des fins de protection de la jeunesse;
- Tous les gouvernements ont recours à la régulation classique et ont légiféré pour combattre la cybercriminalité, et particulièrement la pornographie infantile;
- Tous les gouvernements ont attribué aux organisations sans but lucratif un rôle important d'alphanétisation1 des jeunes, des parents, des éducateurs et des représentants de la loi;
- Tous les gouvernements ont élaboré un programme d'alphanétisation, à l'exception de ceux des provinces canadiennes;
- Certains pays ont commencé à rendre obligatoire l'accès à des services de filtrage des sites Web afin d'en distinguer ceux de nature pour adulte;
- Tous les pays mènent une lutte importante contre la cybercriminalité et le pollupostage, sources de dangers pour la jeunesse;
- Tous les pays, sauf le Canada, se sont dotés d'une loi régissant le pollupostage;
- Tous les pays, sauf le Canada, ont délaissé le mode d'autorégulation pour ce qui a trait à l'accès à l'Internet par mobile;

[1] Alphanétisation : la formation à l'utilisation d'Internet.

- Quelques pays ou provinces ont mis en place une authentification citoyenne pouvant servir de façon sûre à distinguer un jeune d'un adulte sur les sites interactifs d'Internet (lieu de risque). La Belgique s'en sert pour authentifier les jeunes sur un site de clavardage;
- La codification selon l'âge et selon le type de contenu est encore peu courante dans les différents pays mais, pour le contenu accédé par mobile, une certaine tendance se dessine dans la moitié des pays afin de le codifier selon au moins deux classes d'âge (moins de 18 ans et 18 ans et plus);
- La codification selon la taxonomie de l'ICRA est peu répandue (environ 200 000 sites Web en 2006);
- Diverses homologations disparates de contenus ou de fournisseurs ont été initiées par la plupart des pays sauf au Canada ou dans ses provinces;
- Différentes stratégies de filtrage du contenu étudiées permettent globalement de codifier le contenu audiovisuel sur Internet selon l'âge ou selon le type de contenu. Il peut se faire de trois façons :
    - en assignant une étiquette (ou méta-donnée) au contenu selon une codification publique, un peu comme le propose l'ICRA;
    - en assignant un code à un contenu et en emmagasinant le résultat dans une base de données propriétaire (généralement);
    - en assignant une classe d'âge aux sites Web (moins de 18 ans et 18 ans et plus) et en emmagasinant les noms des sites Web dans une « liste verte » (pour les moins de 18 ans) ou une « liste rouge » (pour les 18 ans et plus).

L'ICRA propose une codification selon le type de contenu mais son utilisation, même si elle est officiellement appuyée par l'Europe, n'est pas très répandue. Cependant, la décision de Microsoft de soutenir la nouvelle version de la taxonomie de l'ICRA dans les nouvelles moutures de son fureteur pourrait augmenter le soutien à l'ICRA de façon très significative. Celle utilisée par les logiciels de filtrage est aussi basée sur le type de contenu. Mais actuellement il y a très peu de contenu audiovisuel codifié sur Internet, à moins de passer par un logiciel de filtrage propriétaire ou une liste verte ou rouge.

Une fois le contenu codifié ou les règles de codification établies, une pléthore de logiciels pourront utiliser ce résultat pour effectuer le filtrage, par exemple :

- portail pour les jeunes;
- moteur de recherche pour les jeunes;
- logiciel de filtrage de sites Web;

- vérification de l'identité et de l'âge;
- modération des forums, blogues et clavardage;
- logiciel de filtrage des pourriels;
- logiciel de contrôle parental.

La codification des sites Web par les logiciels propriétaires et la constitution des listes vertes et rouges soulèvent beaucoup de problèmes éthiques et légaux : surfiltrage de sites Web au contenu anodin (comme la Constitution des États-Unis) ou sousfiltrage de sites Web pourtant carrément offensants. Les études sur la fiabilité de filtrage des logiciels montrent que le surfiltrage peut atteindre près de 25 % des sites Web alors que le sousfiltrage semblait stable à 10 %. Donc, quels que soient les moyens de filtrage utilisés,

- le jeune aura accès à du contenu audiovisuel offensant;
- le jeune verra bloqué l'accès à du contenu audiovisuel pouvant lui être utile, comme celui en matière d'éducation sexuelle.

Une étude québécoise publiée en 2006 montre d'ailleurs que tous les adolescents ont été en contact avec de la pornographie sur Internet. On peut en tirer les constats suivants :

- l'importance de l'alphanétisation afin que les internautes québécois connaissent les risques inhérents à l'utilisation d'Internet et les façons d'y faire face;
- les défis reliés à la gouvernance des contenus sur Internet et l'importance de provoquer une réflexion de fond sur les mécanismes actuels de régulation, de sensibilisation et d'information sur les contenus accessibles sur Internet;
- le rôle historique des organismes de sensibilisation comme la Régie du cinéma et l'importance qu'ils s'adaptent aux défis de la gouvernance des contenus dans un monde virtuel et numérique.

Nous avons donc élaboré un ensemble de recommandations ou de pistes d'actions sur la gouvernance du contenu audiovisuel sur Internet au Québec. Elles touchent aux aspects suivants :

- le type de régulation à adopter, sachant que certains éléments sont de portée fédérale (comme les mobiles) et d'autres internationaux;
- la nécessité et le rôle d'une organisation gouvernementale centrale concernant cette gouvernance;
- l'adaptation des lois, politiques ou orientations gouvernementales;

- la classification du contenu audiovisuel sur Internet;
- un programme québécois de protection de la jeunesse incluant l'alphanétisation, l'accès à des services de filtrage, la cybercriminalité, l'homologation et l'authentification;
- la gestion du système de gestion des noms et des adresses d'Internet (Domain Name System – DNS).

1. Objectifs et enjeux de la Régie du cinéma

Cette étude sur la gouvernance d'Internet vise à répondre à un certain nombre de questionnements de la Régie du Cinéma et, partant, de la société québécoise, sur le contenu véhiculé par Internet et accessible par de plus en plus de médias numériques qui dépassent largement les salles de cinéma, les cassettes vidéo et les DVD.

Objectifs

Les objectifs de cette étude sont au nombre de trois, à savoir :

1. Dresser l'état de la situation des autres gouvernements et organismes de classement face à la question de la gouvernance du contenu sur Internet quant à son contenu véhiculé. Cet objectif va permettre de répondre à des questionnements tels que :
   - Quelle est la position de principe des États les plus représentatifs en matière de gouvernance du contenu sur Internet?
   - Quels sont les programmes et règlements mis en place, si règlements il y a?
   - Quel est le degré d'application de ces règlements, si application il y a?
   - Quels sont les autres éléments distinctifs ou significatifs relevés?
   - Quel est le degré de succès de ces programmes et règlements?

2. Établir l'inventaire des filtres et des stratégies actuelles de codification et de classement du contenu sur Internet et en réaliser leur évaluation. Cet objectif va permettre de répondre à des questionnements tels que :
   - Quels sont les moyens techniques pour réaliser le filtrage du contenu sur Internet?
   - Quelles sont les étapes pour arriver à les appliquer?
   - Quelles sont les stratégies de codification et de classement possibles?
   - Quel est le degré d'application de ces filtres et stratégies?
   - Quel est le niveau d'atteinte du filtrage désiré du contenu au moyen de ces filtres et stratégies?
   - Quel est le degré de compatibilité de la codification du contenu sur Internet et du film?

3. Dégager des pistes d'actions concrètes pouvant être envisagées par la Régie du cinéma et la société québécoise si l'on désire mettre en place la gouvernance du contenu sur Internet respectant la culture et les valeurs québécoises.

Enjeux

L'arrivée d'Internet vient questionner de manière directe la stratégie d'intervention de la Régie du cinéma en matière de contrôle d'accès aux films. En effet, Internet offre un nouveau canal de diffusion des images et les jeunes utilisent de plus en plus Internet et même le préfèrent à d'autres canaux de diffusion tels que la télévision. Or, on sait qu'actuellement, les documents audiovisuels accessibles sur Internet ne sont pas tous destinés aux jeunes. C'est pourquoi la Régie du cinéma se questionne sur la façon de prémunir les jeunes contre des sites ou contenus inconvenants.

Seuls les enjeux concernant la protection de la jeunesse sont considérés lors de cette étude, ceux reliés à l'économie ne le sont pas, du moins directement. Les enjeux reliés à la protection de la jeunesse recouvrent un vaste champ de préoccupation que l'on peut regrouper ainsi :

- Enjeu par rapport à la violence (telle que blessure, mutilation, mort de personnages réels ou fictifs);
- Enjeu par rapport à la sexualité, incluant la nudité;
- Enjeu par rapport à la langue et son niveau de langage;
- Enjeu par rapport à des activités dangereuses (telles que celles ayant trait à l'alcool, le tabac, les armes, le jeu, etc.);
- Enjeu par rapport aux stéréotypes (tels que le sexisme);
- Enjeu par rapport à la haine (tel que racisme);
- Enjeu par rapport à la protection de la vie privée.

Il est important de souligner un autre enjeu soulevé par la protection de la jeunesse : celui de la **liberté d'expression**. Cet enjeu peut venir en opposition avec l'enjeu de la protection de la jeunesse, surtout au niveau des mécanismes de protection mis en place. Cet enjeu de la liberté d'expression est aussi rejoint par l'**enjeu du développement de l'industrie québécoise du cinéma et de l'image**. Ces doubles enjeux

seront pris en compte lors de l'élaboration de pistes d'actions concrètes qui seront soumises à la Régie du cinéma.

Tous ces enjeux, on le devine, sont partagés par une multitude de sociétés à travers le monde. Ils revêtent un caractère distinct et sont interprétés selon les valeurs de chacune de ces sociétés. C'est pourquoi on retrouve dans la plupart de celles-ci des organismes de classement des oeuvres cinématographiques telle que la Régie du cinéma au Québec. Nous touchons donc directement à la spécificité de la culture et des valeurs québécoises. Par contre, actuellement, des organismes internationaux, et souvent américains, proposent des solutions de classement et de filtrage des contenus sur Internet. Nous faisons donc face à l'**enjeu de la protection de la spécificité des valeurs québécoises** en voulant étendre le classement aux oeuvres véhiculées par Internet. Cet enjeu demeure donc présent durant toute cette étude.

2. Définition de termes

Il est nécessaire de définir un certain nombre de termes importants pour cette étude afin de partager une compréhension commune entre les participants de la Régie du cinéma et ceux d'ISOC Québec et de permettre une compréhension plus facilement et rapidement de cette étude par le lecteur. Ces définitions permettent de délimiter la portée de l'étude autant pour la revue de littérature réalisée, en grande partie, par la Régie du cinéma que pour les autres étapes réalisées par ISOC Québec. Dès le début de l'étude, il a été convenu de définir un certains nombre de termes auxquels, en cours d'étude, d'autres se sont ajoutés. Les définitions retenues portent sur les termes suivants :

- Gouvernance;
- Gouvernance d'Internet;
- Gouvernance des contenus sur Internet;
- Type de contenu;
- Médias numériques;
- Neutralité de l'architecture d'Internet;
- Web sémantique;
- Codification et classement des contenus audiovisuels numériques;
- Filtrage des contenus audiovisuels numériques codifiés;
- Société civile, gouvernements et secteur privé;
- Alphanétisation;
- Sécurité et sûreté d'Internet.

Voici donc ces définitions.

Gouvernance

Nous retrouvons tout d'abord trois termes qui méritent d'être distingués de façon claire par rapport au sujet de l'étude, soit « gouvernance », « gouvernance d'Internet » et « gouvernance des contenus sur Internet ». Nous constatons d'emblée que ces trois termes passent du général au particulier.

Le terme « gouvernance » est défini par l'Office québécois de la langue française (OQLF) comme étant une « manière d'orienter, de guider, de coordonner les activités d'un pays, d'une région, d'un groupe social ou d'une organisation privée ou publique ». La gouvernance, « renvoie à un processus de coordination qui permet à l'exercice des pouvoirs politiques, économiques et administratifs de s'effectuer à tous les niveaux de la structure du système national, régional et local par différents acteurs disposant à des degrés divers de pouvoirs de décision. Elle se traduit donc concrètement par une participation accrue de la société civile organisée à l'élaboration des décisions et à leur mise en œuvre. »

On peut le constater, le terme « gouvernance » peut s'appliquer à différents secteurs, que ce soit aux entreprises ou aux gouvernements, ou à des domaines de préoccupations planétaires comme l'environnement, la santé, l'éducation et le développement durable.

Bien que ce terme soit apparu dans les années 1930, il est devenu particulièrement à la mode au début des années 2000 avec les concepts de transparence de la gestion, de l'imputabilité des gestionnaires, de reddition de comptes, de l'adéquation des contrôles et de la participation citoyenne. Si on scrute quelque peu le Web, on peut retrouver moult instituts et chaires de recherche en gouvernance d'institutions publiques et privées.

Du côté des entreprises, on n'a qu'à se référer aux scandales financiers de firmes comme Enron aux États-Unis, Nortel et Norbourg au Canada où les rapports financiers des compagnies reflétaient la réalité de ces firmes de façon volontairement erronée. Afin de redonner confiance au système financier et insuffler une meilleure gouvernance auprès des entreprises, les États-Unis ont voté et mis en place la loi Sarbanes-Oxley qui régit les contrôles des entreprises et favorise leur « bonne gouvernance ». Les petits investisseurs ont de plus en plus droit au chapitre en demandant des comptes auprès du Conseil d'administration de leur entreprise et en n'hésitant pas à intenter des recours collectifs tant au Canada qu'aux États-Unis contre les administrateurs des compagnies qui ont floué les investisseurs.

Du côté des gouvernements, il est aussi apparu un intérêt croissant de la gouvernance, d'autant plus que la population fait moins confiance au gouvernement et remet en cause sa légitimité même. Avec le concept de gouvernement en ligne où les gouvernements se sont rapprochés des citoyens par leur prestation de services, il est devenu encore plus important de faire montre de « bonne gouvernance » et, d'une certaine façon, de redonner le pouvoir aux élus et aux citoyens et ainsi de tenter de se réapproprier la confiance des « gouvernés ».

Du côté de grands dossiers internationaux comme celui de l'environnement et du développement durable[2], le concept de gouvernance s'est aussi appliqué où des partenaires gouvernementaux, privés et de la société civile sont appelés à jouer un rôle actif dans la définition et la mise en place de solutions pour le bien-être collectif tant local, que national et international. Bien sûr, la gouvernance est aussi appliquée à Internet et les Nations-Unies ont même convenu de mettre en place un forum sur le sujet (Forum sur la gouvernance d'Internet – FGI[3]).

Comme le souligne l'Institut de la gouvernance[4], le besoin de gouvernance repose sur les trois constats suivants :

- Fin du monopole des gouvernements : « les autorités politiques n'ont plus le monopole de la responsabilité. La gouvernance est une forme de réponse possible pour réconcilier le politique, l'économique et le social en proposant de nouvelles formes de régulation. »;
- Multiplicité des acteurs : « des acteurs de toute nature réclament d'être associés au processus de décision et sont en mesure de proposer de nouvelles solutions aux problèmes collectifs. La gouvernance met l'accent sur le déplacement des responsabilités qui s'opère entre l'État, la société civile et le marché. »;
- Interdépendance des acteurs : « aucun acteur ne dispose des connaissances et des moyens nécessaires pour résoudre seuls les problèmes qui se posent. Des processus itératifs d'interaction / négociation sont devenus nécessaires entre intervenants hétérogènes. La gouvernance implique donc la participation, la négociation et la coordination. »

Avec la gouvernance, est apparu récemment le concept de « bonne gouvernance » où les Nations-Unies en énumèrent les caractéristiques suivantes[5] :

- *la participation :* donner à tous, hommes et femmes, la possibilité de participer au processus décisionnel;
- *la transparence* découlant de la libre circulation de l'information;
- *la sensibilité* des institutions et des processus vis-à-vis des intervenants;
- *un consensus :* des intérêts différents sont conciliés afin d'arriver à un vaste consensus sur ce qui constitue l'intérêt général;

---

[2] Consulter le site de l'OCDE (Organisation de la coopération et du développement économiques) à cet effet portant sur le Développement durable et la gouvernance : www.oecd.org/topic/0,2686,fr_2649_34143_1_1_1_1_37425,00.html
[3] Consulter les sites Web du FGI à www.intgovforum.org/athens_outline.htm et www.igfgreece2006.gr/?tid=55&aid=0
[4] http://i-gouvernance.com/concept/concept-centre.html
[5] p. 4 in « Comprendre la gouvernance », Institut sur la gouvernance, Ottawa, 2001

- *l'équité :* tous, hommes et femmes, ont des possibilités d'améliorer et de conserver leur bien-être;
- *l'efficacité et l'efficience :* les processus et les institutions produisent des résultats qui satisfont aux besoins tout en faisant le meilleur usage possible des ressources;
- *la responsabilité* des décideurs du gouvernement, du secteur privé et des organisations de la société civile;
- *une vision stratégique* des leaders et du public sur la bonne gouvernance et le développement humain et sur ce qui est nécessaire pour réaliser un tel développement.

Ces éléments, qui peuvent apparaître un peu éloignés de notre sujet d'étude, seront importants lorsque viendra le temps d'examiner les pistes d'action.

Deux éléments du concept de la gouvernance sont importants à souligner :

- la gouvernance s'applique autant pour la conduite des affaires des états que celle des entreprises, des organisations sans but lucratif ou des organisations internationales; elle s'applique aussi, par extenso, à des objets d'intérêt national ou international tel qu'Internet et son contenu;
- la gouvernance implique aussi la participation accrue de la société civile. Les gouvernements ou les entreprises doivent de plus en plus, du moins dans les pays dits démocratiques, gérer en tenant compte de la société civile. Des représentants de la société civile, sur une base individuelle ou organisés en association, jouent de plus en plus un rôle de contrôle et même d'orientation des décisions des gouvernements, des entreprises et des organisations internationales.

Ces deux derniers éléments, par exemple, se retrouvent bien présents dans le débat et les interventions dans le domaine environnemental et particulièrement l'application du protocole de Kyoto. Ainsi en est-il de la gouvernance du contenu d'Internet. Elle peut difficilement se faire sans tenir compte des préoccupations de la société civile, d'autant plus que la frontière restera toujours mince entre le droit à l'accès au contenu et le devoir de protéger la jeunesse de certains types de contenus et que cette frontière est extrêmement variable selon chaque société, composée, notamment, de la société civile.

Gouvernance d'Internet

La gouvernance d'Internet est définie par l'OQLF en 2002 ainsi :

> « Gestion administrative et technique d'Internet par des instances internationales qui prennent des décisions sur la base d'un consensus quant à des éléments essentiels.
> Note(s) :
> La coordination des adresses IP et [celle] des noms de domaines sont les principales tâches à effectuer par ces instances. Par exemple, l'ICANN (*Internet Corporation for Assigned Names and Numbers*) définit les règles de fonctionnement du cyberespace et l'IAB (*Internet Architecture Board*) est responsable de son développement technique. »

Cette définition a évolué depuis 2002, particulièrement à la suite des travaux du Groupe de travail sur la gouvernance d'Internet (GTGI) créé par le Secrétaire général de l'Organisation des Nations-Unies. Dans son rapport d'août 2005 (www.wgig.org/docs/WGIGReport-French.doc), le GTGI fournit une définition beaucoup plus large et explicite que voici :

> « Il faut entendre par « gouvernance de l'Internet » l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet. »

Le GTGI a ajouté les notes explicatives suivantes :

1. Cette définition pratique renforce la notion de l'intégration des États, du secteur privé et de la société civile dans les mécanismes de la gouvernance d'Internet. Elle tient compte par ailleurs du fait que pour certains aspects bien précis de la gouvernance d'Internet, les diverses parties prenantes auront des intérêts, des tâches et un degré de participation différents, et qu'il y aura parfois chevauchement.

2. Il faut bien comprendre toutefois que la gouvernance d'Internet recouvre davantage d'aspects que la gestion des noms et adresses et les questions dont s'occupe l'*Internet Corporation for Assigned Names and Numbers* (ICANN) et qu'elle englobe aussi des questions importantes de politique générale, comme les ressources critiques d'Internet, la sécurité et la sûreté du réseau mondial et tout ce qui a trait à son développement et à l'utilisation qui en est faite.

3. Il existe quatre grands domaines d'intérêt général, soit :

a) **Questions relatives à l'infrastructure et à la gestion de ressources critiques d'Internet**, notamment l'administration du système de noms de domaine et d'adresses numériques Internet (adresses IP – Internet Protocol), l'administration du système de serveurs racine, les normes techniques, l'homologation et l'interconnexion, l'infrastructure de télécommunications et le passage au multilinguisme. Ces questions concernent directement la gouvernance d'Internet et relèvent des organisations existantes qui en sont chargées;

b) **Questions relatives à l'utilisation d'Internet**, notamment le pollupostage, **la sécurité des réseaux et la cyberdélinquance**. Bien que ces questions soient directement liées à la gouvernance d'Internet, la nature de la coopération mondiale requise n'est pas bien définie;

c) **Questions qui concernent Internet mais dont les répercussions le dépassent largement, comme les droits de propriété intellectuelle ou le commerce international**, et qui relèvent de la compétence d'organisations existantes. Le GTGI a entrepris d'examiner dans quelle mesure ces questions sont abordées de manière compatible avec la Déclaration de principes intitulée « Construire la société de l'information : un défi mondial pour le nouveau millénaire » adoptée en décembre 2003 lors du Sommet mondial sur la société de l'information (voir www.itu.int/wsis/docs/geneva/official/dop-fr.htm);

d) **Questions relatives aux aspects de la gouvernance d'Internet qui ont trait au développement**, en particulier renforcement des capacités dans les pays en développement. Ce domaine correspond à tous les aspects reliés à la lutte à la fracture numérique observée particulièrement dans les pays en développement et, dans une certaine mesure, dans les zones éloignées des pays industrialisés. Il comprend, notamment, le déploiement d'infrastructure technologique adéquate pour soutenir l'utilisation répandue d'Internet, la formation nécessaire pour permettre à tous les acteurs d'une société de s'approprier des facilités [commodités] inhérentes à Internet et un soutien de l'industrie nationale.

L'*Internet Society* (ISOC) découpe la gouvernance d'Internet en neuf grands domaines (www.isoc.org/pubpolpillar/faq.shtml), à savoir :

- L'accès à Internet;
- Le système des noms de domaine (DNS – Domain Name System);
- La gestion et l'attribution des adresses IP;
- L'internationalisation des noms de domaines (IDN – Internationalized Domain Names);
- La normalisation d'Internet (particulièrement par le biais de l'IETF – Internet Engineering Taskforce);

- Les droits de propriété intellectuelle;
- La protection des données et de la vie privée;
- Le pollupostage, la sécurité et la cyberdélinquance;
- Le développement de capacité (particulièrement par les pays moins nantis), ce dernier domaine correspondant au 4e domaine du GTGI.

Gouvernance des contenus sur Internet

En examinant la définition de la gouvernance d'Internet et les domaines d'intérêt général associés, on peut constater que cette définition peut aussi correspondre à la gouvernance des contenus sur Internet. Les domaines d'intérêt général sont à peu près les mêmes, il s'agit d'y ajouter l'éclairage de la portée de l'étude, soit la protection de la jeunesse.

Nous avons donc choisi de retenir la définition proposée par le GTGI de l'ONU, avec un ajout qui concrétise la portée de l'étude et une certaine adaptation des domaines d'intérêt. La définition est donc la suivante :

> « Élaboration et application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation d'Internet *de façon à protéger la jeunesse.* »

Et les domaines d'intérêt en comptent trois, dont deux proposés par le GTGI et un autre considéré comme étant essentiel à l'étude. Ces domaines sont :

- **Questions relatives à l'infrastructure et à la gestion de ressources Internet critiques**, notamment l'administration du système de noms de domaine et d'adresses numériques Internet (adresses IP), l'administration du système de serveurs racine, les normes techniques, l'homologation et l'interconnexion, l'infrastructure de télécommunications (y compris technologies novatrices et convergentes) et le passage au multilinguisme. Ces questions concernent directement la gouvernance **d'Internet** et relèvent des organisations existantes qui en sont chargées.
  Ce domaine de préoccupation rejoint les quatre sujets d'intérêt d'ISOC en matière de gouvernance : le système des noms de domaine (DNS), la gestion et l'attribution des adresses IP (Internet Protocol), l'internationalisation des noms de domaines et la normalisation d'Internet (particulièrement par le biais de l'IETF – Internet Engineering Taskforce)
- **Questions relatives à l'utilisation d'Internet**, notamment le **pollupostage, la sécurité des réseaux et la cyberdélinquance**. Ce

domaine de préoccupation correspond au même sujet d'intérêt d'ISOC. Aux fins de l'étude, la sécurité n'y sera pas abordée directement.

- **Questions relatives à la liberté d'expression ainsi qu'à la protection des données et de la vie privée**. Ce domaine de préoccupation n'en est pas un, selon le GTGI, même si ces éléments figurent dans ses priorités d'action. La protection des données et de la vie privée fait partie des sujets d'intérêt d'ISOC. Il apparaît important de couvrir explicitement ce domaine car il va de pair, pour cette étude, avec le domaine précédent, soit celui sur l'utilisation d'Internet.

On peut le constater, même dans cette définition, on ne retrouve pas la préoccupation de contenu de façon explicite. Elle se retrouve cependant de façon implicite dans chacun des domaines d'intérêt. Ainsi, si on considère la liberté d'expression, on se réfère évidemment au contenu librement exprimé sur Internet. De même, si on considère la protection de la vie privée, on se réfère à la protection du contenu informationnel relatif à l'identité privée d'une personne, soit ses renseignements personnels.

Nous avons décidé de conserver un éventail le plus vaste possible des domaines d'intérêt. Certains de ces domaines apparaissent, de prime abord, purement techniques ou légaux et peuvent sembler éloignés de notre préoccupation de base. Cependant, très souvent, un sujet pouvant apparaître très technique comme la gestion des noms de domaine (DNS) peut comporter des éléments hautement politiques et porter, éventuellement, sur le contenu véhiculé sur Internet. Nous reprendrons ces éléments dans le prochain chapitre et examinerons comment ils peuvent aider actuellement ou pourraient aider dans un futur plus ou moins rapproché à protéger la jeunesse.

Type de contenu

Le mandat actuel de la Régie du cinéma porte sur le film, que ce soit en 35 mm (diffusé dans les salles de cinéma) ou en vidéo (VHS ou DVD).

L'objet de l'étude déborde le film et couvre tout ce qui est image, animée ou non, intégrée ou non dans un film, accompagnée ou non de sons ou de texte. Il est convenu de référer au « contenu audiovisuel ».

De plus, contrairement au film traditionnel où le contenu audiovisuel est capturé dans quelque chose de fini, de fixe, le contenu audiovisuel sur Internet peut être autant emmagasiné et fini (tel que l'accès aux DVD de films) que temporaire (tel que les images ou petites séquences de film échangées sur des environnements dynamiques lors de clavardage ou

d'échange de messages sur mobile via Internet ou de projection réalisée en direct). Le premier contenu audiovisuel, soit le contenu emmagasiné, présente une caractéristique de pérennité et est souvent destiné à une diffusion plus ou moins large alors que le dernier contenu, soit celui temporaire, représente un caractère éphémère et est généralement destiné pour un usage privé entre deux personnes. Ce dernier contenu peut, quelques fois, être emmagasiné, mais habituellement, pour un visionnement privé[6]. Ce concept de contenu audiovisuel pouvant être à la fois emmagasiné ou éphémère devient extrêmement important lorsque l'on désire effectuer une régulation du contenu afin de protéger la jeunesse, particulièrement en ce qui a trait à la téléphonie mobile où l'éphémère est davantage présent et où l'accès aux services de téléphonie mobile s'effectue généralement loin de la proximité du parent qui ne peut alors exercer de supervision de proximité.

Ces images, afin d'être reconnues par les différents médias numériques sur toute la chaîne d'Internet (production, stockage, diffusion, réception et utilisation), utilisent une pléthore de formats numériques propriétaires ou normalisés tels que Apple Quick Time, Flash, ISO/IEC 14496-15, JPEG, MPEG-4, Ogg, Real Media, etc.[7]

Médias numériques

La technologie permettant de véhiculer le film et, dans un sens large l'image, a évolué énormément et continuera de le faire.

Le film peut se retrouver sur différents supports, certains plus traditionnels, comme la bobine de film utilisée dans les salles de cinéma, et d'autres, plus récents, comme le iPod Video d'Apple ou un appareil multimédia comme le téléphone cellulaire de « troisième génération » (3G) permettant l'accès à Internet. Grâce à ces nouveaux médias numériques, l'image (seule ou incorporée dans un film) devient de plus en plus accessible sur une base personnelle et à la demande.

On inclura dans la notion de « médias numériques » tous les médias numériques qui utilisent Internet pour échanger, d'une quelconque façon, le « type de contenu » dont il a été question précédemment, afin de permettre son stockage ou son affichage.

Par contre, cette étude exclura les médias numériques n'ayant pas recours à Internet, tels que les consoles de jeux (X-Box, Nintendo, etc.). Il ne faut

---

[6] Consulter le document n° 16 du Cahier 3 *Review of regulation of content delivered over convergent devices*, particulièrement aux pages vi et 91 (www.dcita.gov.au/__data/assets/pdf_file/39890/Final_Convergent_Devices_Report.pdf)

[7] Consulter à cet effet les différents formats détaillés sur le site suivant : http://wiki.multimedia.cx/index.php?title=Category:Container_Formats

cependant pas conclure que les jeux sont exclus de l'étude car Internet fournit de grandes capacités de jeux. Il est intéressant de souligner que l'Europe s'est dotée d'un système volontaire de classification des « logiciels de loisir » désigné par le sigle PEGI (*Pan European Game Information*) (voir www.pegi.info/pegi/index.do) alors que l'Amérique du Nord suit un système similaire mais non identique désigné par le sigle ESRB (*Entertainment Software Rating Board*) (voir www.esrb.org).

Neutralité de l'architecture d'Internet

Un des principes de l'architecture d'Internet repose sur la neutralité (ou le principe du « bout en bout » ou « end-to-end ») du réseau par rapport au contenu véhiculé et aux applications ou services qui peuvent en être faits. Voici quelques explications additionnelles tirées d'un article écrit par Bernard Benhamou[8] :

« L'architecture de l'Internet correspond à la superposition de « couches » dont les fonctions sont différentes. Ces trois couches fondamentales de l'Internet sont liées d'une part au transport (infrastructures physiques), puis aux applications (couche logique) et enfin aux informations échangées (couche des contenus).

« L'une des particularités de cette architecture est liée à l'indépendance des différentes couches qui constituent le réseau. En effet, le double protocole fondamental de l'Internet « TCP/IP » assure une séparation entre les fonctions de transport et les fonctions de traitement des informations. Cette séparation est l'un des principes essentiels d'Internet : le principe du « end-to-end » (ou architecture de « bout en bout »). Selon ce principe, l'« intelligence » du réseau est située à l'extrémité des mailles et non centralisée dans le réseau lui-même, les fonctions « nobles » de traitement de l'information étant alors réservées aux ordinateurs (et aux usagers) situés aux extrémités du réseau.

Le principe de neutralité a donné à l'Internet sa souplesse en matière de développement de contenus et d'applications et lui a permis de devenir le plus important réseau de personnes et de contenus.

« … Les réseaux qui adoptent le principe du *end–to-end* sont « neutres » et se limitent à transporter des informations sans les modifier (c'est la raison pour laquelle ce principe est aussi appelé principe de « *neutralité* »).

« Le réseau constitue alors une plate-forme d'expression commune, un « bien commun » qui permet à l'ensemble des utilisateurs de développer de nouveaux contenus et de nouveaux services. C'est cette particularité de l'architecture d'Internet qui a permis à des utilisateurs « isolés » de développer des technologies qui par la suite ont été adoptées mondialement. Ce fut le cas avec le langage HTML qui a donné naissance

[8] Consulter les documents n° 18.1 (www.netgouvernance.org/E2E(f).PDF) et 18.2 (http://netgouvernance.org/ArchitectureEsprit.pdf) du Cahier 4 portant sur l'architecture d'Internet et le principe de la neutralité ou du « **bout en bout** » (end-to-end).

au Web mais aussi plus récemment avec les carnets (ou « blogue ») et les systèmes dits de « pair à pair » (ou peer-to-peer).

« Ce principe a aussi des conséquences sur le fonctionnement économique du réseau. En effet, en favorisant la compétition aux « extrémités » du réseau, il préserve l'égalité d'accès au réseau pour les nouveaux entrants tout en maintenant l'unicité des fonctions essentielles du réseau. Ce principe évite notamment que le réseau ne fasse l'objet d'une appropriation par certaines entreprises ou certains secteurs au détriment de l'ensemble de ses utilisateurs. C'est aussi ce principe qui a donné à Internet sa souplesse en matière de développement de contenus et d'applications et lui a permis de devenir en l'espace de quelques années le plus important réseau de personnes et de contenus. »

Tout traitement des contenus ne peut s'insérer qu'aux extrémités du réseau Internet

Sur la base de ce principe, toute action sur les contenus, telle que leur filtrage, peut difficilement s'insérer à l'intérieur du réseau Internet sans mettre en péril ce principe d'architecture d'Internet. Ce type d'action pourrait, comme tout autre service ou traitement d'information, s'insérer aux extrémités du réseau Internet.

Le principe de neutralité est rendu possible grâce, notamment, à la définition et au respect d'un ensemble de normes telles que TCP/IP (pour le réseau Internet) et la norme HTML (pour la description du contenu).

Web sémantique

Une évolution du Web peut être particulièrement importante pour la caractérisation et le classement des documents audiovisuels sur Internet. Il s'agit du « Web sémantique », aussi appelé « Web 2.0 ».

Le Web sémantique est une extension du Web permettant de publier, de consulter et, tout particulièrement, d'automatiser le traitement de connaissances précisément formalisées. C'est le consortium sur le Web (World Wide Web Consortium – W3C), appuyé par bien d'autres organisations à travers le monde, qui fait la promotion du Web sémantique.

De façon générale, le Web sémantique se base sur le Web « classique » et l'enrichit en ajoutant aux documents des informations formalisées permettant le traitement automatique par des logiciels par la suite. Ces logiciels permettent, notamment de :

- générer des données sémantiques à partir de la saisie d'information par les utilisateurs;
- agréger des données sémantiques afin d'être publiées ou traitées;
- publier des données sémantiques avec une mise en forme personnalisée ou spécialisée;

- échanger automatiquement des données en fonction de leurs relations sémantiques;
- générer des données sémantiques automatiquement, sans saisie humaine, à partir de règles d'inférence.

Techniquement, le Web sémantique se base sur les protocoles et normes du Web « classique » tels que le protocole de communication client-serveur HTTP[9] (Hypertext Transfer Protocol*)* et l'identifiant uniforme de ressource URI[10] (Uniform Resource Identifiers) et le langage XML (EXtensible Mark-up Language). Le Web sémantique ajoute au « Web classique » des protocoles et normes spécifiques tels qu'un modèle conceptuel de description de métadonnées ou d'étiquettes RDF (Resource Description Framework) et des langages de RDF Schema et OWL (Web Ontology Language) (deux langages permettant de créer des vocabulaires plus ou moins complexes et de décrire des objets) ainsi que SPARQL[11] (langage de requêtes permettant d'obtenir des informations à partir des informations codées selon RDF). Ces nouvelles normes de protocoles et de langages permettent le développement de nouvelles applications qui rendent concrète la notion d'intelligence collective[12].

Avec le Web sémantique, tout objet du Web peut se voir attribuer une étiquette (ou « métadonnée ») qui représente fidèlement cet objet. Cette étiquette peut être lue par des logiciels et par des êtres humains. Par objet, il faut entendre une grande variété d'informations telles qu'un média (image, son, vidéo), une page Web, un ensemble de pages, des données plus ou moins structurées, un lien, un site, un service, etc.[13]

Beaucoup d'espoir est fondé dans le format RDF[14] car il peut servir pour plusieurs applications, notamment pour la codification ou la catégorisation

---

[9] Il est utilisé pour échanger toutes sortes de données entre client HTTP et serveur HTTP. Consulter Wikipédia : http://fr.wikipedia.org/wiki/Http

[10] URI est une courte chaîne de caractères identifiant une ressource physique ou abstraite, et dont la syntaxe respecte la norme produite par IETF RFC 3986. Consulter à cet effet Wikipedia : http://fr.wikipedia.org/wiki/Uniform_Resource_Identifier

[11] Pour une description détaillée de la proposition de norme SPARQL, consulter www.w3.org/TR/rdf-sparql-query

[12] Consulter à cet effet les trois sites Web de W3C, soit celui de niveau international (www.w3c.org), celui du Canada (www.cscsi.org/home/CSCSI/Members/swig) et celui du Québec (www.w3qc.org) W3C Québec qui a comme mission de **promouvoir les normes, standards ouverts et bonnes pratiques du Web et du multimédia au Québec.**

[13] Consulter le document n° 4.2 du Cahier 4 *Principes fondamentaux du Web sémantique* (http://websemantique.org/PrincipesFondamentauxDuWebSemantique)

[14] La norme RDF inclut la norme antérieure PICS (Platform for Internet Content Selection) qui est utilisée par plusieurs logiciels de filtrage (consulter les documents n° 15 (www.w3.org/**PICS)** et 16 (www.w3.org/2000/03/PICS-FAQ) du Cahier 5).

des contenus[15]. Ainsi, l'Association de classification du contenu d'Internet (l'ICRA - Internet Content Rating Association) utilise la norme RDF pour permettre de catégoriser[16] (ou d'étiqueter) le contenu des sites Web.

Un autre exemple du Web sémantique est la norme destinée à exprimer les pratiques de protection de la vie privée d'un site Web, soit la P3P (Platform for Privacy Preferences Project). Cette norme permet aux sites Web d'exprimer leurs pratiques dans un format normalisé qui peut être récupéré automatiquement et interprété facilement par des logiciels par la suite. Ceci permet aux utilisateurs d'être informés des pratiques du site Web et éventuellement d'automatiser la prise de décision selon ses préférences[17]. Enfin, d'autres exemples comprennent les annuaires de fil de nouvelles RSS (Really Simple Syndication – Souscription vraiment simple) et les blogues.

Codification et classement des contenus audiovisuels numériques

Il existe un classement assez formel du film. Mais, pour ce qui est des images qui transitent par Internet, à moins que ces images correspondent à des films déjà classés par un organisme de classement comme la Régie du cinéma du Québec, il n'y a pas de mécanisme formel et partagé de codification et de classement. Les définitions qui suivent se basent sur les pratiques actuelles des organismes de classement de films et sur celles en cours sur Internet.

Classement

La classification est le processus de classement des films par catégories d'âge, tout en pouvant lui adjoindre des informations additionnelles précisant le type de contenu. Les classements attribués aux films peuvent varier d'un pays à l'autre ou, comme c'est le cas au Canada, d'une province à l'autre et s'effectuent selon une grille d'analyse propre à chaque société. Un même film peut donc se voir attribuer, par le biais des différents bureaux de classement à travers le monde, des classements dans des catégories différentes.

Au Québec, c'est la Régie du cinéma du Québec qui classe les films dans une des quatre catégories d'âge et, au besoin, ajoute au classement des

[15] Pour plus de détails sur la norme RDF, consulter le document n° 4.3 du Cahier 4 (www.w3.org/RDF/FAQ)

[16] Il faut faire attention au vocabulaire utilisé par la description française de l'ICRA qui indique qu'elle permet de classifier les sites Web, alors qu'en fait elle permet de les catégoriser plutôt. La classification serait plutôt laissée aux logiciels qui exploitent les étiquettes pour les transformer en classes de visionnement selon l'âge, par exemple.

[17] Pour plus de détails sur la norme P3P, consulter www.w3.org/P3P

indications supplémentaires. Les catégories de classement retenues par la Régie du cinéma du Québec sont (voir www.rcq.qc.ca/processus.asp) :

- Visa général – public de tout âge;
- 13 ans et plus;
- 16 ans et plus;
- 18 ans et plus.

Les indications supplémentaires suivantes permettent de préciser la caractéristique dominante du film :

- Pour enfants;
- Déconseillé aux jeunes enfants;
- Langage vulgaire;
- Érotisme;
- Violence;
- Horreur;
- Sexualité explicite.

Codification

La codification, dans le contexte de classement des films, est le système de symboles qui sert à identifier le film. Chaque organisme de classement des films (et vidéos) utilise sa propre codification. La codification utilisée par la Régie du cinéma du Québec comprend les symboles suivants : « G », en vert; « 13 ans + », en jaune; « 16 ans + » en bleu, et « 18 ans + » en rouge.

Dans le monde d'Internet, la codification diffère sensiblement de celle utilisée par les organismes de classement de films et n'est pas axée strictement sur l'âge mais plutôt sur le type de contenu véhiculé, sans égard direct sur la recommandation de classe d'âge des spectateurs. En général, la codification utilisée ne permet pas d'associer le groupe d'âge approprié au contenu. Cependant, il arrive qu'un système de codification basé sur une taxonomie binaire de classes d'âge soit utilisé pour distinguer le contenu adulte ou non (18 ans et plus ou moins de 18 ans). C'est ainsi le cas dans

certains pays pour la codification du contenu sur Internet auquel on accède avec les mobiles[18].

À titre d'illustration de codification sur Internet, l'*Internet Content Rating Association* (ICRA) (www.icra.org/label/generator) propose aux propriétaires de sites Web, sur une base volontaire, une codification de leur site Web (applicable à tout le site Web ou à chacune des pages), selon les catégories suivantes :

- Nudité;
- Contenu à caractère sexuel;
- Violence;
- Langage;
- Activités potentiellement dangereuses;
- Contenu généré par l'utilisateur (tel qu'un forum de discussions);
- Contexte (à vocation artistique, éducative ou médicale par exemple).

Chacune de ces catégories est accompagnée de détails assez élaborés. Voici par exemple les indications qui peuvent accompagner la catégorie « violence » :

- Agression/viol;
- Êtres humains blessés;
- Animaux blessés;
- Personnages imaginaires blessés (dont personnages d'animation);
- Sang et démembrement, êtres humains;
- Sang et démembrement, animaux;
- Torture ou mise à mort d'êtres humains;
- Torture ou mise à mort d'animaux;
- Torture ou mise à mort de personnages imaginaires (dont personnages d'animation);
- Aucun des éléments ci-dessus.

Cette taxonomie de l'ICRA ne permet pas de déduire automatiquement la classe d'âge. C'est probablement une des raisons pour lesquelles le fureteur le plus utilisé, soit Internet Explorer, ne supporte pas la taxonomie actuelle

[18] Le terme « mobile » englobe tout appareil permettant d'accéder Internet sans fil tel que les téléphones cellulaires dits de « 3e génération » ou les « terminaux mobiles de poche » tels que le Blackberry.

de l'ICRA car elle est difficilement automatisable par classe d'âge. Ce fureteur continue à supporter la taxonomie antérieure à l'ICRA, correspondant à la version de 1999 développée par l'organisme *Recreational Software Advisory Council* (RSACi), organisme qui a été intégré à l'ICRA. Voici sa taxonomie où les niveaux peuvent correspondre plus facilement à des classes d'âge :

Niveau	Violence	Nudité	Sexe	Langue
0	Aucune violence	Aucun	Aucun	Argot inoffensif
1	Combats	Tenue révélatrice	Baisers passionnés	Jurons très modérés
2	Tueries	Nudité partielle	Attouchements sexuels sans nudité	Jurons modérés
3	Tueries sanglantes et détails choquants	Nudité de face	Attouchements sexuels non explicites	Gestes obscènes
4	Violence gratuite et cruelle	Nudité de face provocatrice	Activité sexuelle explicite	Langage grossier ou explicite

Source : www.securite.teamlog.com/publication/8/17/181/index.html

Il existe plusieurs autres taxonomies proposées par des producteurs de logiciel de filtrage dont certaines seront examinées au chapitre sur la codification et les filtres. La très large majorité d'entre elles ont recours à une taxonomie basée sur le type de contenu, sans davantage de précision sur l'âge. Dans ce contexte, chaque utilisateur doit remplir le rôle équivalent à un organisme de classement, soit apparier le contenu audiovisuel à une classe d'âge, sur la base d'informations fournies par la taxonomie du logiciel utilisé.

Filtrage des contenus audiovisuels numériques codifiés

Au Canada, le filtrage du contenu qui transite par Internet est laissé à la discrétion de l'industrie. Le Conseil de la radio et de la télévision du Canada (CRTC) se fie à l'autorégulation de cette dernière et au comportement responsable des utilisateurs.

Avec la convergence des médias numériques permettant de diffuser des images et des films par Internet, on se retrouve avec des systèmes de classement de films et des systèmes de filtrage des contenus sur Internet fort différents.

Le filtrage des contenus permet de restreindre l'accès à un site Web ou à une page d'un site Web, selon les critères spécifiques de l'utilisateur, d'une organisation, d'un État, etc. Cette restriction peut prendre différentes formes comme un blocage total ou un avertissement indiquant que le site Web contrevient aux critères d'accès restreint définis par l'utilisateur ou par son organisation.

Le filtrage s'inspire généralement du modèle développé par Resnick en 1998 en six étapes[19] que voici, après y avoir inséré des explications additionnelles :

1. Déterminer le vocabulaire d'étiquetage et les critères d'assignation des étiquettes (soit la taxonomie);
2. Attribuer les étiquettes (= coter ou classifier);
3. Distribuer les étiquettes (= insérer les étiquettes dans le contenu ou distribuer l'information sur la taxonomie utilisée);
4. Écrire le logiciel de filtrage (ou adapter le logiciel d'accès au contenu);
5. Déterminer les critères de filtrage à activer (= personnaliser);
6. Mettre en place et exécuter le logiciel de filtrage (ou tout autre logiciel ayant des fonctionnalités de filtrage).

Le vocabulaire d'étiquetage, ou taxonomie, tel que mentionné précédemment, n'est pas uniformisé dans le monde d'Internet et varie selon les fournisseurs de logiciels de filtrage. On retrouve ainsi un nombre très variable de catégories par taxonomies et une signification variable pour une même catégorie d'une taxonomie à une autre.

Le filtrage peut recourir à différentes stratégies, bien souvent mixtes, dont voici quelques exemples (voir http://internet-filter-review.toptenreviews.com/internet-filter-review-definitions.html) :

- **Filtrage par analyse d'objet** : filtre un site Web selon l'analyse d'objets spécifiques présents dans un site Web. Certains objets sont considérés comme typiques des sites Web pornographiques et reconnaissables par un logiciel de filtrage. Ainsi, plusieurs sites pornographiques utilisent des compteurs très particuliers de fréquentation de visiteurs que l'on ne

[19] Consulter la page Web www.unesco.org/webworld/infoethics_2/eng/papers/paper_24.htm

retrouve que sur de tels sites et qui sont reconnaissables par logiciel. Il est alors possible d'associer un tel site contenant ces objets à un site pornographique et d'en effectuer le filtrage.

- **Filtrage par nom de site Web** : filtre un site Web selon son nom (ou son URL), auquel on a attribué une ou plusieurs catégories convenues d'avance (violence, haine, sexe, drogue, etc.), qui désignent un accès restreint. Le classement du site Web, selon les différentes catégories décidées par le fournisseur du logiciel ou un organisme de l'industrie, s'effectue préalablement et est stocké dans une base de données. L'application de ce filtre s'effectue lors de la demande d'accès à ces sites Web selon la politique de filtrage de l'organisation ou de l'individu (par exemple; une famille pourrait décider de barrer l'accès de leur ordinateur aux sites Web faisant partie des catégories « violence » ou « sexe »). Avec cette stratégie, chaque site Web se voit attribuer une catégorie. Bien qu'il soit possible de réviser le classement du site Web, ce classement est généralement assez statique.

- **Filtrage par mots clés** : filtre basé sur des mots clés contenus dans un site Web.

- **Filtrage par catégorisation dynamique** : filtre un site Web ou une page d'un site Web selon son contenu à l'instant même où l'utilisateur désire y accéder. Ce filtrage dynamique permet des accès variables au contenu. Ainsi, il pourrait être possible d'accéder à un site de nouvelles le matin, mais de ne pas pouvoir le faire en après-midi si le site comporte une nouvelle décrivant un événement violent. De même, il pourrait être possible d'accéder à la presque totalité d'un site sauf à certaines pages tombant sous le coup de catégories à accès restreint. Ce type de filtrage s'effectue généralement page par page d'un site Web et non pas nécessairement pour tout le site Web. Puisque le filtrage s'effectue dynamiquement, page par page, on ne stocke généralement pas le classement obtenu.

  Généralement, ce filtre a recours à des techniques de reconnaissance automatique de contenu (Active Content Recognition -ACR™) lors de la demande d'accès à du contenu sur Internet et ce, selon la politique de filtrage de l'organisation ou de l'individu. (Voir à titre d'exemples les logiciels 602LAN SUITE *Content Filter*, *Pure Sight* et *ScanSafe* ainsi que leurs sites Web respectifs : http://software602.com/products/ls/internetfilter.html, www.puresight.com/products/ps-content.shtml et www.scansafe.net/scansafe/html/services_wf.html).

  Étant donné la reconnaissance automatique de contenu appliquée à cette

stratégie de filtrage, il devient primordial que les règles de filtrage utilisées tiennent compte de la langue du contenu filtré et qu'elles supportent un ensemble de langues nationales suffisantes y incluant la ou les langues de l'utilisation (telles que, pour le Québec, le français, l'anglais et au moins une autre langue nationale – espagnol, arabe, vietnamien, « chinois », etc.).

- **Filtrage par reconnaissance d'image** : filtre des images graphiques inappropriées sur un site Web. Il est à noter que les logiciels de filtrage les plus populaires pour le consommateur (voir http://internet-filter-review.toptenreviews.com/index.html#anchor) ne comportent pas cette capacité.

Société civile, gouvernements et secteur privé

Dans la description des parties prenantes pour la gouvernance d'Internet, on fait appel au triumvirat « société civile, gouvernements et secteur privé » pour les représenter. Le concept de secteur privé et de gouvernement est assez facilement compris par tous, alors que celui de « société civile » peut demander quelques explications.

L'OQLF définit la « société civile » ainsi :

> « Ensemble des mouvements et associations à but non lucratif, indépendants de l'État, dont le but est de transformer, par des efforts concertés, les politiques, les normes ou les structures sociales, à l'échelon national ou international … Par exemple, les associations de quartier, les syndicats, les organisations non gouvernementales, les [représentants des] médias et les groupements religieux font partie de la société civile. »

Dans le contexte de la gouvernance d'Internet et de ses contenus, il conviendrait d'ajouter à cette définition, le citoyen comme faisant partie de la société civile. Ainsi, l'enfant, l'adolescent, le parent et l'éducateur font partie de la société civile, tout en étant conscient que l'éducateur est à la fois citoyen et aussi membre d'une organisation gouvernementale la très grande majorité du temps.

Il demeure une certaine zone grise en ce qui a trait au positionnement des coopératives et des gouvernements locaux comme les municipalités. Certains mouvements coopératifs sont associés à la société civile alors que d'autres le sont au secteur privé. De même, les municipalités ou autres organisations gouvernementales locales sont associées à la société civile plutôt qu'aux gouvernements. Sur le pôle opposé, les institutions gouvernementales internationales comme l'Organisation de Coopération et

de Développement Économiques (OCDE) et l'Organisation des Nations-Unies (ONU) sont associées aux gouvernements.

Alphanétisation

Dans le contexte de la protection de la jeunesse, l'alphanétisation correspond à la maîtrise des habiletés relatives à l'utilisation d'Internet autant par les jeunes que par ceux et celles qui peuvent les guider, tels que les parents et les éducateurs. L'alphanétisation correspond à la traduction du concept de « Internet literacy » proposé par l'OQLF, qu'il définit ainsi :

> « Alphabétisation relative à l'enseignement et à la promotion de l'utilisation d'Internet et des NTIC [Nouvelles Technologies de l'Information et des Communications] dans différents domaines d'activité, afin de démocratiser l'accès à l'information et à la connaissance… La compréhension du fonctionnement du réseau Internet et son utilisation productive sont associées à ce concept.
> L'alphanétisation a notamment pour effet de réduire le fossé [ou fracture] numérique entre les inforiches et les infopauvres…
> Le mot *Net*, présent dans *alphaNÉTisation*, renvoie à *Internet*. »

L'alphanétisation, nous verrons dans le rapport, occupe une place importante dans la stratégie de protection de la jeunesse sur Internet. Dans cette étude, l'alphanétisation inclura la maîtrise, par les jeunes et ceux qui les éduquent, des risques reliés à l'utilisation d'Internet.

Sécurité et sûreté d'Internet

Sous l'optique de la protection de la jeunesse, deux termes pourraient être employés pour caractériser l'utilisation d'Internet par la jeunesse : sécurité et sûreté.

Le terme « sécurité » d'Internet réfère aux cinq caractéristiques de sécurité DICAI – Disponibilité et accessibilité, Intégrité et intégralité, Confidentialité, Authentification et Irrévocabilité. Ce sont très souvent des caractéristiques associées à des aspects techniques d'un système, même si certains aspects sociaux sont aussi en jeu. Le concept de « sûreté » présente un aspect plus global d'un système, que *Le Petit Robert* définit comme « à l'abri du danger ».

Si on essaie de transposer ces deux termes dans le contexte de la protection de la jeunesse, on pourrait donner comme exemples de « sécurité d'Internet » le fait de ne pas se faire voler ses renseignements personnels d'identité ou de pouvoir accéder aux informations sur Internet selon les critères de disponibilité convenus. Comme exemples de « sûreté »

d'Internet, on pourrait prendre le fait de ne pas accéder à des informations qui pourraient être nuisibles à un jeune ou le fait, pour un jeune, de ne pas faire l'objet d'intimidation (bullying) ou de menaces lors de l'utilisation d'Internet. C'est pourquoi, en Europe, le terme « sûreté d'Internet » ou « Internet plus sûr » (« safer Internet ») est préférablement utilisé. Dans cette étude, le terme « sûreté d'Internet » sera retenu pour désigner la « possibilité pour les jeunes d'utiliser Internet à l'abri du danger ». À la limite, ce concept veut aussi dire que si le jeune rencontre un danger, il aura été formé pour y faire face et y répondre adéquatement pour qu'il demeure, en bout de piste, à l'abri du danger. On le devine, la « sûreté d'Internet » est très reliée à l'alphanétisation.

3. Revue de littérature

Une revue exhaustive de littérature sur la gouvernance d'Internet et de ses contenus ainsi que sur les filtres, a été réalisée. Il en a résulté cinq cahiers d'environ trois cents (300) publications, documents ou pages Web dont trois portant sur la gouvernance, un sur les filtres et un autre à la fois sur la gouvernance et les filtres. De plus, pour certains documents plus importants ou volumineux, une synthèse a été produite. C'est à partir de ce corpus de connaissances, qu'ont été rédigés les chapitres suivants.

Afin de consigner la revue de littérature et de permettre la communication entre l'équipe de projet, le format suivant a été retenu :

Cahier	N°	Date	Titre	Auteur	Référence	Mots-clés

	Résumé :

Vous retrouverez à l'annexe 3 « Détail de la revue de littérature » une description des cinq cahiers ainsi que la synthèse de certains documents.

De plus, une copie électronique de la revue de littérature a été constituée et échangée entre les membres du projet. En raison de respect des droits d'auteur pouvant être rattachés à certains des documents référencés, ce corpus électronique restera accessible uniquement à l'intérieur de l'équipe de projet. Cependant, afin de faciliter l'accès à ces documents pour tout lecteur, l'adresse Web de ces documents se retrouve en référence, tout en sachant que l'évolution de chacun des sites Web référencés fait en sorte qu'il est possible que certains documents ne soient plus disponibles à l'adresse fournie où moment où le lecteur voudra y accéder.

Avant d'aborder de front la gouvernance des contenus sur Internet pour la protection de la jeunesse, il convient de situer comment la gouvernance d'Internet se présente actuellement. Ce survol de la gouvernance d'Internet facilitera la compréhension ultérieure de la gouvernance du contenu audiovisuel sur Internet par pays ainsi que le filtrage de ce contenu.

4. Introduction à la gouvernance d'Internet

L'évolution d'Internet et du Web ont permis de créer un vaste réseau mondial de communication et de connaissances accessibles à tous les peuples de la Terre, sans aucune discrimination, du moins du point de vue technique. Comme la plupart des innovations telles que le téléphone et la radio, Internet est passé d'un projet de recherche vers une commodité dans la plupart des pays occidentaux et ses applications sont devenues quelque chose de familier dans le paysage quotidien. Avec la convergence des médias numériques, Internet et ses applications se retrouvent partout et servent autant aux gouvernements qu'au secteur privé et à la société civile et ses innombrables organisations sans but lucratif, et ce, dans toutes les sphères de l'activité humaine. Internet rend possible ce qu'il est convenu d'appeler la « société de l'information » ou la société des connaissances[20]. Il y a maintenant des centaines de millions d'utilisateurs d'Internet dans le monde et environ un milliard de sites Web[21] offrant services et informations sur tout sujet concevable par l'être humain.

4.1 Société de l'information ou société de la communication? Société du savoir!

Si l'on désire protéger la jeunesse des périls d'Internet, il importe de comprendre comment il peut façonner négativement et positivement l'esprit et le comportement des jeunes.

Le concept de la « société de l'information » peut quelque peu embrouiller les pistes. Il est important de souligner que l'information sous-tend un concept de neutralité, quelle que soit la société qui conçoit l'information ou la reçoit. Or, il n'en est rien. L'information n'est pas neutre. Avec Internet et le Web, il faut tenir compte de la communication qui en est faite de cette information dans chacune des sociétés et cultures. Il faut donc tenir compte de l'émetteur et du récepteur et de ses différences cognitives et culturelles.

Pour bien appréhender le sujet de l'étude, il convient de se référer davantage à la société du savoir, qui prend en compte à la fois l'information véhiculée et les parties prenantes à la communication de cette information pour la transformer en savoir agissant. Cette précision apparaît importante

[20] Il y a un débat à savoir si on doit faire référence à Internet à la « société de l'information » ou à l a « société des communications ». Consulter à cet effet, le document n° 5 du Cahier 1 *Compte rendu de l'audition publique du 8 décembre 2005 sur la gouvernance mondiale de l'Internet* (pp. 38-42) (www.assemblee-nationale.fr/12/rap-off/i2891.asp) ainsi que les documents n° 17 du Cahier 2 *A Global Alliance for ICT* (pp. 6-7) (http://internetgovernance.org/pdf/igp-ga.pdf) et n° 39 du Cahier 4 *Protection de l'enfant et usages de l'Internet* (p. 24) (www.sante.gouv.fr/htm/actu/conf_famille2005/rapport_protection.pdf)

[21] Consulter le document n° 1 du Cahier 5 *Internet Filters – A Public Policy Report* (p.1) (www.fepproject.org/policyreports/filters2.pdf)

car si on désire protéger la jeunesse des périls d'Internet, ce n'est pas tellement l'information véhiculée (qui, théoriquement, est neutre) mais plutôt ce que ceux qui créent ces informations veulent que les jeunes en fassent et ce que les jeunes peuvent effectivement faire avec cette information et comment ces connaissances peuvent influencer négativement leurs schèmes de pensées et leurs actions, en fait, leurs connaissances. D'ailleurs, une étude récente réalisée en Europe et au Québec auprès des jeunes illustre bien ce propos : pour les jeunes, Internet est avant tout un outil de communication[22]. C'est pourquoi il est beaucoup plus approprié, à juste titre tel que mentionné lors d'un débat tenu à l'Assemblée nationale française[23], de se référer à la société du savoir ou des connaissances plutôt que de l'information. Étant donné l'omniprésence du terme « société de l'information » dans la littérature et les grandes réunions internationales et l'intérêt à simplifier le vocabulaire, le terme « société de l'information » sera retenu dans le présent document mais il est important pour le lecteur de garder à l'esprit le concept de « société du savoir ».

Internet :

Avant tout un outil de communication pour les jeunes

L'évolution rapide d'Internet, le caractère stratégique acquis grâce aux utilisations qui en sont faites et sa prévalence dans tous les pays ont soulevé plusieurs interrogations sur la gouvernance d'Internet et, de façon plus large, sur la société de l'information. Il est normal qu'un outil de communication, de partage de connaissances et de prestations de services qui a pris une telle importance dans l'économie et la société soulève des questionnements sur sa gouvernance – chacune des parties prenantes désirant y contribuer et y voir ses intérêts et préoccupations bien représentés. Aussi, depuis le début de l'an 2000, l'ONU a organisé deux sommets mondiaux sur la société de l'information (SMSI)[24] dont deux des objectifs étaient de faire en sorte que tous les pays du monde participent à la gouvernance d'Internet et de rendre possible la construction de cette société de l'information. Près de 30 000 personnes en provenance de 175 pays, ont participé à ces deux sommets.

---

[22] Consulter les document n° 48.1 et 48.1f du Cahier 4 *The Appropriation of New Media by Youth* (www.clemi.org/international/mediappro/Mediappro_b.pdf) (p. 6) et (www.mediappro.org/publications/finalreport.pdf)

[23] Référence sur la société des communications de l'Assemblée nationale

[24] Mandatée par le Conseil économique et social des Nations-Unies, l'Union internationale des télécommunications (UIT) a organisé deux SMSI en 2003 (Genève) et 2005 (Tunis). Consulter le site Web des SMSI pour plus de détails : www.itu.int/wsis/index-fr.html

4.2 Principes de gouvernance

Un des principaux documents du SMSI constitue la « Déclaration de principes – Construire la société de l'information : un défi mondial pour le nouveau millénaire »[25]. Si on se réfère à la définition de la « Gouvernance d'Internet », un des premiers jalons de cette définition a trait justement aux principes qui influenceront toutes les actions subséquentes pour créer une telle société de l'information et assurer une « bonne gouvernance » d'Internet.

Cette déclaration de principes comportant 67 énoncés est divisée en trois sections, une première (les 18 premiers principes) a trait à la « conception commune de la société de l'information », une deuxième a trait aux principes fondamentaux de la société de l'information (principes 19 à 64) qui sont regroupés sous onze thèmes, et une troisième a trait à l'expression de la volonté de concrétiser le partage des savoirs par un plan d'action (principes 65 à 67). En prenant en compte le sujet à l'étude, les principes les plus pertinents ont été regroupés en dix thèmes susceptibles d'influencer non seulement la « gouvernance d'Internet » mais particulièrement la « gouvernance du contenu sur Internet ». Ces thèmes serviront d'orientation de tout moyen d'action pouvant être envisagé pour la protection de l'enfance. Ces thèmes sont :

- Droit à la liberté d'opinion et d'expression (principes 4 et 55) :
  En conformité avec « l'article 19 de la Déclaration universelle des droits de l'homme, tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontière, les informations et les idées par quelque moyen d'expression que ce soit. »
  « Nous réaffirmons notre adhésion aux principes de la liberté de la presse et de la liberté de l'information, ainsi qu'à ceux de l'indépendance, du pluralisme et de la diversité des médias, qui sont essentiels à la société de l'information. »;
- Reconnaissance et respect des droits et libertés d'autrui (principe 5) :
  En conformité avec l'article 29 de la Déclaration universelle des droits de l'homme, tout « individu a des devoirs envers la communauté … et que, dans l'exercice de ses droits et dans la jouissance de ses libertés, chacun n'est soumis qu'aux limitations établies par la loi exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique. »;

[25] Consulter www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-F.doc

- Égalité souveraine de tous les États (principe 6);
- Protection des enfants et de la famille (principes 11, 57 et 59) :
  « Nous sommes également résolus à créer des conditions propices au développement d'applications et de services TIC tenant compte des droits des enfants ainsi que de leur protection et de leur bien-être. »
  « La famille devrait bénéficier de la protection la plus large possible. »
  « Tous les acteurs de la société de l'information devraient prendre les mesures appropriées … pour empêcher les utilisations abusives des TIC, par exemple … toutes les formes de maltraitance des enfants, en particulier ... la pornographie infantile. »;
- Prise en compte de minorités dont les peuples autochtones (principe 15);
- Participation de toutes les parties prenantes à la société de l'information (principes 20, 48 et 49) :
  « La gestion internationale de l'Internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales. »
  « La gestion de l'Internet recouvre aussi bien des questions techniques que des questions de politique publique et devrait associer toutes les parties prenantes et les organisations intergouvernementales ou internationales concernées. »;
- Établissement, rétablissement ou renforcement du climat de confiance et de sécurité dans l'utilisation des technologies de l'information et des communications (TIC) (principes 35 à 37), particulièrement en matière d'authentification, de protection de la vie privée et du consommateur, de cybersécurité, de cybercriminalité et de pollupostage;
- Importance de la normalisation internationale (principe 44) et de la contribution des organisations internationales (principe 49, e) afin « de créer des conditions permettant au consommateur d'avoir accès aux services, partout dans le monde, et quelle que soit la technologie utilisée. »;
- Respect de la diversité culturelle et linguistique (principe 52) :
  « La société de l'information devrait être fondée sur le respect de l'identité culturelle, de la diversité culturelle et linguistique, des traditions et des religions. » Ce principe s'appuie d'ailleurs sur la Déclaration universelle de l'UNESCO sur la diversité culturelle votée en 2001 et qui a par la suite été appuyée en octobre 2005 par la *Convention sur la protection et la promotion de la diversité des expressions culturelles*[26];

[26] Consulter le document n° 5 du Cahier 1 *La gouvernance mondiale d'Internet* (pp. 38-42) et les propos de M. Dominique WOLTON, Directeur de recherche au CNRS. Consulter aussi la *Déclaration universelle de l'Unesco sur la diversité culturelle* adoptée en 2001 – document n° 6 du Cahier 4 (http://unesdoc.unesco.org/images/0012/001271/127160m.pdf) et la *Convention sur la protection et la promotion de la diversité des expressions culturelles* adoptée, de justesse, en

- Utilisations éthiques des TIC (principes 56 à 59)
  « L'utilisation des TIC et la création de contenus [devraient] respecter les droits de l'homme et les libertés fondamentales d'autrui, notamment la vie privée ainsi que la liberté d'opinion, de conscience et de religion, conformément aux instruments internationaux pertinents. »
  « Tous les acteurs de la société de l'information devraient prendre les mesures appropriées … pour empêcher les utilisations abusives des TIC, par exemple les actes délictueux dictés par le racisme, la discrimination raciale et la xénophobie, ainsi que l'intolérance, la haine et la violence qui en résultent, de même que toutes les formes de maltraitance des enfants, en particulier la pédophilie et la pornographie infantile, ainsi que la traite et l'exploitation d'êtres humains. »

2005 (document n° 7 du Cahier 4
http://unesdoc.unesco.org/images/0014/001429/142919f.pdf)

4.3 Typologie de gouvernance d'Internet (GI)

Il convient de rappeler que c'est le gouvernement des États-Unis d'Amérique qui a financé le développement d'Internet[27]. La gouvernance d'Internet (GI) est donc caractérisée historiquement par l'hégémonie américaine. Les deux derniers SMSI ont été très souvent l'occasion, pour tous les autres pays, de décrier cette situation. Bien que certains éléments ont été nettement exagérés, d'autres étaient et sont encore bien réels et dénotent un malaise. Le présent document ne vise pas à ajouter d'autres arguments à cette discussion. Cependant, l'explication de la gouvernance d'Internet ne permet pas d'éviter de faire référence, au besoin, au rôle du gouvernement américain, pour bien comprendre la situation actuelle qui demeure en mouvance.

La sensibilisation mondiale à la gouvernance d'Internet, particulièrement lors des deux derniers SMSI, a été l'occasion pour plusieurs chercheurs et organismes de pression de proposer une solide réflexion sur la structure de gouvernance en général et de la gouvernance d'Internet en particulier. Ce fut, dans un sens, une occasion de faire avancer les concepts de la gouvernance. Certains de ceux-ci se retrouvent d'ailleurs dans la définition de la « gouvernance d'Internet » retenue en 2005 et dans les principes retenus en 2003 sur la construction de la société de l'information et, partant, de la gouvernance d'Internet et de son contenu. Certains éléments de cette réflexion seront utilisés dans les chapitres subséquents, notamment sur la « gouvernance des contenus » et sur les « pistes de solution » abordées en « Conclusion ».

Un des éléments de la gouvernance qu'il convient d'expliquer tout de suite est le type de régulation pouvant être mis à contribution dans la gouvernance, soit l'autorégulation, la corégulation ou la régulation.

L'autorégulation (self-regulation) est une régulation où le secteur privé (avec ou sans la collaboration de la société civile et des utilisateurs d'Internet) définit volontairement des règles d'engagement sans intervention étatique. Ce sont, par exemple, les codes d'éthique, les normes et les conventions de numérotage. L'association de classification du contenu sur Internet (ICRA – Internet Content Rating Association) est un très bon exemple d'organisation faisant appel à l'autorégulation des producteurs de contenus.

---

[27] Consulter à cet effet la figure de la page 16 décrivant l'évolution d'Internet (Figure 8. Simplified chronology of Internet technical coordination structures), dans le document produit par l'OCDE en 2005 - document n° 24 du Cahier 2 *OECD Input to the United Nations Working Group on Internet Governance (WGIG)* (www.oecd.org/dataoecd/1/46/36779934.pdf)

La **corégulation** est une régulation où une organisation gouvernementale délègue des tâches au secteur privé tout en conservant la possibilité de voter des lois, règlements et même de retirer cette délégation. Pour que la corégulation fonctionne bien, cela exige des intérêts cohérents des parties prenantes, une participation de toutes les parties prenantes, des résultats facilement mesurables et un soutien par le public en général. L'Internet Corporation for Assigned Names and Numbers (ICANN) est actuellement un bon exemple de corégulation : ICANN détient son autorité du gouvernement américain et toutes les parties prenantes interviennent à la gestion d'ICANN. De même, un programme de formation ou de veille financé par un gouvernement mais réalisé par une organisation de la société civile ou du secteur privé constitue un exemple de corégulation car le gouvernement conserve le contrôle ultime de l'existence de ce programme de par son financement.

La **régulation** (« classique ») est une régulation où les gouvernements établissent les règles du jeu par des directives, lois et règlements. Cela correspond à une régulation gouvernementale nationale ou régionale (comme c'est le cas avec l'Union européenne et le Conseil de l'Europe) qui est habituellement contraignante et basée sur des lois, des règlements et des sanctions comme en ce qui a trait à la cybercriminalité. En matière de gouvernance d'Internet, on observe un 2^{e} mode de régulation gouvernementale où en lieu et place de lois, règlements, directives et sanctions, on retrouve des recommandations, souvent accompagnées d'aide financière pour permettre à la société civile ou au secteur privé de donner suite à ces recommandations. Pour distinguer ces deux formes de régulation, on les désignera respectivement « **régulation – mode directive** » et « **régulation – mode recommandation** ».

Bien qu'il existe plusieurs variations pour présenter la GI, on peut la détailler, globalement, en deux types :

- La gouvernance portant sur les aspects techniques d'Internet : cela inclut toute l'infrastructure technique permettant au contenu de transiter d'un utilisateur à un autre;
- La gouvernance portant sur les contenus et les services d'Internet : cela inclut toutes les préoccupations à la fois techniques et politiques permettant à deux utilisateurs et plus d'échanger des informations ou des services pertinents.

Certains auteurs proposent, explicitement ou non, une répartition de la gouvernance entre gouvernance technique et gouvernance politique. Cette répartition n'a pas été retenue car il est difficile, comme nous le verrons plus loin, d'extirper les considérations « politiques » de la gouvernance technique. Le gouvernement du Québec illustre assez bien cette difficulté :

> « Les difficultés viennent du fait que les dimensions techniques et institutionnelles de la gouvernance de l'Internet sont interreliées et ne peuvent être totalement séparées. Ainsi, le contrôle technique du serveur racine est fondamentalement lié à la stabilité et à la sécurité du réseau qui s'avèrent des conditions sine qua non au bon fonctionnement du commerce et des transactions électroniques. Il en va ainsi de la création de nouveaux noms de domaine … qui peut être vue comme une question purement technique, cependant elle a des conséquences économiques (revenus des enregistrements, commerce électronique, etc.), politiques (souveraineté, contrôle, etc.) et sociales. De plus, la promotion des cultures et la diversité linguistique dépendent de la technologie d'Internet. L'utilisation des caractères latins dans les codes et dans le système DNS limite l'utilisation d'autres alphabets différents. La diffusion et le contrôle du contenu sont étroitement liés aux technologies pouvant être utilisées sur le réseau de l'Internet qui, elles, dépendent des normes et des standards utilisés par les systèmes racine. »[28]

La diffusion et le contrôle du contenu sont étroitement liés aux technologies pouvant être utilisées sur le réseau de l'Internet qui, elles, dépendent des normes et des standards

Cette gouvernance, telle qu'illustrée dans la figure suivante, s'inscrit, bien sûr, dans une gouvernance plus vaste des technologies de l'information et des communications (TIC). Il est important de ne pas oublier cette couche de gouvernance car, bien souvent, les éléments de gouvernance établis pour les TIC peuvent s'appliquer intégralement ou presque pour la GI. Il ne s'agit donc pas de tout réinventer mais plutôt d'ajouter les éléments nécessaires pour obtenir une « bonne gouvernance » d'Internet.

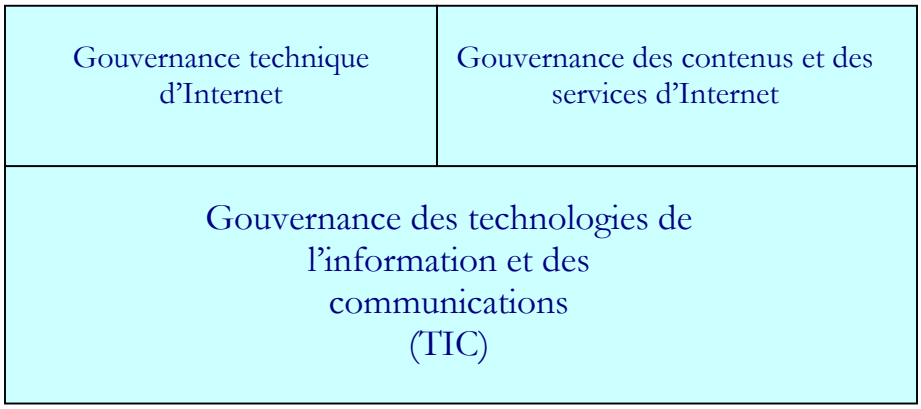


Figure 4.1 – Typologie de gouvernance[29]

[28] Consulter le document n° 21 du Cahier 4 *Gouvernance de l'Internet* (p. 3) (www.services.gouv.qc.ca/fr/enligne/societe/gouvernance.asp)

[29] Types de gouvernance basés notamment sur les travaux décrits dans le document n° 4 du Cahier 1 *Internet Governance : Theory and First Principles*

Cette interdépendance des couches de gouvernance comporte une caractéristique singulière : de par l'importance de plus en plus grande d'Internet, la gouvernance technique d'Internet est devenue une couche fondamentale et stratégique des TIC, d'où une focalisation importante, particulièrement durant les deux derniers SMSI, sur cette partie.

4.4 Gouvernance technique d'Internet

La gouvernance technique d'Internet repose principalement sur des normes, une collaboration d'institutions privées et publiques, des organismes dédiés à Internet et … une implication du gouvernement américain.

Le bon fonctionnement actuel d'Internet repose essentiellement sur une infrastructure technique robuste et sur un système de nommage et d'adressage éprouvé, le DNS (Domain Name System). Examinons la gouvernance de ce système.

4.4.1 Gouvernance du système de nommage et d'adressage (DNS)

Le DNS comprend les noms de domaine et leurs adresses Internet (adresses IP – Internet Protocol) correspondantes ainsi qu'une base de données réparties permettant, entre autres, d'établir cette correspondance. C'est une des bases de données les plus actives de toute la planète et celle, sans aucun doute, qui traite le plus de requêtes de correspondances par jour :

- Il y a des milliards d'adresses IP en usage;
- Il y a des milliards de requêtes faites au système de nommage chaque jour (environ 10 milliards de requêtes uniquement pour le « .com » géré par la firme VeriSign);

(http://web.si.umich.edu/tprc/papers/2005/441/Bauer-TPRC-2005-fin.pdf). Un autre auteur distingue trois objets de gouvernance, soit les politiques techniques, les politiques ayant trait à l'infrastructure de communication et les politiques sur les contenus et les services (consulter le document n° 14 du Cahier 4 *Guide to the International ICT Policy Making* - www.unicttaskforce.org/perl/documents.pl?id=1312). Pour les fins de l'étude, les deux premiers objets ont été regroupés en un seul.

- Il y a des changements tous les jours des noms de domaines et des adresses IP correspondantes;
- Il y a de nouveaux noms de domaines qui sont créés chaque jour;
- Il y a des milliers de personnes qui travaillent à effectuer les changements aux noms de domaine ou en acheter de nouveaux[30].

Le système des noms de domaine permet de naviguer facilement dans Internet. Ce système permet aux utilisateurs, pour aller à un site Web spécifique, d'utiliser un nom de domaine facile à mémoriser tel que celui de la Régie du cinéma du Québec : www.rcq.qc.ca . Le DNS transpose ce nom de domaine en une adresse IP composée d'un groupe de quatre nombres (ou octets), exprimés en décimal, séparés par des points, permettant d'identifier la connexion Internet désirée. Ainsi, www.rcq.qc.ca devient 142.090.10.27, par exemple et ce, de façon transparente pour l'utilisateur. C'est par l'adresse IP que le réseau Internet et ses différents ordinateurs peuvent communiquer entre eux. Cette adresse IP est basée sur la version 4 d'IP (appelée aussi IPv4) qui comporte 32 bits (et permet une possibilité de plus de 4 milliards d'adresses IP uniques) alors que la version 6 d'IP (IPv6) en cours d'implantation dans le monde comportant 128 bits présente une structure quelque peu différente mais entièrement compatible avec IPv4[31]. À titre d'exemple, le Canada dispose de IPv6[32]. La différence fondamentale entre ces deux versions d'adresses IP est que IPv6 permet de supporter un nombre beaucoup plus grand d'adresses IP et donc, de noms de domaine. Cette augmentation du nombre possible d'adresses IP sera particulièrement utile dans le contexte de l'internationalisation des noms de domaine (IDN – Internationalized Domain Names) permettant la prise en compte des alphabets des différentes langues du monde (telles que le français, l'arabe, l'hébreu, le chinois et le japonais). Cependant, tel que souligné par le Multilingual Internet Names Consortium (MINC), composé de 39 membres de toutes les régions du monde, le DNS, dans sa forme internationalisée (IDN) actuellement déployée, présente déjà des problèmes de fragmentation importants mais solubles si la communauté Internet et particulièrement l'ICANN et l'ISOC s'y penche[33].

---

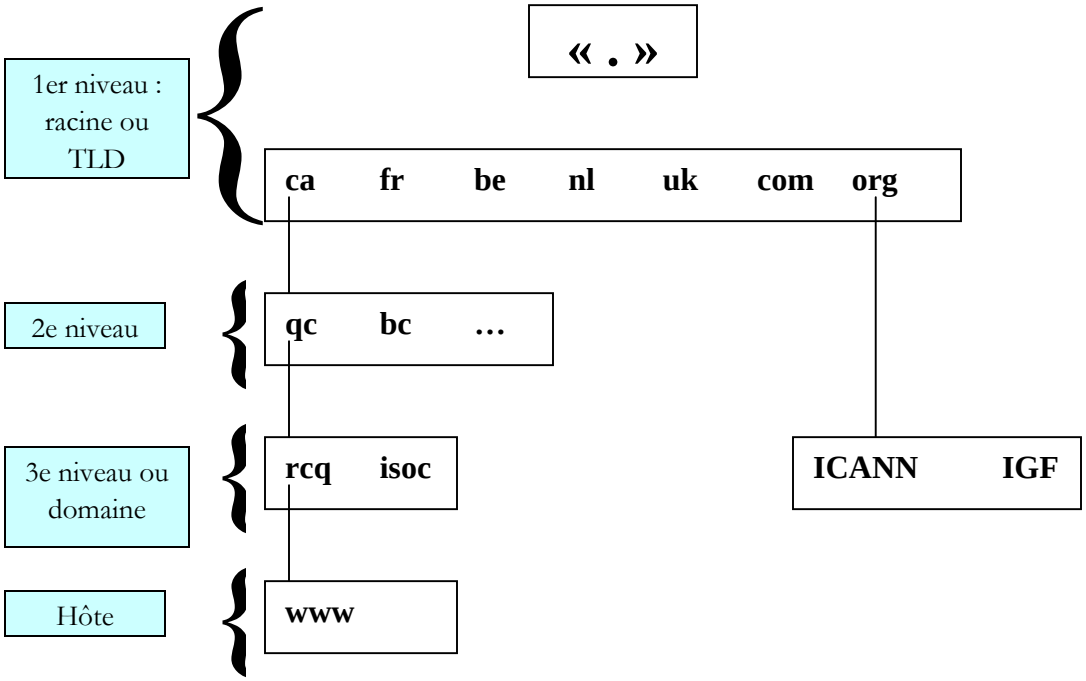
[30] Consulter le document n° 12 du Cahier 4 *How Domain Name Servers Work* (http://computer.howstuffworks.com/dns.htm/printable)

[31] Pour une information plus technique, consulter la norme d'IETF RFC 3513 décrite dans le document n° 9 du Cahier 4. (www.ietf.org/rfc/rfc3513.txt?number=3513)

[32] En date du 29 septembre 2006, consulter le document n° 10 du Cahier 4 *Root servers* (www.root-servers.org)

[33] Consulter le document n° 30 du Cahier 4 *De-fragmenting the Internet Namespace* produit par le MINC (www.minc.org/data/d6570566088xpdw_Final%20MINC%20IDN%20TLD%20Report.pdf)

La structure des noms de domaine est une vaste arborescence inversée. Au sommet, on retrouve la " *racine* " d'Internet, délimitée par le premier caractère « . » (à cette fin, lire le nom de domaine de droite à gauche). Au premier niveau, on trouve les « *Top Level Domains* » (TLD), puis viennent les domaines de second, troisième niveau, et ce jusqu'à une possibilité de 127 niveaux ! Mais en fait, on dépasse rarement les cinq niveaux. Chaque niveau de la hiérarchie est délimité par un « . » dans l'adresse Internet. Voir l'illustration à la figure suivante.



Exemples : www.rcq.qc.ca et www.icann.org

Figure 4.2 – Arborescence des noms de domaine[34]

Le terme « serveurs racine » sert justement à décrire les serveurs qui gèrent la partie de la base de données des noms de domaine correspondant au premier niveau des noms de domaine. Pour des raisons historiques, les « serveurs racine » sont au nombre de treize dont 10 sont situés aux États-Unis et 3 autres répartis dans le reste du monde (Japon, Royaume-Uni et Suède). Cependant, il est important de noter que ces treize serveurs racine

[34] Consulter le document n° 11.1 du Cahier 4, *Le système de nommage* (p. 3) (www.gouvernance-internet.com.fr/information/JRES2001.html)

ont mis en place des serveurs miroirs (copies des serveurs racine) de sorte que l'on retrouve, en réalité, plus d'une centaine de sites de serveurs racine répartis dans une quarantaine de pays, dont trois au Canada (Montréal et Toronto) et un de ceux-ci supportant IPv6[35]. Cette redondance des serveurs assure une très bonne stabilité, sécurité et performance du DNS. De plus, afin de garantir une plus grande stabilité ou sûreté du réseau Internet en Europe et éventuellement se doter d'une certaine indépendance par rapport à l'hégémonie américaine, les Européens ont mis en place une initiative (ORSN – European Open Root Server Network). Cette initiative permet de constituer une base de données européennes à partir de la partie de la base données des racines du DNS gérées par ICANN et de se doter ainsi d'une certaine indépendance ou autonomie pour le bon fonctionnement du système de nommage et d'adressage d'Internet si le DNS, à contrôle américain, arrêtait d'être disponible pour les Européens[36]. Il faut bien comprendre que ce n'est pas un système parallèle différent du DNS mais bien une copie identique, rafraîchie à tous les jours à partir du DNS « américain ».

Le premier niveau des noms de domaine, ou le niveau racine, comporte deux types :

- Nom de domaine de code de pays de premier niveau (country code Top Level Domain – ccTLD);
- Nom de domaine générique de premier niveau (generic Top Level Domain – gTLD).

Le nom de code de pays (ou de territoires) est composé de deux caractères[37] distincts (au nombre de 244 à la fin de septembre 2006) et définis selon la norme ISO 3166, laquelle est mise à jour selon les indications des Nations-Unies. Ainsi, on retrouve « .ca » et « .fr » pour le Canada et la France, respectivement. Il convient de souligner que chaque pays est libre de gérer le contenu de son domaine de la façon qu'il le désire. Ainsi, on assiste présentement à une certaine dérive de la signification de ces codes de pays dans le cas où le pays décide de l'utiliser pour autre chose

---

[35] Consulter la liste des serveurs racine et de leur miroirs répartis à travers le monde dans le document n° 10 du Cahier 4 *Root servers* (www.root-servers.org)

[36] Consulter le site Web d'ORSN : http://european.de.orsn.net/tech-switch-win.php et le document n° 14 du Cahier 2 *Political Oversight of ICANN* (p. 6) (http://internetgovernance.org/pdf/political-oversight.pdf) :

> « Already, alternative root server systems such as ORSN (European Open Root Server Network) in Europe have formed to provide a check on U.S. authority over the root zone.»

[37] Consulter www.iana.org/root-whois/index.html#c pour une liste complète et à jour des codes de pays. Cette liste est basée sur la norme ISO 3166 (document n° 13 du Cahier 4 - www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-fr1.html).

que la description des sites Web de son pays (tel que « .tv » attribué à l'île de Tuvalu mais utilisé pour décrire du contenu télévisuel et « tk » attribué à l'île de Tokelau mais utilisé pour décrire des services d'encans). De plus, certains pays ont décidé de structurer les autres niveaux de noms de domaine en y intégrant des noms qui se situent aussi comme premier niveau de domaine générique. On se retrouve ainsi au Japon avec « .com.jp » ou « .org.jp ». Ce qui fait qu'une organisation donnée peut se retrouver avec un nom de domaine différent selon ses propres choix d'inscription au DNS. La liberté est privilégiée mais pour l'utilisateur et la gouvernance, il est important de tenir compte de ce flou.

Les noms de domaine générique sont au nombre de 19 (fin septembre 2006) et comportent un nombre variable de caractères. Ils comprennent des noms génériques restreints (soit .edu, .gov et .mil réservés pour les États-Unis, .int réservé pour les organisations régies par des traités internationaux, et .arpa réservé pour le DNS et la correspondance entre les noms de domaine et les adresses IP) et d'autres noms génériques. Les noms de domaine générique ne possédant pas de taxonomie structurée, ISOC Québec en propose une à titre d'illustration :

- formes d'organisations (.biz, .com, .coop, .name, .org, .pro);
- secteurs d'activités (.aero, .jobs, .museum, .travel);
- communautés (.asia et .cat);
- types de technologies supportées (.mobi et .tel);
- autre (.info et .net)[38].

Contrairement aux noms de domaine de code de pays, la taxonomie des noms génériques (gTLD) n'étant pas soumise à une norme, présente une certaine difficulté de compréhension pour en retrouver la cohérence. Ainsi, il est difficile de trouver la différence entre « .com » et « .biz », et puisque tous les sites Web contiennent de l'information, il est difficile de comprendre la nécessité d'avoir ajouté le domaine générique « .info ».

Qui gère ce système de nommage et d'adressage ?

C'est principalement ICANN (Internet Corporation of Assigned Numbers and Names), organisme sans but lucratif incorporé en Californie, qui gère ce système en collaboration avec une multitude d'autres acteurs. La structure organisationnelle d'ICANN peut être représentée selon la figure suivante (en date d'octobre 2006).

[38] Consulter une courte explication des TLD génériques à la page 4 du document n° 11.2 du Cahier 4 *Le Domain Name System (DNS)* (www.commentcamarche.net/internet/dns.php3)

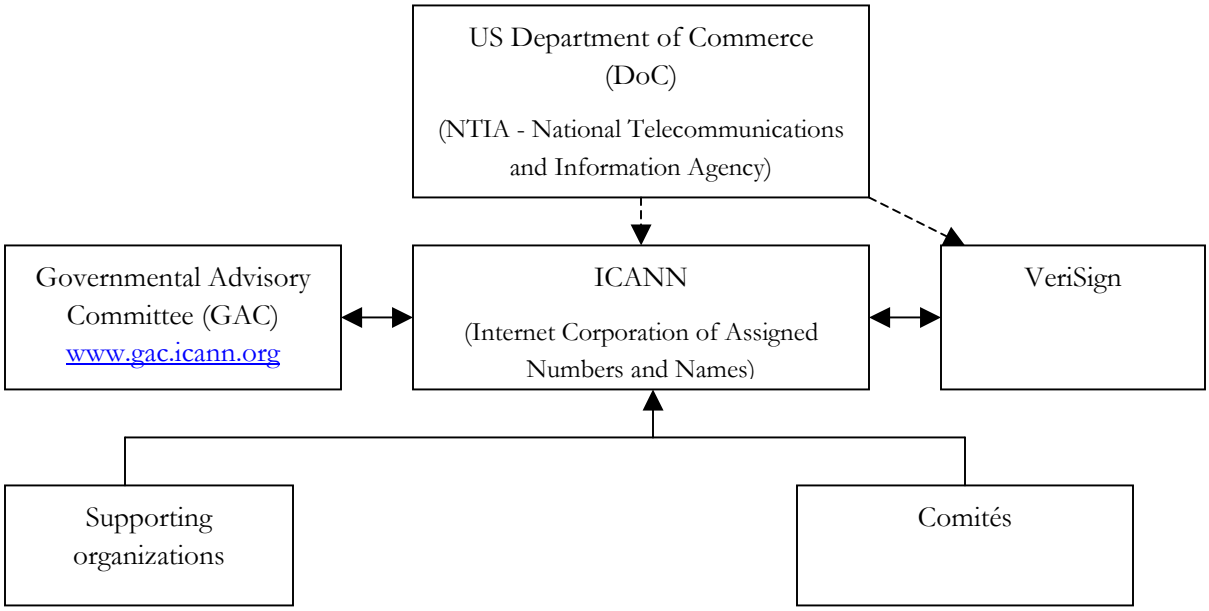


Figure 4.3 – Structure organisationnelle de gestion du DNS

Voici une description de certaines des entités de cette organisation de la gestion du DNS.

Agence NTIA

L'agence NTIA (National Telecommunications and Information Agency) du Département du Commerce américain (Department of Commerce – DoC ou USG – United States Government), a donné le mandat à ICANN de

gérer le système de nommage et d'adressage. Ce mandat, décrit dans l'entente du 1er octobre 2006, est valide pour une durée de trois ans[39].

L'agence a aussi accordé en 1998 un contrat, toujours valide, à la firme VeriSign (auparavant NSI) pour mettre à jour le fichier maître des racines du DNS[40] :

> « NSI agrees to continue to function as the administrator for the primary root server for the root server system …
>
> While NSI continues to operate the primary root server, it shall request written direction from an authorized USG official before making or rejecting any modifications, additions or deletions to the root zone file. »

Ce dernier contrat permet donc au gouvernement américain, s'il le désire, de bloquer ou d'initier des changements au fichier maître des racines du DNS.

ICANN

ICANN est un organisme sans but lucratif, incorporé en Californie. Il a la mission suivante, telle qu'exprimée dans l'entente intervenue en octobre 2006 avec le gouvernement américain : coordonnateur des fonctions techniques de la gestion du DNS d'Internet pour laquelle la stabilité et la sécurité constituent une priorité. ICANN a la responsabilité des fonctions suivantes (auparavant assumées par IANA – Internet Assigned Numbers Authority) :

- attribution des adresses IP (Internet Protocol) auprès des cinq registres (qui, à leur tour, se chargeront de les répartir selon les besoins de leurs régions desservies);
- sélection des protocoles utilisés;

---

[39] Consulter l'entente liant ICANN et le DoC dans le document n° 15 du Cahier 4 *Joint project agreement between DoC and ICANN* (www.icann.org/general/JPA-29sep06.pdf)

[40] Consulter l'entente entre NSI (devenue VeriSign) et le DoC dans le document n° 16 du Cahier 4 *Special Award Conditions NCR-9218742 Amendment No. 11* (www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm) et l'analyse de cette entente dans le document n° 14 du Cahier 2 *Political Oversight of ICANN: A Briefing for the WSIS Summit* (p. 6) (http://internetgovernance.org/pdf/political-oversight.pdf) :

> « 4. A cooperative agreement with VeriSign VeriSign, operator of the .com and .net domains and the world's largest commercial domain name registry, has a cooperative agreement with the U.S. Department of Commerce. The agreement, which dates back to the early days of the public Internet, authorizes it to run the hidden master server that publishes the official root zone file to the Internet's root servers. … The agreement is important for two reasons: 1) it was the instrument by which the U.S. government obtained and continues to exercise its authority to control the root; and 2) it compelled VeriSign to conform to the ICANN regime's regulations on registries and registrars. »

- gestion du système de nommage des premiers niveaux génériques (gTLD) et des codes de pays (ccTLD);
- supervision du système des noms de domaine (DNS);
- gestion du système des serveurs racine.

Tel que décrit sur son site Web, « ICANN est engagé à préserver la stabilité opérationnelle d'Internet, à promouvoir la compétition, à atteindre une large représentation des communautés d'Internet et à développer des politiques appropriées à sa mission au moyen de processus établis par le consensus en partant de la base des différentes communautés (bottom up). »[41] Et sur ce même site Web, ICANN insiste pour indiquer que les questions relatives aux utilisateurs d'Internet telles que le contrôle d'Internet, le pollupostage et la protection des données, ne sont pas de son ressort. Bien qu'ICANN se défend bien de toucher de près ou de loin au contrôle d'Internet, et en cela, respecte en tout point le principe de neutralité d'Internet, ICANN n'est pas entièrement indépendant du contrôle du contenu. Ainsi, récemment, le fait de vouloir créer le nom de domaine générique « .xxx » (gTLD), qui aurait servi à décrire du contenu pour adulte, et d'avoir révisé sa décision à la suite du veto du gouvernement américain, indique bien que ICANN n'est pas totalement étranger aux préoccupations de contenu que le DSN peut véhiculer, sous la perspective du gouvernement des États-Unis.

Bien qu'officiellement, le contrôle du contenu d'Internet n'est pas du ressort d'ICANN, le système DNS géré par ICANN n'est pas totalement dénué de politique publique en matière de contenu.

ICANN, est organisé de façon internationale, avec une équipe basée en Californie mais aussi répartie sur plusieurs continents. Il est appuyé par des collaborateurs gouvernementaux et du secteur privé (avec ou sans but lucratif) du monde entier. ICANN est gouverné par un Conseil des directeurs (Board of Directors) qui effectue un suivi sur le développement des politiques nécessaires à la gouvernance des aspects techniques d'Internet. Il est épaulé par trois « Organisations de soutien » (Supporting Organizations) et divers comités.

ICANN :

La meilleure organisation à l'heure actuelle pour effectivement gérer les aspects techniques d'Internet

ICANN, malgré toutes les critiques pouvant avoir été formulées à son endroit, est considéré comme la meilleure organisation à l'heure actuelle pour effectivement gérer les aspects techniques d'Internet et représenter toutes les parties prenantes mondiales d'Internet.

VeriSign

VeriSign est une organisation à but lucratif, incorporée au Delaware, qui a la mission, notamment, de mettre à jour le fichier maître racine du DNS, sur recommandation d'ICANN et approbation de l'agence

[41] Consulter www.icann.org/general

gouvernementale NTIA. Il est important de noter que VeriSign, s'est vue attribuer de la part du gouvernement américain, sans appel d'offres, la responsabilité de la gestion des domaines génériques « .net » et « .com », soit les domaines les plus imposants et lucratifs. De plus, VeriSign a la responsabilité de deux des treize serveurs racine et de la vingtaine de sites miroirs correspondants répartis à travers le monde, incluant deux des trois sites miroirs pour le Canada. Pour l'instant, il ne supporte que IPv4.

Il faut aussi signaler que VeriSign s'est vu attribuer en 2004 la gestion de « l'Internet des objets » ou le ONS (Object Naming Service), système servant à soutenir, au niveau mondial, le système d'identification et de repérage des objets basé sur les plaquettes d'identification par radiofréquence (RFID - Radio Frequency Identification) et les codes électroniques des produits (EPC - Electronic Product Code) correspondants[42] et, éventuellement; bien d'autres normes de codage de produits[43]. VeriSign gère le système ONS de la même façon que le DNS. Le système ONS, selon son utilisation future, peut devenir un système aussi important que le DNS d'Internet et éventuellement venir le complémenter.

On le constate, VeriSign constitue un joueur majeur dans la gouvernance d'Internet et les nouvelles technologies de nommage et d'adressage.

Governmental Advisory Committee (GAC)

Le « Comité consultatif des gouvernements » (GAC) est formé d'environ 90 représentants de gouvernements nationaux, d'organisations gouvernementales multinationales, d'organisations régies par un traité et d'autorités publiques.

Le mandat du GAC est de fournir des avis sur les activités d'ICANN qui concernent les gouvernements, soit les politiques publiques relatives aux fonctions assumées par ICANN[44].

Supporting organizations (SO)

Les organisations de soutien, au nombre de trois, comprennent :

---

[42] Consulter le document n° 5 du Cahier 1 *La gouvernance mondiale d'Internet* (p. 37) (www.assemblee-nationale.fr/12/rap-off/i2891.asp)

[43] Consulter les documents 17.1 *VeriSign to run EPC Directory* (www.rfidjournal.com/article/view/735) et 17.2 *EPC Network Architecture* (www.verisign.com.sg/guide/epc/epc_architecture.pdf) du Cahier 4 sur le nouveau système ONS développé par VeriSign.

[44] Pour plus de détails sur le GAC, consulter le document n° 19.1 du Cahier 4 *Introduction au GAC* (http://gac.icann.org/web/about/Introduction_to_the_GAC_in_French.ppt)

- Address Supporting Organization (ASO) - www.aso.icann.org;
- Country Code Domain Name Supporting Organization (CCNSO) - www.ccnso.icann.org;
- Generic Names Supporting Organization (GNSO) - www.gnso.icann.org.

L'Address Supporting Organization (ASO) est un comité formé de représentants des cinq Registres Régionaux d'Internet (RIR – Regional Internet Registry), soit :

- AFRINIC (African Network Information Center);
- APNIC (Asia-Pacific Network Information Center);
- ARIN (American Registry for Internet Numbers);
- LACNIC (Latin American and Caribbean Internet Addresses Registry);
- RIPE NCC (Réseaux IP Européens Network Coordination Centre).

Il a comme mission de passer en revue et développer, à l'intention du Conseil d'administration d'ICANN, des recommandations sur la politique des adresses IP gérées par les cinq RIR et de conseiller ce conseil sur ces sujets.

Les cinq RIR ont comme mission de gérer l'espace d'adresses IP dans leur région respective et ce, autant pour la version 4 que la version 6 (IPv4 et IPv6). Chaque RIR redistribue les adresses IP aux fournisseurs d'accès Internet de sa région (FAI/FSI) qui, à leur tour, les rend disponibles à leurs clients (commerciaux ou de la société civile), une fois qu'ils ont obtenu l'enregistrement de leur nouveau nom de domaine auprès des différents registraires tel qu'illustré à la figure suivante.

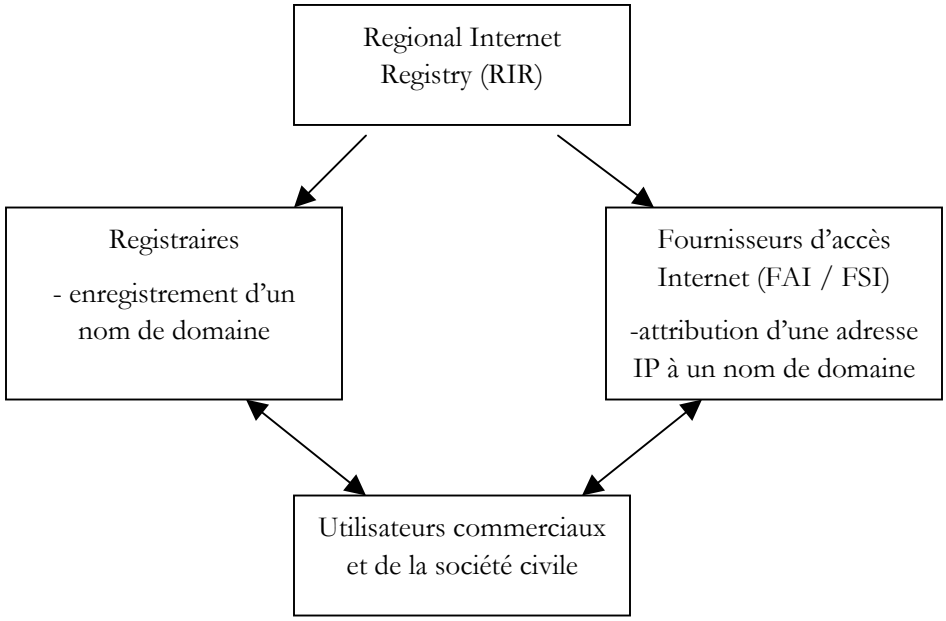


Figure 4.4 – Intervenants locaux dans le processus d'attribution d'adresses IP et d'enregistrement de noms de domaine

Le *Country Code Domain Name Supporting Organization* (CCNSO) est un comité formé, sur une base volontaire, de gestionnaires des domaines des codes de pays (ccTLD). Il a comme mission de développer et recommander, à l'intention du Conseil d'administration d'ICANN, des politiques globales relatives aux domaines de premier niveau des codes de pays (ccTLD) et ce, sur la base d'un consensus établi auprès de la communauté des gestionnaires des ccTLD. Il peut aussi, sur une base volontaire, développer un ensemble de « bonnes pratiques » à l'intention de ceux-ci et une meilleure coopération opérationnelle et technique entre ceux-ci[45].

Le Generic Name Supporting Organization (GNSO) est un comité formé, sur une base volontaire, de gestionnaires des domaines génériques (gTLD) et de toute autre partie prenante concernée. Il a comme mission de développer et recommander, à l'intention du Conseil d'administration d'ICANN, des politiques globales relatives aux domaines génériques de

[45] Consulter les règlements d'ICANN dans le document n° 19.2 du Cahier 4 *Bylaws For ICANN* (hwww.icann.org/general/bylaws.htm#IX)

premier niveau (gTLD). Plus, spécifiquement, les types d'entités faisant partie du GNSO sont les suivantes :

- des registres des gTLDs (extensions génériques, comme le « .com ») représentant tous les registres sous contrat avec ICANN;
- des registraires (marchands de noms) représentant tous les registraires accrédités et sous contrat avec ICANN;
- des fournisseurs d'accès et de services Internet (FAI / FSI);
- des entités commerciales et d'affaires d'Internet;
- des entités non commerciales utilisatrices d'Internet (organisations de la société civile d'Internet) (www.ncdnhc.org);
- des représentants des intérêts relatifs aux marques de commerce et à la propriété intellectuelle dans le DNS.

Tel qu'indiqué précédemment, la robustesse et l'utilisabilité d'Internet doivent leur force notamment à la présence de normes ou de standards. Deux organisations apportent une contribution significative à la normalisation, soit :

- ISOC – Internet Society;
- W3C – World Wide Web Consortium.

L'Internet Society – ISOC

ISOC est une organisation sans but lucratif, non gouvernementale, de stature internationale. Elle est composée de plus d'une centaine d'organisations professionnelles (incluant des entreprises, des fournisseurs d'accès à Internet, des fournisseurs de contenu d'Internet, des organisations sans but lucratif représentant des groupes d'intérêt public, des organisations professionnelles et d'affaires, des institutions d'enseignement et de recherche, des agences gouvernementales et d'autres organisations internationales) et de plus de 20 000 membres individuels répartis dans plus de 180 pays. ISOC compte près de 80 sections (Chapters) à travers le monde dont celle d'ISOC Québec (www.isoc.qc.ca). Son membership en fait une des organisations les plus représentatives de la communauté d'Internet à travers le monde.

Sa mission est de s'assurer du développement, de l'évolution et de l'utilisation d'Internet pour qu'il demeure ouvert pour le bénéfice de tous. Sa devise est « Internet pour tous. ». Internet Society focalise ses activités sur le développement des normes d'Internet et sur la formation technique et les politiques reliées la technologie. ISOC, pour accomplir sa mission, abrite plusieurs organisations en son sein que l'on peut représenter à la figure suivante. ISOC est particulièrement active, en politique publique,

dans les questions relatives à la censure, la liberté d'expression, la taxation, la gouvernance et la propriété intellectuelle.

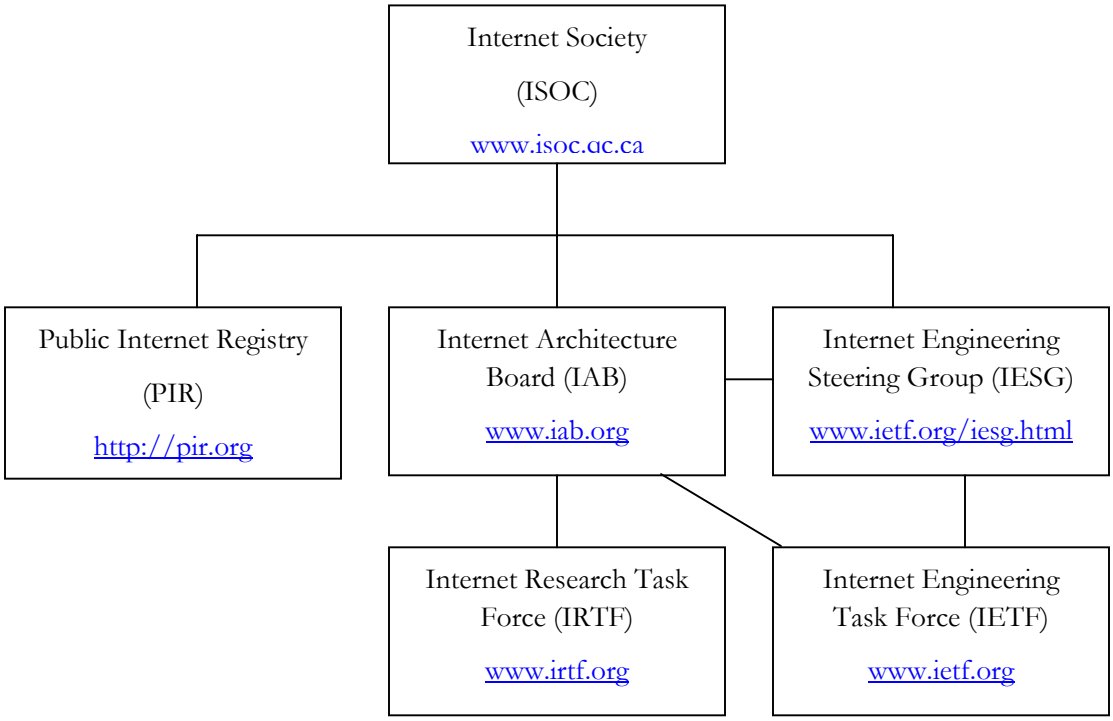


Figure 4.5 – ISOC et ses organisations associées

Voici une brève description de chacune de ces organisations.

Le *Public Internet Registry* (PIR - http://pir.org) est une organisation sans but lucratif créée par ISOC qui agit à titre de registraire pour gérer le domaine « .org ».

L'Internet Architecture Board (IAB) sert à plusieurs fins en architecture d'Internet :

- Comité pour l'IETF;
- Entité conseil pour ISOC;
- Entité d'appel concernant les décisions prises par l'IESG;
- Commanditaire de l'Internet Research Task Force (IRTF).

À titre de comité pour l'IETF, il a pour mission de s'occuper de la planification à long terme et de la coordination des différents domaines d'activité de l'IETF. L'IAB exerce une veille sur les questions importantes d'Internet et passe en revue la cohérence et l'intégrité architecturale des nouveaux groupes de travail de l'IETF.

L'*Internet Research Task Force* (IRTF) a pour mission de promouvoir la recherche névralgique pour l'évolution d'Internet en créant des groupes de travail de recherche à long terme sur des sujets reliés aux protocoles d'Internet, aux applications, à l'architecture et à la technologie.

L'*Internet Engineering Steering Group* (IESG) est formé d'une vingtaine de personnes provenant principalement de grandes firmes en technologies de l'information et des communications. Il a pour mission la gestion technique des activités des groupes de travail de l'IETF et du processus des normes d'Internet selon des règles et des procédures approuvées par ISOC. L'IESG approuve ou corrige le résultat des travaux de normalisation de l'IETF et facilite la mise en place de groupes de travail d'IETF et leur dissolution. Une recommandation acceptée par l'IESG devient un RFC (Request for Comments) puis éventuellement une norme, après validation par d'autres instances (soit l'Internet Architecture Board et l'Internet Society).

L'*Internet Engineering Task Force* (IETF), organisation ouverte à tous, regroupe des personnes intéressées par les évolutions d'Internet : concepteurs de réseaux, administrateurs de systèmes, producteurs de matériel et de logiciels, développeurs, chercheurs et autres. L'IETF, structuré en groupes de travail temporaires, élabore des propositions de normes (à destination de l'IESG) ou fournit des procédures d'élaboration de normes, pouvant servir par la suite à d'autres organismes de normalisation (tels que W3C et ISO – Organisation internationale de normalisation). Plus précisément, l'IETF a pour mission :

- d'identifier et de résoudre les problèmes immédiats affectant le fonctionnement d'Internet;
- de spécifier des protocoles ou des architectures de réseaux susceptibles de limiter ces problèmes à l'avenir;
- d'émettre des propositions de normes et de standards pour Internet auprès de l'IESG;
- de favoriser le transfert de technologies et d'informations de la part de l'IRTF vers la communauté Internet mondiale;

- de fournir un forum d'échanges d'information au sein de la communauté d'Internet et ses différentes parties prenantes.

Le World Wide Web Consortium - W3C

Le W3C regroupe aujourd'hui plus de 400 membres (sociétés, organisations issues de l'industrie, organismes de recherche et gouvernementaux). Le W3C emploie par ailleurs plus de 70 personnes réparties sur trois sites (États-Unis, Europe et Japon). Si l'on essaie de distinguer d'une façon simple entre W3C et IETF, on pourrait dire que W3C porte son attention sur les normes du Web (le contenu) alors que IETF porte son attention sur les normes d'Internet (le contenant, y incluant le DNS). La devise de W3C est « Le Web pour tous ». Cependant, le membership à W3C n'est pas gratuit et peut-être un frein à un membership élargi. Heureusement, certaines sections locales de W3C telle que celle de W3C Québec (www.w3qc.org) ont réduit les frais d'adhésion de façon à éliminer presque complètement ce frein à une adhésion locale.

Les activités du W3C sont organisées en quatre domaines :

- Architecture (développement des technologies requises par le Web);
- Interaction (amélioration de l'interaction entre le Web et ses utilisateurs);
- Technologie et Société (développement des infrastructures du Web en vue de répondre aux problématiques sociales, légales et de politique publique);
- Initiative pour l'Accessibilité du Web (développement de solutions pour rendre le Web accessible, principalement aux personnes handicapées).

La mission du W3C est :

- de proposer une vision aussi précise que possible du futur du Web afin de permettre le développement de solutions techniques aux enjeux qu'il soulève;
- de concevoir des technologies allant dans le sens de la réalisation de cette vision et tenant compte aussi bien des technologies déjà existantes que de celles à venir;
- de participer à l'effort de standardisation des technologies du Web en créant des « recommandations » librement disponibles à tous.

W3C aborde de plus d'autres problématiques auxquelles il tente de répondre telles que la protection de la vie privée (notamment avec la norme P3P), l'innovation en matière de gestion des brevets ou encore les

implications sociales du « Web sémantique » (et la norme RDF utilisée notamment par l'ICRA pour la classification du contenu de sites Web)[46].

4.4.2 Gouvernance de l'infrastructure technique

La gouvernance de l'infrastructure technique de communications est assurée principalement par l'Union Internationale des Télécommunications (UIT - www.itu.int). D'autres instances plus nationales ou régionales interviennent pour préciser ou coordonner les télécommunications. C'est le cas, au niveau régional par exemple, de l'Union européenne avec l'organisme European Telecommunications Standards Institute (ETSI).

Union internationale des télécommunications (UIT)

L'Union internationale des télécommunications compte quelque 800 membres incluant 191 états membres. L'UIT est une organisation à part entière des Nations-Unies. C'est d'ailleurs l'UIT qui a été choisie pour organiser les deux sommets mondiaux sur la société de l'information (SMSI). Les membres sont aussi bien des décideurs et des représentants des organismes de réglementation du secteur que des opérateurs de réseaux, des équipementiers, des concepteurs de matériels et de logiciels, des organisations régionales de normalisation ou encore des institutions de financement. Les activités, stratégies et orientations de l'UIT sont donc déterminées et conçues par l'industrie.

L'UIT repose sur le principe de la coopération internationale entre les gouvernements et le secteur privé. Il convient de noter que l'UIT ne comporte pas de membres, du moins actuellement, représentatifs de la société civile. Elle représente une instance mondiale au sein de laquelle le secteur public et le secteur privé peuvent se réunir pour parvenir à un consensus sur une grande diversité de questions.

Les activités de l'UIT se retrouvent regroupées en trois secteurs qui collaborent à la mise en place des réseaux et des services de demain, soit :

- Secteur des radiocommunications (UIT-R);
- Secteur de la normalisation des télécommunications (UIT-T);
- Secteur du développement des télécommunications (UIT-D)[47].

46 Consulter le document n° 20 du Cahier 4 *W3C* (www.dicodunet.com/definitions/normes/w3c.htm)

Leurs activités s'étendent à toutes les branches des télécommunications, soit : normalisation visant à faciliter l'interfonctionnement transparent des équipements et des systèmes à l'échelle mondiale, adoption de procédures d'exploitation pour une gamme de services hertziens qui ne cesse de s'élargir et élaboration de programmes destinés à améliorer les infrastructures de télécommunication dans les pays en développement. C'est en grande partie grâce aux travaux de l'UIT que les télécommunications ont pu atteindre un niveau d'activités se chiffrant à mille milliards de dollars (USD).

À titre d'exemples de normalisation, on peut citer les normes suivantes :

- norme mondiale de téléphonie cellulaire IMT-2000 permettant la mise en place de nouveaux services interactifs ou services « de la troisième génération » : accès rapide aux données, messagerie unifiée et services multimédias à large bande. Si l'industrie décide de mettre en place des réseaux et services de la troisième génération utilisant la norme IMT-2000, les abonnés aux systèmes cellulaires de la troisième génération pourront bientôt utiliser en toute continuité des systèmes réellement mobiles à l'échelle mondiale et y avoir accès en tous lieux et à tout moment;
- norme de compression des signaux vidéo H.264 permettant l'accès par Internet à la vidéo en temps réel depuis des serveurs distants;
- norme H.323 facilitant l'acheminement des signaux téléphoniques, vidéo et de données sur les réseaux informatiques tels qu'Internet et jouant ainsi un rôle essentiel dans la conception de nouveaux services de téléphonie utilisant le protocole IP (VoIP).

European Telecommunications Standards Institute (ETSI)[48]

L'ETSI est une organisation sans but lucratif dont la mission est de produire des normes de télécommunications et de contribuer ainsi à l'effort mondial de normalisation en matière de technologies de l'information et des communications (TIC). Elle offre aussi des services de bancs d'essai d'interopérabilité. Elle est basée en France et est officiellement reconnue pour la normalisation du secteur des TIC au sein de l'Union européenne. Elle compte 654 membres provenant de 59 pays tant de l'Europe que de l'extérieur de l'Europe. Ses membres comprennent des équipementiers, des opérateurs de réseaux, des administrateurs, des fournisseurs de services, des entités de recherche et des utilisateurs. Elle se préoccupe de domaines tels

---

[47] Consulter le document 14 du Cahier 4 *Guide to International ICT Policy Makers* (pp. 24 à 27) (www.unicttaskforce.org/perl/documents.pl?id=1312) ainsi que le document n° 25 du Cahier 4 *L'UIT et ses trois secteurs d'activités* (www.itu.int/aboutitu/overview/index-fr.html)

[48] Consulter le site Web de l'ETSI : www.etsi.org/about_etsi/5_minutes/5min_a.htm

que les télécommunications, incluant la téléphonie de 3e génération, la télédiffusion (« broadcasting »), le transport intelligent et l'électronique médicale.

4.5 Gouvernance des contenus et des services d'Internet

Avant d'aborder la gouvernance des contenus et des services d'Internet, il convient de rappeler le contexte de l'étude : la protection de la jeunesse par rapport aux documents audiovisuels circulant sur Internet. Les dangers reliés à l'utilisation d'Internet, rappelons-le, sont de différente nature, à savoir[49] :

- Images blessantes ou traumatisantes (racisme, violence, pornographie voire pédopornographie);
- Mauvaises rencontres (leurres dans les « chats » : adultes qui se font passer pour des enfants);
- Dépendance (perte de temps, abrutissement, désinvestissement des relations «incarnées», désinvestissement social …);
- Addiction;
- Cyber marketing;
- Cyber intimidation;
- Atteintes au droit à l'image et à la vie privée;
- Vol d'identité;
- Responsabilités civiles et pénales pouvant être engagées par certains agissements sans que les parents et leurs enfants en soient conscients.

On peut le constater, ce ne sont pas tous les dangers énumérés ci-dessous qui sont reliés aux documents audiovisuels. En fait, c'est principalement le premier, soit les « images blessantes ou traumatisantes », qui constitue celui directement associé aux documents audiovisuels numériques. D'autres dangers, indirects cette fois-ci, mais tout aussi importants et réels, peuvent découler de ce premier danger comme la dépendance et le vol d'identité.

Il est important de plus de rappeler que la protection de la jeunesse s'inscrit directement dans le programme de travail découlant du SMSI de Tunis (Agenda de Tunis) :

49 Synthèse du Congrès sur la famille tenu en 2005. Consulter le document n° 24 du Cahier 4 *Protection de l'enfance et Internet* (http://docsite.cgt.fr/1119018938.pdf)

> « Élément 24: cadres de référence de la régulation du contenu visant à protéger les utilisateurs d'Internet de contenu nuisible et d'abus en ligne, mais uniquement en relation avec les enfants et les adolescents. »

La gouvernance des contenus et des services englobe des questions importantes telles que la protection des mineurs, la cybercriminalité, le commerce électronique et la confiance qui lui est accordée, la sécurité et la vie privée, les droits d'auteur et la création de contenu local. Étant donné le lien étroit entre la gouvernance du contenu et les valeurs culturelles et sociales, des approches nationales (ou même par province ou état) sont souvent plus appropriées et préférées. D'ailleurs, dans le chapitre suivant sera abordée justement la gouvernance des contenus sur Internet selon différents pays.

Malgré ce fait, il est fréquent que des choix nationaux aient des répercussions au niveau des autres pays et que ces choix commandent une certaine coordination à l'échelle mondiale. À cet effet, se référer au cas de Yahoo en France ainsi qu'à la législation européenne adoptée en 2002 contre le pollupostage rendant obligatoire l'abonnement (opt-in) mais qui ne peut s'appliquer aux organisations non européennes[50]. Dans cette section, seule cette coordination internationale sera abordée.

Des initiatives ont été prises pour mettre en place une gouvernance de contenu et des services respectueuse des utilisateurs d'Internet. Ces initiatives ont recours à des approches de gouvernance variées, qu'on pourrait qualifier de « gouvernance multicouche » faisant appel à l'autorégulation, la corégulation ou la régulation dite classique[51].

Ces initiatives se retrouvent parrainées par des organisations comme l'Internet Content Rating Association (ICRA), l'UNESCO, le Conseil de l'Europe, l'Union Européenne, le Réseau européen de la corégulation d'Internet, l'Organisation mondiale du Commerce (OMC) et l'Organisation Mondiale de la Propriété Intellectuelle (OMPI). D'autres organisations nationales, tant au Canada qu'aux États-Unis, ont aussi mis en place de telles initiatives. Nous réserverons la couverture des initiatives nationales dans le chapitre suivant sur la gouvernance des contenus sur Internet par pays.

---

[50] Consulter le document n° 26 du Cahier 4 *Report on « Internet Governance »* (http://network.foruminternet.org/article.php3?id_article=23)
[51] Consulter le document n° 4 du Cahier 1 *Internet Governance: Theory and First Principles* (http://web.si.umich.edu/tprc/papers/2005/441/Bauer-TPRC-2005-fin.pdf)

L'Internet Content Rating Association (ICRA - www.icra.org) est une organisation à vocation internationale à but non lucratif réunissant les leaders d'Internet (particulièrement de l'Europe et des États-Unis) et visant à développer un Internet plus sûr. Sa mission est double :

- protéger les enfants des contenus potentiellement dangereux;
- protéger la liberté d'expression sur Internet.

L'ICRA est financé en partie par le programme européen « Safer Internet »[52]. L'ICRA a développé une approche d'étiquetage (ou de catégorisation), sur une base volontaire, du contenu d'Internet et qui, pour être déployée, commande une coordination à l'échelle mondiale dans le domaine du contrôle du contenu d'Internet. Son approche de gouvernance est basée sur une autorégulation visant à atteindre un meilleur équilibre entre la libre circulation des contenus numériques et la protection des enfants contre les contenus potentiellement dangereux. La proposition d'affaires de l'ICRA est double :

- méthode d'étiquetage (ou de catégorisation) du contenu;
- logiciel de filtrage du contenu, sur la base des « étiquettes ICRA ».

La méthode d'étiquetage repose avant tout sur un vocabulaire descriptif, souvent appelé « questionnaire de l'ICRA »[53] qui permet aux fournisseurs de décrire le contenu de leurs sites Web (au niveau de tout un site, d'une seule page ou d'un seul objet). Le questionnaire porte sur des sujets tels que la nudité et le contenu sexuel d'un site, la violence, le langage utilisé, le jeu, les drogues, l'alcool et les facilités d'interaction (par clavardage, forum ou autre). Cette description formalisée sert à produire des étiquettes (en format RDF) que le fournisseur de contenu va inclure dans son site Web.

Ce n'est donc pas l'ICRA qui effectue ce travail, mais bien les fournisseurs de contenu. Il est à noter que le vocabulaire descriptif, mis au point par un comité international, se veut aussi neutre et objectif que possible. Il ne recourt donc pas à des évaluations basées sur l'âge. Il a été révisé en 2005 pour permettre une meilleure application à un plus large éventail de contenus numériques, et pas seulement aux sites Web. Le vocabulaire descriptif supporte plusieurs langues, dont le français, l'anglais et le « chinois ». En 2006, environ 200 000 sites Web (dont ceux de Microsoft, Yahoo et AOL) utilisaient des étiquettes d'ICRA pour décrire le contenu de leur site Web. Ce nombre demeure cependant minime si l'on se réfère aux dizaines de millions de sites Web dans le monde et encore plus minime si

[52] Consulter le document n° 4 du Cahier 5 *100,000 websites apply descriptive labels* (www.saferinternet.org/ww/en/pub/insafe/news/articles/0505/icra.htm)
[53] Pour une description détaillée du vocabulaire de l'ICRA, consulter le document n° 23 du Cahier 4 *Vocabulaire descriptif de l'ICRA* (www.icra.org/vocabular)

l'on prend en compte les millions de blogues et sites de clavardage (« chat ») où peuvent transiter du texte mais aussi des documents audiovisuels. C'est un peu une démonstration que l'autorégulation, non soutenue énergiquement, n'est pas (toujours?) très efficace pour la protection de la jeunesse sur Internet.

Les internautes, et en particulier les parents de jeunes enfants, peuvent ensuite utiliser un logiciel de filtrage pour autoriser ou interdire l'accès à certains sites Web en fonction des informations présentes dans l'étiquette. La décision subjective d'autoriser ou d'interdire l'accès à un contenu est donc prise par les parents. ICRA et bien d'autres fournisseurs de logiciels, proposent un logiciel de filtrage qui permet d'exploiter les « étiquettes ICRA ». Le logiciel d'ICRA, ICRA Plus, a ceci de particulier qu'il est offert gratuitement[54].

Mission de l'UNESCO : favoriser la libre circulation des idées par le mot et par l'image.

L'Organisation des Nations Unies pour la Science, l'Éducation et la Culture (UNESCO - United Nations Educational, Scientific and Cultural Organization[55]) est une organisation des Nations-Unies dont la mission est « d'autonomiser les populations via la libre circulation des idées par le mot et par l'image, et par l'accès à l'information et au savoir. »[56] Une des pièces maîtresses qui guide l'UNESCO est bien sûr la *Déclaration des droits de l'homme* qui affirme les libertés fondamentales sans égards à la race, au sexe, à la langue ou à la religion. L'UNESCO dispose de deux organisations particulièrement concernées pour le sujet de l'étude présente, soit le Secteur des communications et de l'information (UNESCO-CI) et le Groupe de travail sur les technologies de l'information et des communications UN-ICT Taskforce).

UNESCO-CI comporte six thèmes de travail, à savoir :

- accès à l'information - avoir accès et contribuer aux flux d'information et de connaissances;
- renforcement des capacités - permettre à chacun d'acquérir, d'évaluer et d'utiliser l'information avec un regard critique dans sa vie professionnelle et privée, par le biais de programmes d'éducation aux médias et d'alphabétisation numérique. Un des sous-thèmes porte sur « la jeunesse et la société de l'information » et inclut le programme InfoJeunesse mis en

[54] Ce logiciel ne fonctionne que sous le système d'exploitation Windows. Il est à noter que ce logiciel arrive bon dernier lors de l'évaluation des logiciels de filtrage publiée sur le site Web de l'organisme Action Innocence qui a pour vocation de donner une information détaillée de différents filtres existants sur le marché. Consulter le document n° 35.2 du Cahier 4 *Tests des logiciels des contrôles parentaux* (www.filtra.info/web/resultats.aspx?nav=3)
[55] Consulter www.unesco.org ou http://portal.unesco.org/fr/ev.php-URL_ID=29009&URL_DO=DO_TOPIC&URL_SECTION=201.html
[56] Consulter le document n° 14 du Cahier 4 *Guide to International ICT Policy Makers* (pp. 43 et suivantes) (www.unicttaskforce.org/perl/documents.pl?id=1312)

œuvre par l'Institut national de la Jeunesse et de l'Éducation populaire de France;

- développement de contenu – particulièrement le contenu créatif (radio, télé et nouveaux médias) et le multilinguisme dans le cyberespace;
- liberté d'expression;
- développement des médias;
- préservation de la mémoire des peuples.

L'UN-ICT Taskforce[57] a été mis sur pied par le Secrétaire général des Nations-Unies pour le conseiller en matière de TIC et particulièrement en matière de gouvernance concernant la société de l'information et les deux sommets mondiaux de la société de l'information (SMSI) organisée par les Nations Unies. Le Groupe de travail a produit de nombreux documents sur la gouvernance d'Internet.

Le *Conseil de l'Europe*[58] est composé de 46 pays de l'Europe (dont les 27 de l'*Union européenne*) et de cinq pays observateurs, dont le Canada. Le Conseil de l'Europe a établi, en ce qui a trait au thème « médias et démocratie », les priorités suivantes :

- l'équilibre entre la liberté d'expression et d'autres droits fondamentaux (droit au respect de la vie privée, droit à un procès équitable, etc.);
- les services en ligne et la démocratie (« cybercontenus » illicites et préjudiciables, initiation à Internet);
- la convergence des technologies et services de communication et son impact sur la régulation des médias;
- le pluralisme et la diversité des médias, à la lumière du développement de la concentration, des nouvelles technologies et des nouveaux services de communication;
- l'interaction entre la liberté d'expression et d'information et la lutte contre le terrorisme.

Le *Conseil de l'Europe* englobe de plus *l'Observatoire européen de l'audiovisuel*. Il collecte auprès de 35 États membres et de la *Commission européenne*, traite et distribue des informations sur le développement du marché, du droit et du financement de l'audiovisuel.

---

[57] Consulter le site Web www.unicttaskforce.org/perl/documents.pl?id=1594
[58] Pour plus de détails sur le *Conseil de l'Europe*, consulter le site Web www.coe.int/T/F/Com/A_propos_Coe/medias.asp

L'*Union européenne* est composée de 27 pays de l'Europe. Elle adopte des politiques publiques, des normes et règlement élaborés par la *Commission européenne,* en matière de technologies de l'information et des communications (TIC) pour l'Europe. La *Commission européenne*, en plus de son rôle de recommandation de politiques, normes et règlements, joue un rôle de suivi de leur mise en place, une fois adoptés par le parlement de l'*Union européenne*. La *Commision européenne* comporte plusieurs secteurs d'activités dont trois méritent d'être soulignés, soit celui de l'Éducation et de la Culture, celui de la Société de l'information et celui des Marchés internes.

La *Direction générale de l'Éducation et de la Culture* a pour mission la préservation et l'amélioration de la diversité culturelle européenne dans divers domaines, dont celui de l'audiovisuel. Elle inclut des politiques reliées au secteur de l'audiovisuel tel que le cadre réglementaire « Télévision sans frontière »[59]. Ce dernier inclut, notamment, une directive actuellement à l'étude sur les « Services de médias audiovisuels », des recommandations adoptées sur la « Protection des mineurs dans un environnement en ligne »[60] et le « Patrimoine des films européens » ainsi qu'une charte des films en ligne (European Charter on Film Online[61]).

La *Direction générale de la Société de l'information* a pour mission de favoriser la mise en place d'une culture électronique, particulièrement avec son programme « i2010 » permettant à l'Europe de soutenir sa croissance et son emploi. Cette direction s'intéresse à plusieurs domaines lui permettant d'atteindre ces objectifs dont le RFID.

La *Direction générale des Marchés internes* a pour mission d'assurer la libre circulation des personnes, des biens, des services et du capital à l'intérieur de l'Union européenne. Cette directions se préoccupe de sujets tels que la protection des données, les droits d'auteur et de propriété intellectuelle.

Le *Réseau européen de la corégulation d'Internet* (EICN - European Internet Coregulation Network)[62] est composé de neuf organisations principalement

[59] Consulter le site Web de la *Commission européenne* sur le sujet : http://ec.europa.eu/comm/avpolicy/index_en.htm

[60] Consulter les documents n° 29.1 *Protection of Minors and Human Dignity - Recommendation* (http://ec.europa.eu/comm/avpolicy/reg/minors/index_en.htm) et 29.2 *Recommandation du parlement européen et du conseil sur la protection des mineurs* (http://eur-lex.europa.eu/LexUriServ/site/fr/com/2004/com2004_0341fr01.pdf) du Cahier. 4.

[61] Consulter le site Web http://ec.europa.eu/comm/avpolicy/other_actions/content_online/index_en.htm#charter

[62] Pour plus de détails, consulter le site Web http://network.foruminternet.org/article.php3?id_article=2

européennes. Il a pour mission de mettre en place un réseau d'expertise sur les questions légales relatives à Internet, d'organiser des débats avec toutes les parties prenantes sur les questions d'utilisation d'Internet dont le pollupostage, la protection des mineurs et les droits de la propriété intellectuelle ainsi que de faire des propositions auprès des institutions européennes. C'est ainsi cet organisme qui a proposé le document de réflexion sur la protection des mineurs et la téléphonie mobile[63]. De plus, l'EICN a dégagé cinq principes en matière de protection des mineurs sur Internet, soit :

- l'éducation est la clé pour atteindre une sûreté plus élevée sur Internet;
- un soutien important pour le développement d'outils de contrôle basés sur l'âge devrait aider les producteurs de contenus à rendre Internet plus sûr pour les mineurs;
- les logiciels et services de contrôle parental sont des outils complémentaires pour la protection des enfants de contenus nuisibles;
- le pollupostage devrait être combattu à titre de porteur de contenus nuisibles;
- toutes les parties prenantes devraient viser à faire d'Internet mobile de la prochaine génération (3G) plus sûr qu'Internet en général.

L'*Organisation mondiale du Commerce* (OMC)[64] est composée de 149 pays et d'une organisation de quelque 600 personnes ayant son siège à Genève. Elle s'occupe des règles régissant le commerce entre les pays et s'acquitte plus précisément des fonctions suivantes :

- Administration des accords commerciaux de l'OMC;
- Cadre pour les négociations commerciales;
- Règlement des différends commerciaux;
- Suivi des politiques commerciales nationales;
- Assistance technique et formation pour les pays en développement;
- Coopération avec d'autres organisations internationales.

L'OMC a le mandat d'examiner toutes les questions reliées au commerce global, y incluant le commerce électronique. Ainsi, depuis 1998, un moratoire a été décrété sur les taxes aux douanes pour les biens ou services échangés de façon électronique.

---

[63] Consulter le document n° 27 du Cahier 4 *Protecting Minors from Exposure to Harmful Content on Mobile Phones* (http://network.foruminternet.org/IMG/pdf/reco-mobile-20050728.pdf)

[64] Consulter le site Web www.wto.org/french/thewto_f/whatis_f/whatis_f.htm

L'*Organisation mondiale de la propriété intellectuelle* (OMPI)[65] est une institution spécialisée des Nations-Unies qui a son siège à Genève et composée de 183 états-membres. Sa mission consiste, selon les termes de l'OMPI, à « élaborer un système international équilibré et accessible de propriété intellectuelle qui récompense la créativité, stimule l'innovation et contribue au développement économique tout en préservant l'intérêt général. » Par propriété intellectuelle, on entend la propriété industrielle d'une part, comprenant des éléments tels que les brevets et les marques et, d'autre part, le droit d'auteur comprenant des éléments tels que les films, les oeuvres musicales, les oeuvres d'art telles que dessins, peintures, photographies et sculptures.

Il est important de noter que l'OMPI ne prend pas en compte les efforts d'autres organisations visant à élargir le concept de protection des droits d'auteur tel que le Creative commons destiné à favoriser la diffusion d'œuvre dans un contexte beaucoup plus libre de droit d'auteur ainsi que le concept de « copyleft » proposé par le mouvement du logiciel libre sur lequel reposent par exemple, plusieurs des logiciels utilisés sur Internet dont 75 % des serveurs Web à travers le monde.

Dans le cadre de son programme « Digital Agenda » en réponse à la convergence d'Internet, des technologies digitales et du système de propriété intellectuelle, l'OMPI a entrepris des discussions pour encourager la dissémination et l'utilisation de la propriété intellectuelle telle que la musique et les films, tout en protégeant les droits de leurs créateurs et de leurs propriétaires.

Les efforts pour internationaliser le DNS d'Internet comportent des défis techniques et d'interopérabilité, aussi bien qu'un certain nombre de défis concernant le contenu tels que des accords administratifs appropriés pour les domaines multilingues et les noms de domaines de premier niveau (TLD). Cela implique un dispositif de résolution de conflit qui puisse être disponible à l'échelle de tous les pays. D'ailleurs, l'OMPI, de concert avec d'autres organisations[66], gère pour l'ICANN, sur une base volontaire, le processus de résolution de conflit des droits de propriété intellectuelle relatifs aux noms de domaine (Uniform Dispute Resolution Process – UDRP). En date d'octobre 2006, l'OMPI avait réglé quelques 25 000 cas reliés aux noms de domaine, dont la majeure partie de ceux-ci sont reliés au cybersquattage - pratique abusive consistant à faire enregistrer des noms de domaine relatifs à des marques de commerce connues, dans l'intention de

[65] Consulter le site Web www.wipo.int/portal/index.html.fr

[66] Ces autres organisations accrédités pour gérer les conflits selon le processus convenu par ICANN comprennent : Asian Domain Name Dispute Resolution Centre, CPR: International Institute for Conflict Prevention and Resolution et The National Arbitration Forum (NAF). Consulter le site Web : www.icann.org/dndr/udrp/approved-providers.htm

réaliser un profit en les revendant aux sociétés propriétaires de ces marques (source : OQLF)[67].

On peut le constater, la gouvernance des contenus et des services ne contient pas énormément d'organisations internationales, avec la préoccupation de la protection de la jeunesse. Nous le verrons dans le chapitre suivant, il y a davantage d'organisations à portée nationale qui porte cette préoccupation. La protection de la jeunesse sur Internet est un peu dans son enfance ! La situation est cependant tout à fait compréhensible et cohérente avec les principes mêmes de l'architecture d'Internet dont celui de la neutralité (ou du principe du « bout en bout ») où l'on place l'intelligence aux extrémités du réseau. On s'est préoccupé énormément de la mise en place et du bon fonctionnement du réseau lui-même. Maintenant qu'il fonctionne plutôt bien et qu'il s'étend à d'autres technologies telles que la téléphonie mobile, la protection de la jeunesse devient davantage pressante à être abordée et maîtrisée et ce, en mode de « gouvernance multicouche ».

4.6 Gouvernance des technologies de l'information et des communications (TIC)

Internet fait partie de l'ensemble plus vaste des technologies de l'information et des communications (TIC). Avec l'omniprésence d'Internet dans plusieurs des sphères des TIC, la gouvernance d'Internet est devenue très importante. Cependant, il est important de retenir que plusieurs des organismes nationaux et internationaux existants avant l'ère d'Internet ont tout simplement élargi leur champ de préoccupation pour englober Internet. Bien sûr, une organisation aussi dédiée à Internet telle que ICANN fait partie de la gouvernance spécifique d'Internet et a d'ailleurs été créée à cette fin. Par contre, la plupart des autres organisations déjà mentionnées dans les deux sections précédentes sur la gouvernance, jouent un rôle de premier plan dans la gouvernance des TIC dans leur ensemble. Nous ne ferons dans cette section qu'énumérer brièvement

[67] Consulter les pages Web du WIPO Arbitration and Mediation Center : www.wipo.int/edocs/prdocs/en/2006/wipo_pr_2006_464.html et www.wipo.int/amc/en/domains

celles de niveau international pour ce qui a trait à l'infrastructure et au contenu[68].

Infrastructure et normalisation

- *Union internationale des télécommunications* (UIT);
- *European Telecommunications Standards Institute* (ETSI);
- *EPCGlobal* – organisation regroupant des entreprises visant le développement de normes pour l'Electronic Product Code (EPC) destiné à soutenir l'utilisation du RFID (Radio Frequency Identification) dans les réseaux de commerce électronique[69];
- *Organisation internationale de normalisation (ISO)* – la plus haute instance de normalisation au monde composée de 156 organismes de normalisation nationaux et comprenant près de 3 000 comités et groupes de travail[70]. ISO a publié quelques 15 000 normes dont 1 200 uniquement en 2005 portant sur neuf secteurs dont ceux de la santé, de l'agriculture, et de l'électronique, les technologies de l'information et télécommunications. Ce dernier secteur traite notamment des télécommunications, des techniques audio et vidéo, des technologies de l'information et des technologies de l'image. Certaines de ces normes sont très connues telles que la série de normes ISO 9000 pour l'assurance qualité ainsi que ISO 14000 pour l'environnement. D'autres de ces normes touchent directement la gouvernance d'Internet (telle que la norme ISO 3166 pour les codes de pays) ou l'audiovisuel (telle que les normes MPEG - Représentation codée de l'image et du son);
- L'*Organisation de la Coopération et du Développement Économiques* (OCDE)[71] regroupe 30 pays membres (dont le Canada) et maintient des relations avec plus de 70 autres pays, organisations non gouvernementales (ONG) et la société civile. Ses travaux couvrent tout le champ économique et social. « L'OCDE joue un rôle phare en favorisant la bonne gouvernance des secteurs public et privé. Par son travail sur les questions émergentes et en identifiant les politiques qui ont du succès, elle permet aux décideurs d'adopter des orientations stratégiques. ». L'OCDE aborde de nombreux thèmes dont ceux relatifs à la « gouvernance et gestion publique » et aux « technologies de l'information et communication – TIC ». Sous ce dernier thème, l'OCDE aborde des questions relatives à la cyberfraude, à la protection de la vie privée (et ses directives qui ont servi de guide à l'élaboration des lois sur la protection de la vie privée à travers le monde), à l'accès à haut débit à Internet, aux réseaux de la 3e génération en matière de

[68] Consulter les documents suivants : n° 3 du Cahier 1 *Reframing Internet Governance Discourse* (www.ssrc.org/programs/itic/publications/Drake2.pdf) et n° 14 du Cahier 4 *Guide to International ICT Policy Makers* (www.unicttaskforce.org/perl/documents.pl?id=1312)
[69] Consulter à cet effet le site Web de EPCGlobal : www.epcglobalinc.org
[70] Consulter le site Web d'ISO : www.iso.org/iso/fr/ISOOnline.frontpage
[71] Consulter le site Web de l'OCDE : www.oecd.org

téléphonie mobile, et à la création, la diffusion et l'accès au contenu numérique. L'OCDE ne produit pas de normes comme telles. Elle propose des façons de faire au moyen de « lignes directrices » et réalise des comparaisons entre pays permettant une certaine synergie et émulation entre les pays.

Contenu et services

- L'*Organisation Mondiale de la Propriété Intellectuelle* (OMPI);
- L'*Organisation Mondiale du Commerce* (OMC);
- L'*Organisation de la Coopération et du Développement Économiques* (OCDE);
- L'*Organisation des Nations-Unies pour l'Éducation, la Science et la Culture* (United Nations Educational, Scientific and Cultural Organization - UNESCO);
- *EPCGlobal;*
- L'*Union Internationale des Télécommunications* (ITU);
- La *Coopération économique pour l'Asie-Pacifique* (Asia-Pacific Economic Cooperation - APEC)[72] est composée de 21 États-membres (dont le Canada) représentant environ 40 % de la population mondiale. L'APEC est un forum visant à faciliter la croissance économique, la coopération, le commerce et l'investissement dans la région de l'Asie-Pacifique. L'APEC ne produit aucune norme, directive, ligne directrice ni même traité. Les décisions prises par l'APEC sont atteintes par consensus et leur mise en œuvre s'effectue sur une base volontaire. L'APEC travaille notamment à créer un environnement pour la circulation transfrontière sûre et efficiente des biens, services et personnes par le biais de l'ajustement des politiques et la coopération économique et technique (ECOTECH).

Nous avons dressé un panorama de la gouvernance d'Internet et des TIC qui va nous permettre d'aborder maintenant les deux prochains chapitres portant sur la gouvernance des contenus audiovisuels et les filtres vue par le prisme de la protection de la jeunesse en pouvant se référer à cette gouvernance qui nous est maintenant plus familière.

[72] Consulter le site Web de l'APEC : www.apec.org

5. Gouvernance des contenus sur Internet pour la protection de la jeunesse : état de la situation par pays

La gouvernance des contenus sur Internet est principalement tributaire des valeurs d'un pays et des modes de gouvernance d'Internet déjà mis en oeuvre. Ce chapitre, en visitant un certain nombre de pays choisis en fonction de leur représentativité et de la disponibilité des informations, permettra de dégager les similitudes, les différences et éventuellement certaines tendances de la gouvernance des contenus pour la protection de la jeunesse.

À cette fin, ce chapitre est divisé en trois parties. Une première partie (5.1) présentera la grille d'analyse qui sera utilisée pour présenter la situation des différents pays. On y expliquera en quoi les différentes parties de la définition de la « Gouvernance du contenu sur Internet » peuvent contribuer à influencer le choix des gouvernements et des autres parties prenantes dans la protection de la jeunesse. Une deuxième partie (5.2) présentera, par pays, comment s'articule cette gouvernance selon les différents aspects de la grille d'analyse retenue. En troisième partie (5.3), des conclusions découlant de cette analyse seront dégagées. Le lecteur qui désire aller à l'essentiel peut aller directement à cette 3e partie.

.

5.1 Grille d'analyse

La grille d'analyse retenue se base principalement sur les éléments qui se retrouvent dans la définition de la « Gouvernance du contenu audiovisuel d'Internet ».

Première partie de la définition

La première partie de la définition, rappelons-la, est la suivante :

> « Élaboration et application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet *de façon à protéger la jeunesse.* »

Cette première partie commande les trois analyses suivantes :

- La répartition de la responsabilité de la gouvernance du contenu auprès des différents intervenants : gouvernement, secteur privé et société civile. Cette répartition permettra de vérifier le degré de mobilisation des différentes parties prenantes dans la gouvernance et jusqu'à quel point les organisations apparentées à la Régie du cinéma du Québec interviennent dans la gouvernance du contenu audiovisuel sur Internet;
- Le type de régulation retenu (autorégulation, corégulation et régulation classique)*;*
- Les moyens de régulation retenus : principes, lois, directives, règles, normes, et programmes communs.

Cette première partie de la définition permettra, après analyse, de présenter les trois tableaux récapitulatifs suivants.

Le premier tableau de la grille portera sur la répartition de la responsabilité de la gouvernance du contenu.

La répartition de la responsabilité vise à indiquer quel type d'organisation, dans un pays spécifique, exerce la gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse. Cette répartition comprend quatre possibilités, soit :

- une organisation gouvernementale ayant une mission semblable à celle de la Régie du cinéma du Québec;
- une organisation gouvernementale autre;
- une organisation du secteur privé;
- une organisation de la société civile (essentiellement une ONG – organisation non gouvernementale).

En général, cette responsabilité sera partagée.

Pays	**Responsabilité**			
	Org. semblable à la RCQ	**Org. gouv. autre**	**Org. du secteur privé**	**Org. non gouv. (ONG)**
Pays 1				
Pays 2				
...				
Pays n				

Tableau 5.1 – Tableau de la répartition de la responsabilité de la gouvernance du contenu audiovisuel sur Internet

Le deuxième tableau de la grille d'analyse portera sur le type de régulation :

Pays	**Type de régulation**			
	Autorégulation	**Corégulation**	**Régulation – mode recommandation**	**Régulation – mode prescription**
Pays 1				
Pays 2				
...				
Pays n				

Tableau 5.2 – Tableau du type de régulation par pays pour la gouvernance du contenu audiovisuel sur Internet

Le troisième tableau de la grille portera sur les moyens de régulation utilisés :

Pays	**Moyens de régulation**		
	Principes	**Lois, directives, règles et normes**	**Programmes communs**
Pays 1			
Pays 2			
...			
Pays n			

Tableau 5.3 – Tableau des moyens de régulation par pays pour la gouvernance du contenu audiovisuel sur Internet

Deuxième partie de la définition

La deuxième partie de la définition de la « gouvernance du contenu sur Internet » comprend trois domaines détaillés en « questions relatives à … » que l'on rappelle ici :

1. **Questions relatives à l'infrastructure et à la gestion de ressources Internet critiques**, notamment l'administration du système de noms de domaine et d'adresses numériques Internet (adresses IP), l'administration du système de serveurs racine, les normes techniques, l'homologation et l'interconnexion, l'infrastructure de télécommunications (y compris technologies novatrices et convergentes) et le passage au multilinguisme. Ces questions concernent directement la gouvernance d'Internet et relèvent des organisations existantes qui en sont chargées;
2. **Questions relatives à l'utilisation d'Internet**, notamment le **pollupostage, la sécurité des réseaux et la cyberdélinquance**. Ce domaine apparaissant comme le point central de la protection de la jeunesse, se verra attribuer plusieurs autres éléments à considérer comme la catégorisation, le classement et le filtrage du contenu. Seul l'élément « sécurité » ne sera pas abordé directement.
3. **Questions relatives à la liberté d'expression ainsi qu'à la protection des données et de la vie privée**. Il apparaît important de prendre ce domaine en considération explicitement car il va de

pair, pour cette étude, avec le domaine précédent. Il faut noter que la protection de la vie privée peut toucher, indirectement, à la sécurité, même s'il a été convenu qu'elle ne sera pas prise en compte directement dans le contexte de cette étude.

Si l'on reprend chacun de ces domaines, on peut déterminer les éléments qui feront l'objet d'analyse par pays, soit :

1. **Questions relatives à l'infrastructure et à la gestion de ressources Internet critiques.** Les éléments suivants seront abordés :

   a) **DNS :**
   Actuellement, le DNS peut être utilisé pour le filtrage du contenu tel que les listes de noms de sites Web permettant d'accéder au contenu (« listes vertes ») ou non (« listes rouges »). De plus, les enregistrements du DNS peuvent servir à réaliser une certaine authentification du contenu, notamment concernant l'authentification du courriel, source de pollupostage et de danger pour la jeunesse.
   De plus, la nomenclature des noms de domaine générique de premier niveau (gTLD) pourrait éventuellement contribuer à la protection de la jeunesse. Il faut souligner que cette nomenclature n'étant pas normalisée comme celui pour les codes de pays (ccTLD), il est difficile de prévoir son évolution. Mais déjà, tout récemment, ICANN a failli introduire un domaine de premier niveau pour décrire du contenu pour adulte (soit « .xxx »). Il n'est donc pas exclu que le premier niveau d'un nom de domaine puisse comporter à l'avenir de l'information qui indique le type de contenu du site Web ou même la classe d'âge à laquelle il s'adresse.
   Enfin, avec l'évolution possible du système parallèle d'adressage des objets (« l'Internet des objets » ou le ONS – Object Naming System, basé sur les plaquettes d'identification RFID portant un code de produits), il est possible que le DNS, dans une future mouture, puisse servir à caractériser du contenu à un niveau de granularité permettant de l'appliquer sur des images ou des films, dans leur entièreté ou par séquence ou scène;

   b) **Serveurs racine :**
   C'est une utilisation peu probable, notamment à cause du principe de « neutralité » de l'architecture d'Internet et de la libre circulation de l'information. Cependant, dans le futur, on pourrait éventuellement accepter d'introduire une certaine forme de gouvernance du contenu à leur niveau, par exemple, pour renforcer ou indiquer la présence d'une étiquette du site ou de la page Web (par le biais de la norme RDF ou autre) ou pour contrer le pollupostage. Tout en respectant le concept de neutralité de l'architecture d'Internet, il pourrait y avoir

un renforcement de certaines caractéristiques ou normes techniques du DNS au niveau des serveurs racine;

c) **Normes ou standards :**
Ils servent à décrire le contenu, en faire un classement ou permettre une reconnaissance du contenu de « bout en bout » d'Internet. Ce sont principalement les normes définies par IETF ou W3C;

d) **Multilinguisme :**
Cet élément comprend autant l'internationalisation des noms de domaine (IDN – Internationalized Domain Names) que celle du contenu des sites Web et concerne le recours aux différentes langues pour aider à reconnaître le contenu d'un site Web. Ceci pose des défis particulièrement importants aux logiciels ayant à reconnaître adéquatement la (les) langue(s) du site Web et décider du traitement approprié. Un des moyens possibles pour faciliter cette reconnaissance serait de faire en sorte que le propriétaire d'un site Web indique systématiquement la langue ou les langues supportées par son site. L'approche du Web sémantique pourrait éventuellement être mise à contribution mais déjà, l'initiative d'étiquetage « Dublin Core » permet de véhiculer l'information sur la langue du contenu d'un site Web[73]. L'internationalisation des noms de domaine et de leur contenu continue à représenter un défi pour reconnaître adéquatement leur contenu et encore plus avec les sites multilingues.

2. **Questions relatives à l'utilisation d'Internet.** Les éléments suivants seront abordés :

a) **Création du contenu – catégorisation**
Cette catégorisation correspond à la codification selon le type de contenu;

b) **Création du contenu – classement**
Ce classement correspond à la codification selon l'âge;

c) **Homologation**
L'homologation ou la certification de contenu consistent à s'assurer que le contenu correspond bel et bien à ce qui est décrit ou que le processus de codification du contenu ou de définition de certaines caractéristiques est conforme à des pratiques convenues. L'homologation peut fonctionner en mode d'autorégulation (sans participation gouvernementale), de corégulation (participation mixte gouvernement, secteur privé ou société civile) ou même de régulation (pour donner suite à une exigence ou recommandation gouvernementale);

d) **Contrôle du contenu - filtrage** (de toute nature);

[73] Consulter le site Web de l'initiative d'étiquetage Dublin Core (*Dublin Core Metadata Initiative*) au site Web : http://dublincore.org/documents/dcmi-terms

e) Contrôle du contenu - lutte à la cybercriminalité (ou cyberdélinquance)
Cette lutte inclut notamment la cybersurveillance et le cybersignalement. La cybersurveillance de la cybercriminalité est habituellement exercée par les autorités policières ou représentants de la loi spécialement dédiés à cette fin tant au niveau national qu'international. Le cybersignalement de la cybercriminalité s'effectue, sur une base volontaire, par tout citoyen auprès d'un réseau de « points de contact » qui peut alors faire enquête et prendre des mesures, au besoin.

Voici quelques chiffres permettant de situer le défi[74] :

- Plus de 433 472 sites Web pédocriminels recensés au 31 décembre 2005;
- 20 % des enfants sont sollicités sexuellement sur Internet*;*
- En moyenne, 50 000 pédophiles sévissent sur Internet à tout moment;
- 20 nouveaux enfants apparaissent chaque mois sur des sites de pornographie infantile (selon le FBI).

f) Contrôle du contenu – lutte au pollupostage.
Le pollupostage (ou « spamming ») représente un défi de la gouvernance d'Internet et de la protection de la jeunesse. Voici quelques statistiques :
- les pourriels (« spam ») représentent en moyenne 65 % de tous les courriels, avec des pointes pouvant atteindre jusqu'à 90 % à certaines périodes;
- environ 50 % des internautes ont un jour cliqué sur un pourriel pour en voir le contenu;
- le pollupostage constitue la cause majeure de l'abandon d'Internet par les usagers des pays industrialisés et de sa faible utilisation sur les liaisons à Internet à faible vitesse;
- près de 50 % des pourriels se retrouvent actuellement sous la forme d'images afin de tromper les logiciels de filtrage[75].

g) Utilisation / création du contenu – pédagogie.
Cet élément comprend tout activité ou programme d'activités visant à sensibiliser et former les internautes et particulièrement les enfants et les adultes devant les accompagner lors de l'utilisation d'Internet. Ceci correspond à participer à l'alphanétisation des jeunes, des parents, des éducateurs, et de tout autre adulte concerné, avec le souci de

[74] Consulter le document n° 38.2 du Cahier 4 *Statistiques sur Internet et enfants* (www.innocenceindanger.org)
[75] Consulter le document n° 8 du Cahier 1 *Régulation et gouvernance de l'Internet - Rapport Vox Internet 2005* (www.voxinternet.fr/article.php3?id_article=1&lang=fr)

protection de la jeunesse. Ces activités pédagogiques incluent généralement la lutte contre la discrimination pouvant se retrouver sur du contenu audiovisuel sur Internet, notamment selon les définitions de la Charte des droits de l'Homme (racisme, haine, sexisme, etc.), lutte qui dépasse la seule protection de la jeunesse car elle peut s'étendre à la protection de l'ensemble de la société.

3. **Questions relatives à la liberté d'expression ainsi qu'à la protection des données et de la vie privée.** Les éléments suivants seront abordés :

   a) **Liberté d'expression :**
   Cet élément permet de déterminer le respect de la liberté d'expression. Toute limitation de la liberté d'expression incluse dans des moyens destinés à protéger les mineurs peut être remise en cause et mettre en péril l'existence de ces moyens. Un défi particulier se présente concernant le respect la liberté d'expression des enfants et adolescents par rapport à la responsabilité parentale ou des institutions d'enseignement;

   b) **Protection des données et de la vie privée :**
   Cet élément permet de déterminer le respect de la vie privée. Sachant qu'avec Internet, le consommateur (ou l'enfant) n'est plus passif comme avec les autres moyens de diffusion audiovisuelle, mais qu'il peut aussi produire du contenu audiovisuel, la protection de sa vie privée et du droit à l'image devient importante sur Internet. Un défi particulier se présente concernant la protection de la vie privée de la jeunesse par rapport à ses parents ou ses éducateurs. Il existe peu de débats, de balises, d'orientations claires ou de recommandations sur la question. Étant donné que le jeune est souvent plus alphanétisé que ses parents ou éducateurs, s'il considère que les logiciels de contrôle parental briment sa vie privée, il peut décider de contourner ces contrôles et ainsi quelque peu anéantir l'efficacité de ces logiciels et se mettre à risque de ne pas protéger sa propre vie privée;

   c) **Gestion de l'identité et authentification :**
   La reconnaissance des personnes, de leur âge et de leurs caractéristiques (ou profil), si fournies volontairement, peut les aider à définir le type de contenu qu'elles veulent/peuvent accéder. Ce point est en étroite relation avec la préoccupation de sécurité car c'est souvent par le biais de la sécurité qu'est abordée l'authentification des personnes et leur accès au contenu correspond à leur profil[76]. C'est évidemment un outil qui peut être très utile pour permettre de reconnaître un jeune et les accès possibles aux contenus et aussi pour permettre à ce jeune de distinguer entre un jeune et un adulte,

[76] Un congrès international annuel (Digital ID World) se tient sur l'authentification. Consulter pour plus d'information à jour le site de ce congrès de septembre 2006 : http://conference.digitalidworld.com/2006/index.html

éventuellement. Le risque de leurre d'un enfant par un prédateur sur les sites permettant une interaction (comme le clavardage ou les blogues) existe et l'authentification peut éventuellement aider les jeunes à s'en prémunir. Évidemment, l'authentification se heurte au défi de protection de la vie privée et à la liberté d'expression car elle enlève beaucoup le caractère d'anonymat. Cet anonymat sert les prédateurs sexuels mais sert aussi de facteur facilitant la socialisation des jeunes car ces derniers, grâce à l'anonymat, explorent des rôles en se « fabriquant » de nouvelles personnalités ou traits de caractère.

Cette deuxième partie de la définition pourra être représentée sous forme du tableau type suivant représentant le domaine 1 portant sur l'infrastructure et la gestion de ressources Internet critiques :

Pays	**1. Questions relatives à l'infrastructure et à la gestion de ressources Internet critiques**			
	a. DNS	**b. Serveurs racine**	**c. Normes ou standards**	**d. Multilinguisme**
Pays 1				
Pays 2				
...				
Pays n				

Tableau 5.4 – Tableau des éléments d'infrastructure utilisés dans la gouvernance du contenu audiovisuel sur Internet

5.2 Analyse de la gouvernance par pays

Cette section présente l'analyse de la gouvernance du contenu audiovisuel sur Internet de différents pays. Chaque pays sera analysé séparément et par la suite des tableaux récapitulatifs pour l'ensemble des pays seront présentés. Il est à noter que l'Europe sera considérée comme un pays étant donné ses actions communes dans la gouvernance du contenu d'Internet. D'ailleurs, récemment, l'Europe s'est vu attribuer un code de pays comme premier niveau de nom de domaine, soit « .eu » à titre de ccTLD. Les pays et provinces retenus à des fins d'analyse comparative sont les suivants :

- Australie;
- Canada;
- Canada – Québec;
- Canada – Ontario;
- Canada – Nouveau-Brunswick;
- Canada – Colombie britannique;
- Europe;
- Allemagne;
- Belgique;
- Danemark;
- France;
- Espagne;
- Royaume-Uni;
- États-Unis d'Amérique.

Ces pays et provinces ont été retenus principalement sur la base de la disponibilité de l'information, sur la proximité géographique des pays ou provinces par rapport au Québec, sur la similitude de gestion des technologies de l'information et des communications (TIC) avec le Québec ainsi que sur la couverture géographique des principales régions du monde. Il faut souligner l'absence de pays de l'Asie (tels que le Japon ou la Corée du Sud) ou de l'Amérique du Sud (tel que le Brésil) qui peuvent présenter des similitudes avec le Québec. Cependant, la disponibilité d'information, les différences de langue et l'étendue de cette étude ne nous ont pas permis de les prendre en compte. Sans pour autant préjuger des innovations possibles de gouvernance dans ces régions du monde, il est permis de croire que les pays et provinces retenus fournissent un aperçu représentatif

des pratiques mondiales actuelles en matière de gouvernance du contenu audiovisuel sur Internet.

5.2.1 Australie

Responsabilité et types de régulation

La gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse s'effectue principalement, en Australie, par la corégulation et la régulation.

L'Office de classification des films et de la littérature (Office of Film and Literature Classification – OFLC - (www.oflc.gov.au/special.html)[77] gère le système de classification national, notamment par l'intermédiaire de son « Bureau de classification » (Classification Board - www.oflc.gov.au/special.html?n=250&p=58), en collaboration avec les États et les territoires, conformément à une loi[78]. Son champ d'application porte sur les films, incluant les vidéos et les DVD, les jeux par ordinateurs et certaines publications. L'obtention d'une classification est obligatoire pour une diffusion en public. Le Bureau de classification fournit le même système de classification à utiliser pour le contenu sur Internet. C'est l'organisme gouvernemental australien ACMA qui prend en charge cette classification par un mode de corégulation : le gouvernement australien fournit le système de classification et l'industrie Internet d'Australie applique ce système, sur une base volontaire.

L'organisme de la régulation des médias et des communications de l'Australie (**Australian Communications and Media Authority - ACMA - www.acma.gov.au**)[79] est responsable de la régulation de la télévision, des radiocommunications, des télécommunications et du contenu sur Internet. Il relève du ministre des Technologies de l'information, des Communications et des Arts (Minister for Communications Information Technology and the Arts).

Ses responsabilités incluent :

- La promotion de l'autorégulation et de la compétition dans l'industrie des télécommunications, tout en protégeant les consommateurs;
- La facilitation d'un environnement où les médias électroniques respectent les standards de la communauté et satisfont les besoins de la clientèle.

[77] Le site de Wikipedia offre une information intéressante sur cet organisme : http://en.wikipedia.org/wiki/Office_of_Film_and_Literature_Classification_(Australia)
[78] Selon la Loi de la classification (Classification Act) - Classification (Publications, Films and Computer Games) Act 1995
[79] Cet organisme, constitué en juillet 2005, est le résultat d'une fusion de deux organismes, soit le Australian Communications Authority (ACA) et le Australian Broadcasting Authority (ABA).

Pour ce qui est d'Internet, l'ACMA administre un cadre de gouvernance du contenu sur Internet en corégulation[80], renforce la loi antipourriels de l'Australie et peut établir des règles concernant l'accès à Internet par le biais des services tarifés de téléphonie mobile. Ces services peuvent inclure, par exemple, les services de clavardage et de rencontres ou les sites Web comportant du contenu pour adultes.

Ce cadre de gouvernance est conçu pour répondre aux préoccupations de la communauté relatives au matériel offensant et illégal et, particulièrement, à des fins de protection des enfants. À cette fin, l'ACMA remplit les rôles suivants :

- Enquête sur les plaintes relatives au contenu sur Internet et sur les services de pari sur Internet;
- Incitation au développement de codes de pratiques pour l'industrie d'Internet et suivi du respect de ces codes;
- Guide et information à la communauté sur les défis de sûreté sur Internet, particulièrement ceux relatifs à l'utilisation d'Internet par les enfants;
- Recherche sur les questions relatives à l'utilisation d'Internet et dissémination de l'information sur les tendances;
- Liaison avec les organismes internationaux pertinents.

À cet effet, trois codes de pratiques relatifs au contenu sur Internet (incluant la téléphonie mobile) ont été élaborés en 2005[81], conformément à la loi, et sont présentement en application : un code destiné aux hébergeurs de contenu de sites Web (Code 3) et deux codes destinés aux fournisseurs de services Internet (FSI) (Code 1 et 2). L'ACMA peut contraindre les FSI et les hébergeurs à se conformer au code et des offenses sont possibles selon la loi. Le Code de pratiques relatif à la téléphonie mobile (Code 2) empêche l'accès général à du contenu pour adulte et exige une preuve d'âge de 18 ans et plus pour y avoir accès. Le Code de pratiques destiné aux hébergeurs inclut, dans le cas de contenu Internet pour adultes hébergé à l'extérieur de l'Australie, une disposition permettant d'exiger au besoin une modification des logiciels de filtrage par ses fournisseurs. Rappelons que chaque FSI doit rendre disponible[82] un logiciel de filtrage à chaque client.

---

[80] Ce cadre de gouvernance du contenu sur Internet est établi selon la « Schedule 5 » de la Loi *Broadcasting Services Act 1999* afin de, notamment, contrôler le matériel illégal ou hautement offensant publié sur des services en ligne tels que Internet.

[81] Consulter le document n° 42.2 du Cahier 4 *Internet Industry Codes of Practice* (www.iia.net.au/files/IIA/Codes%20of%20Practice/Content%20Code/ContentCodes10_4.pdf)

[82] Ce logiciel de filtrage peut résider sur le portail du FSI ou de l'Association des FSI (Internet Industry Association – IIA - www.iia.net.au) ou sur l'ordinateur du client.

1.a DNS

DNS est utilisé pour des fins de filtrage.

1.b Serveurs racine

Non utilisés pour la gouvernance du contenu.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

L'Australie a recours au multilinguisme pour ce qui est du contenu afin de soutenir plusieurs langues, de par sa proximité avec l'Asie.

2.a Création du contenu – catégorisation

L'Australie catégorise le contenu sur Internet, sur une base volontaire, selon le système de classification en usage pour les films et les jeux par ordinateur.

2.b Création du contenu – classement

L'Australie attribue un classement aux pages ou sites Web, sur une base volontaire, selon le système de classification en usage pour les films et les jeux par ordinateur.

2.c Contrôle du contenu – homologation

L'Australie n'a pas, à notre connaissance, d'initiative d'homologation du contenu permettant de contribuer à la protection de la jeunesse sur Internet.

Cependant, un sceau, le « Ladybird Seal », a été mis en place pour reconnaître les FSI qui respectent le(s) code(s) de pratiques d'Internet de l'Australie. Ce sceau va dans le sens des résultats de recherche internationale sur l'importance, dans le contexte de l'autorégulation ou la corégulation d'Internet, de l'accréditation ou l'homologation[83].

2.d Contrôle du contenu – filtrage

L'Australie oblige les FSI à offrir à leurs clients l'accès à un logiciel de filtrage, selon des modalités (prix et mode de services) que les FSI sont libres de déterminer.

Récemment, le ministère des Communications, des Technologies de l'information et des Arts du gouvernement de l'Australie a décidé de déployer un Plan national de filtrage de l'ordre de 116 M $ AU[84] afin de rendre disponible à toute famille australienne un accès à un service de filtrage gratuit sur Internet. La justification de ce choix peut se résumer ainsi :

> "You wouldn't send your child out to ride their bike without a helmet, or let them travel in a car without a seatbelt, so why would we let them surf the Internet without the protection of an effective filter? "

Ce plan intègre de la sensibilisation et de la formation destinées aux parents.

2.e Contrôle du contenu – lutte à la cybercriminalité

L'Australie, par l'ACMA, fait partie du réseau international de « Hotlines » anglophone Virtual Task Force dédié à la lutte contre l'abus d'enfants ainsi que du réseau européen INHOPE (www.inhope.org)[85].

---

[83] Consulter le document n° 8 du Cahier 5*Self-regulation of digital media converging on the Internet* (http://pcmlp.socleg.ox.ac.uk/text/execsummary.pdf)

[84] Consulter le document n° 42.4 du Cahier 4 *Plan national de filtrage* (www.govtech.net/magazine/story.print.php?id=99998)

[85] Consulter le site Web de l'ACMA : www.acma.gov.au/ACMAINTER.1966346:STANDARD::pc=PC_90166

2.f Lutte au pollupostage

L'Australie a déjà légiféré dans ce domaine par le *Spam Act 2003*[86] visant à bannir l'envoi de messages électroniques non sollicités, incluant le courriel et les messages sur les mobiles (SMS – Small Message Service) ainsi que la collecte des adresses de courriel (« farming »). Récemment, l'association de l'industrie Internet (Internet Industry Association – IIA - www.iia.net.au) a développé, en collaboration avec d'autres associations Internet, un code de pratiques gouvernant les pratiques des FSI et des fournisseurs de services de courriels destinées à combattre le pollupostage. Le code s'applique autant aux fournisseurs australiens que ceux qui fournissent de tels services en Australie. L'ACMA a enregistré ce code de pratiques pour l'ajouter aux autres codes pratiques sur lesquels il exerce une surveillance[87].

De plus, le gouvernement de l'Australie, par le biais de l'ACMA, a mis en oeuvre d'autres mesures tant nationales qu'internationales pour combattre le pollupostage. Ainsi, au niveau national, l'ACMA offre des facilités pour cybersignaler les pourriels, soit auprès de son site Web directement ou à partir du logiciel de courriel des internautes[88]. Au niveau international, consciente que le pollupostage est un phénomène qui dépasse largement ses frontières, l'Australie a établi plusieurs accords multilatéraux (dont un accord avec les pays de l'Asie du Sud-Est) afin de réaliser une lutte conjointe[89].

2.g Pédagogie

Il existe plusieurs initiatives gouvernementales ou de la société civile pour augmenter l'alphanétisation des jeunes, de leurs parents et de leurs enseignants et pour les rendre sensibles aux risques reliés à l'utilisation d'Internet et aux façons d'y faire face.

---

[86] Consulter le site Web de l'ACMA : www.acma.gov.au/ACMAINTER.1900810:STANDARD::pc=PC_2008 ou le document n° 42.3 du Cahier 4 *Internet Industry Spam Code Of Practice* (www.acma.gov.au/acmainterwr/_assets/main/lib100234/iia_spam_code_dec_2005.pdf)

[87] Il est en vigueur depuis le 16 juillet 2006.

[88] L'ACMA fournit un module à télécharger et insérer dans le logiciel de courriel, permettant ainsi à l'internaute par la suite de détruire le pourriel reçu et de le cybersignaler à l'ACMA. Le site Web concernant le cybersignalement des pourriels est : (http://www.acma.gov.au/ACMAINTER:STANDARD::pc=PC_2008)
Consulter le document n° 68 du Cahier 4 *Lutte au SPAM – ACMA* (www.acma.gov.au/ACMAINTER.1507598:STANDARD::pc=PC_2008)

[89] Consulter le document n° 68 précédent ou la page Web de l'ACMA sur la coopération internationale en cette matière : www.acma.gov.au/ACMAINTER.1507598:STANDARD::pc=PC_2935

Ainsi, le gouvernement de l'Australie a mis sur pied une agence sans but lucratif sur la sûreté en ligne, soit Net Alert **(**www.netalert.net.au/02246-About-NetAlert.asp), comme partie intégrale de sa stratégie de corégulation du contenu d'Internet. NetAlert est financé par le gouvernement de l'Australie et hébergé par l'ACMA (Australian Communications and Media Authority). NetAlert a pour mission de fournir :

- des avis indépendants;
- de la formation sur la sûreté sur Internet et sur la gestion de l'accès au contenu sur Internet, particulièrement auprès des mineurs et leurs familles, en insistant sur les défis, les risques et les dangers associés à l'usage d'Internet et sur la façon de minimiser les risques, d'éviter les problèmes et utiliser Internet de façon sûre et responsable.

Un autre site gouvernemental, soit Cyber Smart Kids (www.cybersmartkids.com.au), est développé et soutenu par l'ACMA. Il est destiné aux enfants et à leurs parents pour les guider dans la navigation sur Internet, le clavardage et le courriel.

Plusieurs autres sites de la société civile et du gouvernement sont disponibles concernant la sensibilisation et la formation. L'association IIA a produit un guide à l'intention des utilisateurs d'Internet[90] qui fournit en référence plusieurs sites Web ou organismes dédiés à l'alphanétisation.

3.a Liberté d'expression

L'Australie est tenue par la loi au respect de la liberté d'expression.

3.b Protection des données et de la vie privée

L'Australie est tenue par la loi au respect de la vie privée.

3.c Gestion de l'identité et authentification

[90] Consulter le document n° 42.5 du Cahier 4 *Guide for Internet Users* (www.iia.net.au/index.php?option=com_content&task=view&id=416&Itemid=9)

L'Australie n'offre pas de service de gestion de l'identité et de l'authentification destiné aux jeunes, sauf par le biais du nouveau service d'une firme privée du Royaume-Uni (NetId) offert en Australie. L'expérience passée à cet égard[91] qui a entraîné, à la fin des années 1980, la chute du gouvernement d'alors, a rendu depuis le gouvernement extrêmement prudent sur tout projet dans ce sens.

---

[91] Consulter le document n° 60.4 du Cahier 4 *Arguments contre un système d'identification national* (http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61882&als[theme]=National%20ID%20Cards&headline=On%20Campaigns%20of%20Opposition%20to%20ID%20Card%20Schemes)

5.2.2 Canada

Le système fédéral canadien répartit la responsabilité de la gouvernance du contenu audiovisuel pour la protection de la jeunesse entre les instances fédérales et celles des provinces ou territoires. La gouvernance réalisée par le gouvernement fédéral s'applique à l'ensemble des provinces et territoires qui à leur tour, peuvent particulariser et compléter la gouvernance du contenu selon leurs compétences respectives. C'est ainsi de la responsabilité de chaque province ou territoire de classifier le contenu audiovisuel diffusé. Cependant, pour ce qui est des vidéos de films, il existe un système canadien de classement (SCCCV - www.cmpda.ca/jsp/v-rating.jsp) qui est géré par l'Association canadienne des distributeurs de films (Canadian Motion Picture Distributors Association – CMPDA - www.cmpda.ca/jsp/video.jsp). Le classement correspond à une moyenne des classements de six des organismes provinciaux. Ce classement n'a pas force de loi et c'est toujours celui d'une province qui prévaut.

Nous verrons donc dans un premier temps cette gouvernance au niveau fédéral canadien et par la suite, nous l'examinerons dans quatre provinces, soit la Colombie britannique, le Nouveau-Brunswick, l'Ontario et le Québec, pour souligner les particularités spécifiques.

Responsabilité et types de régulation

La gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse s'effectue, au Canada, par la régulation, mode directive, pour ce qui est du contenu illégal sur Internet à l'autorégulation ou même à l'absence de régulation pour tout autre contenu sur Internet. Cependant, la participation active des instances gouvernementales fédérales dans l'alphanétisation et son financement permet de souligner une certaine forme de corégulation.

Moyens de régulation

Quelques principes importants orientent la régulation du contenu sur Internet dont les trois suivants :

- le principe de l'autorégulation en matière de contenu sur Internet est mis de l'avant[92] dans la « Stratégie canadienne pour l'utilisation sécuritaire, prudente et responsable d'Internet ». Donc, le principe de la non-intervention de l'état dans la régulation d'Internet est privilégié afin de permettre, notamment, à l'industrie d'Internet de croître;
- le principe de la primauté de la liberté d'expression. Ainsi, malgré le tragique attentat dans un collège de Montréal en 2006 qui a causé morts et blessures et qui avait fait l'objet d'annonce à peine voilée par l'auteur de l'attentat sur un site Web, n'a pas fait changer ce principe[93];
- le principe de non-tolérance de contenu illégal sur Internet et particulièrement concernant la pornographie infantile.

1.a DNS

Les logiciels de filtrage sont reconnus et utilisés et, dans ce sens, le Canada a recours au DNS pour la gouvernance du contenu.

1.b Serveurs racine

Non-utilisation des serveurs racine pour la gouvernance du contenu.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

De par le caractère officiel du bilinguisme, le Canada a recours au multilinguisme pour ce qui est du contenu mais ne supporte pas présentement l'internationalisation des noms de domaine. L'Autorité

[92] Consulter le document n° 43.1 du Cahier 4 *Gouv. Fédéral - contenu illégal et offensant* (http://cyberwise.ca/epic/internet/incyby-cybj.nsf/fr/h_uz00054f.html)

[93] En effet, « Le Premier ministre canadien Stephen Harper s'est dit scandalisé par la violence parfois véhiculée sur internet, mais, a-t-il ajouté, "nous aurons du mal à concilier ce sentiment avec notre attachement à la liberté et à notre désir d'éviter la censure". » Consulter le document n° 43.3 du Cahier 4 *Événement de Dawson et contrôle d'Internet* (www.rcinet.ca/rci/fr/news/2006/09/20060914.shtml)

canadienne pour les enregistrements Internet (ACEI – www.ACEI.ca) travaille cependant sur un projet visant à l'offrir au Canada.

2.a Création du contenu – catégorisation

Aucune initiative de catégorisation n'a été détectée. C'est davantage du ressort des provinces et territoires, sauf en ce qui a trait au contenu Internet accessible en mode télécommunication (comme avec les mobiles) qui est du ressort fédéral.

2.b Création du contenu – classement

Aucune initiative de classement n'a été détectée. C'est davantage du ressort des provinces et territoires, sauf en ce qui a trait au contenu Internet accessible en mode télécommunication (comme avec les mobiles) qui est du ressort fédéral

2.c Contrôle du contenu – Homologation

Aucune initiative d'homologation n'a été détectée.

2.d Contrôle du contenu – filtrage

Dans la « Stratégie canadienne pour l'utilisation d'Internet », il est mentionné que les solutions de filtrage du contenu peuvent constituer un outil pour la protection de la jeunesse. Mais aucune action ou initiative additionnelle n'a été trouvée. Les fournisseurs de services Internet, incluant ceux de la téléphonie mobile, sont libres d'offrir ou non de tels services de filtrage. Généralement, les fournisseurs de services Internet offrent une solution de filtrage selon une tarification additionnelle alors que ceux de la téléphonie mobile avec accès à Internet n'en offrent aucune.

2.e Contrôle du contenu – lutte à la cybercriminalité

Le gouvernement du Canada est extrêmement actif dans la lutte à la cybercriminalité par le biais de la cybersurveillance et du cybersignalement,

particulièrement en ce qui a trait à la pornographie infantile. Il songe à mettre sur pied un nouveau « Cyber-Security Task Force »[94].

Il finance le service pancanadien de signalement d'enfants exploités sexuellement sur Internet, soit **Cyberaide.ca** - www.cybertip.ca/fr/cybertip. Cyberaide.ca fait partie du réseau européen de cybersurveillance et de cybersignalement INHOPE du programme « Safer Internet » et du réseau international anglophone de cybersignalement Virtual Task Force[95]. Cyberaide.ca est aussi un centre d'information, d'aiguillage et de ressources pour la sécurité des enfants sur Internet.

Industrie Canada a mis sur pied et soutient le service **CyberAverti.ca** (www.cyberAverti.ca) qui fournit des renseignements aux parents, aux enseignants, aux intervenants jeunesse et aux jeunes en vue de contribuer à protéger les enfants contre l'exploitation sexuelle sur Internet. Ce site a été créé dans le cadre de la « Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet ».

Le Centre national de coordination contre l'exploitation des enfants (CNCEE - http://ncecc.ca) de la Gendarmerie royale du Canada (GRC) offre un site Web - www.securitecanada.ca, qui fait office de sensibilisation et d'éducation concernant la sécurité sur Internet (comme la cyberintimidation et le hameçonnage) et particulièrement la sécurité des enfants. Ce site renvoie plusieurs services au site de Web Averti (voir plus loin) .

De plus, sur l'initiative d'un détective du Service de police de Toronto (SPT), le CNCEE, en collaboration avec Microsoft qui a investi plusieurs millions de dollars, et plusieurs autres organismes, a développé un logiciel spécialisé destiné à combattre la pornographie infantile CETS (Child Exploitation Tracking System)[96].

Enfin, le CNCEE collabore avec le réseau scolaire RESCOL (www.rescol.ca - ou School Net en anglais), partenariat entre le gouvernement fédéral, les gouvernements provinciaux et territoriaux, la

---

[94] Consulter les documents suivants :
- n° 20 du Cahier 2 *The Legal Limits of Government Tinkering With Technology* (http://michaelgeist.ca/index.php?option=com_content&task=view&id=1212&Itemid=85)
- n° 25 du Cahier 3 *Cyber-Security Plans* (www.michaelgeist.ca/content/view/1269/159)
- n° 25.3 du Cahier 3 *Groupe de travail sur la cybersécurité* (http://direct.srv.gc.ca/cgi-bin/direct500/RFou=CSTFS-GTCS)

[95] Consulter le site Web www.virtualglobaltaskforce.com

[96] Consulter le document n° 43.5 du Cahier 4 *Logiciel CETS* (http://ncecc.ca/cets_f.htm)

communauté enseignante et le secteur privé. RESCOL, par le biais de différentes activités de recherche, d'apprentissage et autres, participe à la promotion de l'utilisation sécuritaire d'Internet auprès des enfants, des jeunes, des parents, des enseignants et des intervenants jeunesse.

RESCOL, de même que les autres initiatives en matière de lutte contre la cybercriminalité, participe à l'effort d'alphanétisation et de sensibilisation à l'utilisation d'Internet.

2.f Lutte au pollupostage

Le gouvernement du Canada, par le biais d'Industrie Canada, a investi de façon importante pour faire le point sur le sujet, établir une stratégie nationale et mettre en oeuvre des mesures nationales de lutte contre le pollupostage.

Ainsi, Industrie Canada a mis sur pied un Groupe de travail sur le pourriel (http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00170f.html). Le rapport du groupe de travail produit en 2005 inclut une analyse exhaustive du pollupostage, réalisée avec la collaboration d'un nombre impressionnant d'organisations tant nationales qu'internationales, et souligne, notamment, la possibilité de certification de courriels (par le biais de « listes blanches » ou de techniques de reconnaissance de pourriels) au moyen de certains logiciels du marché[97]. Le site Web qui en a résulté offre de l'aide pour se protéger des menaces venant d'Internet. Le site inclut une série de statistiques, de conseils et de ressources sur **le pourriel**, **les logiciels espions**, **le hameçonnage** et le **vol d'identité**. (http://arretezlepourrielici.ca/index.html).

D'autres organisations offrent des sites Web où le pollupostage est traité :

- CIPPIC - La Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC - www.cippic.ca/fr) de la Faculté de droit de l'Université d'Ottawa. cherche à assurer un équilibre entre la politique et la procédure de prise de décision relativement aux questions que soulèvent les nouvelles technologies. Elle présente plusieurs dossiers, généralement en anglais, fort bien documentés sur des sujets tels que le pollupostage, les logiciels espions, les cartes d'identité nationale et la protection de la vie privée. Elle est très

[97] Consulter la page Web sur l'évaluation de la certification du courriel (http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00312f.html) ou le document n° 43.7 *Freinons le courriel* (http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/freinons_le_pourriel_mai2005.pdf/$file/freinons_le_pourriel_mai2005.pdf)

active à intenter des poursuites ou soutenir des poursuites visant à protéger la vie privée et le droit des consommateurs sur Internet et ce, selon les lois canadiennes ou de chacune des provinces et territoires;

- GRC - Le site de la Gendarmerie royale du Canada propose différentes informations sur les escroqueries sur Internet. - www.rcmp-grc.gc.ca/scams/spam_f.htm;
- Pourriel.ca – site entièrement consacré au sujet - www.pourriel.ca;
- CAUCE Canada (Coalition Against Unsolicited Commercial Email) : une association bénévole qui milite en faveur d'une réglementation antipourriel. - www.cauce.ca .

2.g Pédagogie

On retrouve au niveau de l'alphanétisation, les mêmes organismes précédents oeuvrant pour la lutte à la cybercriminalité, y incluant le réseau RESCOL.

De plus, le gouvernement fédéral finance le **Réseau Web Averti** (www.webaverti.ca/french/default.aspx) pour concrétiser son programme national d'information publique sur la sécurité de la navigation sur Internet. Par ce réseau, le gouvernement vise à s'assurer que les jeunes Canadiens puissent tirer parti des ressources offertes sur Internet, mais en toute sécurité et en agissant de façon responsable dans le cyberespace[98]. L'initiative *WebAverti* comporte deux objectifs :

- Informer les parents des dangers du cyberespace pour leurs enfants et de la nécessité de prendre certaines mesures à cet égard;
- Fournir aux parents des informations et des outils pratiques, afin qu'ils puissent bien gérer l'utilisation d'Internet à la maison et apprendre à leurs enfants à être des internautes avertis.

Le Réseau Web Averti a été créé principalement par trois partenaires, soit Réseau Éducation Médias, Microsoft et Bell Canada, ainsi que plusieurs autres provenant tant du gouvernement (tels que le Solliciteur général de l'Alberta et le Service de police de Toronto), du secteur privé (tels que Alliance Atlantis et Telus), que de la société civile (tels que Club Kinsmen et Globe and Mail). Le site Web a ceci de particulier qu'il adapte ses conseils selon cinq catégories d'âge des jeunes (2 à 4, 5 à 7, 8 à 10, 11 à 13 et 14 à 17) afin de tenir compte du développement de l'enfant.

[98] Consulter le document n° 43.2 du Cahier 4 *Web Averti* (www.webaverti.ca/french/aboutus.aspx)

Un partenaire majeur dans l'alphanétisation et la formation aux périls d'Internet constitue le **Réseau Éducation-Médias** (le Réseau) (www.media-awareness.ca/francais/organisation/qui_sommes_nous/index.cfm), qui offre une des plus complètes collections de ressources en éducation aux médias et à Internet. Son site est destiné principalement aux enseignants et aux parents tout en comportant plusieurs jeux éducatifs destinés aux jeunes de 8 à 13 ans reliés notamment aux menaces, à l'intimidation, aux préjugés, stéréotypes et à la protection de leurs informations personnelles. Le travail du Réseau part de l'idée que les jeunes, pour fonctionner adéquatement dans le monde actuel, doivent être en mesure de se livrer à une « lecture critique » de l'avalanche quotidienne de messages qui visent à les informer, les divertir ou leur vendre des produits.

Le Réseau a développé trois programmes de base, offerts sur son site, soit :

- **Éducation aux médias** avec plus de 300 activités pédagogiques proposées. Il comprend de plus une section sur les enjeux des médias : stéréotypes, violence, vie privée, publicité visant les jeunes, reflet de la diversité canadienne et propos haineux sur Internet;
- **La Toile et les jeunes**, rendant disponibles, notamment, des ateliers de perfectionnement professionnel à l'usage d'Internet pour les enseignants, bibliothécaires et parents. Il couvre notamment les sujets suivants : sécurité en ligne, protection de la vie privée, authentification de l'information et marketing visant les jeunes. Il intègre de plus des ressources en alphanétisation conçues spécifiquement pour les jeunes. Le gouvernement du Canada a fait de *La Toile et les jeunes* le pilier de sa stratégie Cyberaverti d'éducation publique à Internet. Les ateliers offerts comprennent :
  - *Naviguer en toute sécurité* : former des jeunes internautes prudents et responsables;
  - *Jeunes à vendre* : marketing en ligne et protection de la vie privée;
  - *Fait ou fiction* : authentifier l'information en ligne;
  - *Cyberintimidation* : importance des comportements éthiques sur Internet.
- **Jeunes canadiens dans un monde branché** : le Réseau a lancé en 2001 une étude sur les usages et le comportement des jeunes, âgés de 9 à 17 ans, anglophones et francophones, sur Internet. 6000 jeunes ont été sondés en tout[99]. Le résultat de cette étude apparaît dans un rapport publié en 2005[100].

---

[99] Consulter le document n° 39 du Cahier 4 *Protection de l'enfant et usages de l'Internet* (www.sante.gouv.fr/htm/actu/conf_famille2005/rapport_protection.pdf)

[100] Consulter le document n° 43.8 du Cahier 4 *Étude Jeunes canadiens dans un monde branché* (www.media-awareness.ca/francais/recherche/JCMB/phaseII/upload/JCMBII_tendances_rec.pdf)

Réseau Éducation-Médias est membre du réseau européen INSAFE[101].

3.a Liberté d'expression

La liberté d'expression constitue un des principes de la régulation (ou de la non-régulation) du contenu sur Internet et est soutenue par la Charte canadienne des droits et libertés.

3.b Protection des données et de la vie privée

La protection de la vie privée est aussi soutenue par la Charte canadienne des droits et libertés. D'ailleurs, une étude publiée en novembre 2006 permettait de classer le Canada et l'Allemagne comme les meilleurs défenseurs de la vie privée[102].

3.c Gestion de l'identité et authentification

Aucune initiative spécifique d'authentification destinée à protéger la jeunesse n'a été trouvée, sauf le fait que l'offre récente de la firme du Royaume-Uni NetID[103] est disponible au Canada.

---

[101] Consulter le document n° 1 du Cahier 3 *Insafe – Europe et monde* (www.saferinternet.org/ww/en/pub/insafe/focus.htm)

[102] Consulter la page Web du journal Globe and Mail : (www.theglobeandmail.com/servlet/Page/document/v4/sub/MarketingPage?user_URL=http://www.theglobeandmail.com%2Fservlet%2Fstory%2FRTGAM.20061101.wpriv1101%2FBNStory%2FNational%2F%3Fpage%3Drss%26id%3DRTGAM.20061101.wpriv1101&ord=1163442966379&brand=theglobeandmail&force_login=true)

[103] Pour plus de détails sur cette offre, consulter la gouvernance du Royaume-Uni qui est traitée plus loin.

5.2.3 Canada – Québec

Responsabilité et types de régulation

La gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse se réclame, au Québec, du même type de régulation que pour le Canada, le Québec n'ajoutant peu ou prou à cette gouvernance canadienne. Ainsi, la politique québécoise de l'autoroute de l'information ne comprend aucune disposition pour la protection de la jeunesse reliée au contenu audiovisuel[104] et les orientations gouvernementales en matière d'agression sexuelle ne comportent aucune référence à Internet[105].

De son côté, l'organisme responsable du classement québécois des films, des vidéos et des DVD conformément à *Loi sur le cinéma*[106], soit la Régie du cinéma du Québec (www.rcq.qc.ca)[107], n'a aucune compétence concernant le contenu audiovisuel sur Internet. Cependant, elle s'interroge sur le maintien de l'absence de régulation sur ce contenu et c'est pourquoi elle a commandé cette étude.

Il est intéressant de noter la participation du Québec à l'étude européenne universitaire Mediappro (pour Media Appropriation) portant sur l'appropriation des médias par les jeunes. Le Québec a été la seule entité nationale non européenne à y avoir participé, par le biais des chercheurs de l'Université de Montréal et de l'Université de Sherbrooke. L'étude s'est réalisée de septembre 2005 à mai 2006 auprès d'une clientèle d'environ 9000 jeunes de 12 à 18 ans[108] dont 1300 au Québec. L'hypothèse de l'étude est la suivante : la sûreté des enfants sur Internet dépend de leurs propres actions. Les risques dépendent majoritairement de leurs comportements, leurs attitudes et perceptions. D'où l'importance de les rendre compétents et habiles dans l'utilisation d'Internet. Il est donc important d'augmenter leur responsabilité, leur autonomie et leur conscientisation.

Voici quelques résultats de l'étude spécifiques ou appropriés pour le Québec :

---

104 Consulter le document n° 46.1 du Cahier 4 *La politique québécoise de l'autoroute de l'information* (www.services.gouv.qc.ca/fr/publications/enligne/societe/politique_autoroute.pdf)

105 Consulter le document n° 46.5 du Cahier 4 *Orientations gouv. en matière d'agression sexuelle – 2001* (www.mfacf.gouv.qc.ca/publications/pdf/CF_orientations_agression_sexuelle.pdf)

106 Selon la loi de la classification (Classification Act) - *Classification (Publications, Films and Computer Games) Act 1995*

107 Pour plus de détails sur la loi, consulter la page Web de la Régie du cinéma : www.rcq.qc.ca/la_regie/loi.asp

108 Cette étude a été réalisée dans 9 pays (7400 jeunes) et le Québec (1350 jeunes). La collecte de données s'est effectuée par questionnaire et a été complétée par une entrevue auprès de 240 jeunes, soit 24 jeunes par pays ou nation.

- L'enseignement explicite d'Internet dans les écoles apparaît être sérieusement sous-développé : 82 % en Europe et 90 % au Québec : « Schools fail to teach the skills of information retrieval, search, site evaluation and creative production » (p. 16 du Rapport);
- Lieu d'utilisation d'Internet (Europe) : 67 % à la maison et 26 % à l'école;
- L'utilisation d'Internet dans les institutions d'enseignements semble au point mort ou même avoir régressé de 2000 à 2006;
- 90 % des jeunes indiquent qu'ils ne parlent à peu près jamais d'Internet avec leurs enseignants;
- 90 % des jeunes au Québec indiquent que leurs parents ne leur imposent aucune règle d'utilisation d'Internet;
- 80 % des jeunes déclarent que le contenu d'Internet devrait être régulé, particulièrement le contenu des sites reconnus dangereux en termes de pornographie, de haine ou de racisme;
- Nouveau danger : cyberexclusion ou fracture numérique (due à la difficulté d'accès à Internet à large bande à prix abordable et au problème d'alphanétisation);
- Autorégulation des enfants p/r à la sécurité sur Internet, particulièrement en France, principalement grâce au programme massif de sensibilisation et d'éducation sur les périls et les moyens d'y faire face : « Young people report being in dangerous, or even uncomfortable, situations extremely rarely » (p. 16).

Le rapport d'étude comprend plusieurs recommandations destinées aux parents, aux écoles et enseignants, aux gouvernements et politiciens ainsi qu'aux chercheurs universitaires.

2.e Contrôle du contenu – lutte à la cybercriminalité

Une activité spécifique sur le territoire du Québec en matière de lutte à la cybercriminalité est réalisée par le **Module de la cybersurveillance et de la vigie (MCV)** de la **Sûreté du Québec**. Ce module a pour mandat d'analyser les plaintes relatives à la cybercriminalité qui lui sont acheminées, de les valider, de récupérer certains éléments de preuve et de les retransmettre aux autorités concernées.

Il a également pour mandat de détecter et d'analyser les tendances liées à la cybercriminalité et de former les membres de la Sûreté du Québec en matière de la lutte à la criminalité sur Internet[109].

[109] Consulter la page Web du module de cybersurveillance de la Sûreté du Québec : www.suretequebec.gouv.qc.ca/lutte/cybersurveillance/cybersurveillance.html

2.g Pédagogie

Outre les activités de pédagogie réalisées par les organismes canadiens, il convient de mentionner que la Sûreté du Québec participe à la sensibilisation et à l'éducation des jeunes et de leurs parents dans l'utilisation d'Internet et a produit un dépliant à cet effet[110]. De plus, il existe un groupe de recherche sur les jeunes et les médias, rattaché à l'Université de Montréal (GRJM - www.grjm.umontreal.ca/accueil.html) qui se penche sur les façons dont les nouveaux contenus médiatiques et les nouvelles plates-formes (incluant Internet et les mobiles) interagissent avec le développement cognitif, affectif et psychosocial des jeunes[111].

3.b Protection des données et de la vie privée

Le Québec possède des lois concernant la protection de la vie privée qui s'applique autant auprès des organismes publics qu'auprès des organismes privés et couvre donc les activités de toutes les organisations et des individus au Québec dans ce domaine. Ces lois sont entièrement compatibles avec celles que l'on retrouve aux niveaux fédéral et international.

5.2.4 Canada – Ontario

Responsabilité et types de régulation

En Ontario, le classement des films, y compris ceux sur support vidéo, DVD, VCD et les jeux vidéo, est effectué, selon la Loi de 2005 sur le classement des films[112], par la Commission de contrôle cinématographique de l'Ontario (www.ofrb.gov.on.ca/Francais) qui, tout en étant indépendante dans son fonctionnement, relève du ministre des Services gouvernementaux.

---

[110] Consulter le document n° 46.2 du Cahier 4 *Prudence sur le NET* (www.suretequebec.gouv.qc.ca/publications/publications/prudence_net.pdf)
[111] Consulter le document n° 46.4 du Cahier 4 *Groupe de recherche sur les jeunes et les médias* (www.grjm.umontreal.ca/accueil.html)
[112] Consulter la page Web suivante de la Loi : www.e-laws.gov.on.ca/DBLaws/Statutes/French/05f17_f.htm

Tout film et tout jeu vidéo, pour être distribué ou présenté en Ontario, doit avoir été classé par cette commission. Cependant, elle n'a aucune compétence concernant le contenu audiovisuel sur Internet et aucun autre organisme n'en a.

2.e Contrôle du contenu – lutte à la cypercriminalité

En Ontario, c'est la Section de la pornographie juvénile de la **Police provinciale de l'Ontario** (**Project P** - **OPP**) www.opp.ca/Organisation/Enquetesetcrimeorganise/opp_000700.html qui assume la responsabilité première dans ce domaine. Elle a pour mandat d'enquêter sur toutes personnes reliées à la pornographie juvénile et d'intenter, le cas échéant, des poursuites à leur endroit. Elle est également chargée de l'application des dispositions du code criminel du Canada sur le leurre (« luring ») des enfants et donne la priorité à ce type d'enquêtes.

Une autre organisation de Trenton en Ontario et qui a un rayonnement au niveau mondial, est le **Cyber Law Enforcement Organization** (**CLEO**) (www.cyberlawenforcement.org). Elle se spécialise dans les enquêtes sur la cybercriminalité et offre une assistance en ligne aux victimes de la cybercriminalité (comme la cyberintimidation ou le cyberharcèlement) et fait œuvre de pédagogie sur ce sujet.

2.g Pédagogie

Il est intéressant de noter l'organisation internationale située à Toronto, **TakingITGlobal** (http://about.takingitglobal.org)[113] qui est dirigée par les jeunes et soutenue par la technologie et son site Web multilingue. Cette organisation permet d'interconnecter les jeunes à travers le monde intéressés par des cultures différentes et vise à développer la capacité des jeunes dans l'expression artistique et des médias, à rendre l'apprentissage plus engageant et à impliquer les jeunes dans certaines prises de décision globales. Elle est soutenue par des agences de l'ONU, des compagnies et des organisations de jeunes. Elle comprend plus de 130 000 membres provenant de plus de 200 pays ou territoires. Cette organisation présente un volet d'éducation sur la sûreté en ligne (www.takingitglobal.org/themes/onlinesafety). Elle a d'ailleurs participé au *Youth Summit for Online Safety* qui s'est tenu en juin 2006 en Californie[114].

---

[113] Consulter le document n° 47.1 du Cahier 4 *TakingIGGlobal* (www.takingitglobal.org)
[114] Consulter le document n° 47.2 du Cahier 4 *Youth Summit for Online Safety* (www.govtech.net/magazine/channel_story.php/94208)

5.2.5 Canada – Nouveau-Brunswick

Responsabilité et types de régulation

C'est la province de la Nouvelle-Écosse qui se charge, pour le Nouveau-Brunswick et l'Île-du-Prince-Édouard, du classement des films, y compris ceux sur support vidéo. L'organisme gouvernemental, le **Film Classification** de l'**Alcohol and Gaming Authority** (www.gov.ns.ca/enla/agd) réalise ce classement et la loi rend obligatoire de le respecter. Pour ce qui est des jeux vidéos, la classification utilisée depuis 2005 est celle de l'organisation **Entertainment Software Rating Board** (ESRB - www.esrb.org/index-js.jsp), organisation indépendante de classement des jeux vidéos et sur ordinateur qui opère sur une base d'autorégulation et dont son système de classification se retrouve répandu auprès des clubs de jeux vidéos du Québec. Il n'y aucune catégorisation ni aucun classement du contenu audiovisuel sur Internet pour le Nouveau-Brunswick.

2.g Pédagogie

Le gouvernement du Nouveau-Brunswick participe activement à l'alphanétisation et à la sensibilisation aux risques liés à l'utilisation d'Internet. Ainsi, sur la première page du portail du gouvernement du Nouveau-Brunswick (www.gnb.ca/index-f.asp), on retrouve la campagne de sensibilisation « Soyez en sécurité sur Internet » et « Internet 101 » qui est géré par le ministère de la Sécurité publique (www.gnb.ca/0276/Internet101/index-f.asp) et destiné aux jeunes, à leurs parents et éducateurs. Il est le résultat de la collaboration de plusieurs organisations policières (dont la GRC et la Sûreté du Québec) et de la société civile.

5.2.6 Canada – Colombie britannique

Responsabilité et types de régulation

L'Office de classification des films (Film Classification Office - www.bcfilmclass.com), qui relève du ministère de la Sécurité publique et du Solliciteur général (Ministry of Public Safety and Solicitor General), effectue le classement des films en Colombie-britannique et pour le compte de la Saskatchewan. Seuls les films montrés en public sont soumis au classement. Certains autres films sur support vidéo sont aussi classés par cet office.

2.f Lutte au pollupostage

Le ministère de l'Éducation réfère à un site Web à l'extérieur de la province, soit le Community Learning Network (www.cln.org/spam.html), où il est question de pollupostage. Mais on n'y a détecté aucune initiative particulière en matière de pollupostage ni spécifiquement pour la protection de la jeunesse.

2.g Pédagogie

Quelques organismes gouvernementaux déploient des efforts pour réaliser une certaine sensibilisation et formation destinées à la protection des jeunes sur Internet.

Le Ministère du développement des enfants et de la famille (www.safekidsbc.ca/links.htm#internet) fournit sur une page Web sur la prévention d'abus d'enfants où il indique deux références spécifiques à la sûreté d'Internet : une première qui provient du ministère de l'Éducation de la Colombie britannique et qui fournit des conseils aux parents pour aider leurs enfants à naviguer de façon sûre sur Internet[115], et une deuxième qui est un site Web des États-Unis, soit NetSmartz Workshop (www.netsmartz.org), qui offre une ressource interactive et éducationnelle relative à la sûreté sur Internet, selon l'âge des enfants, offerte par le National Center for Missing & Exploited Children (NCMEC) et Boys & Girls Clubs of America (BGCA) à l'intention des enfants de 5 à 17 ans, leurs parents, tuteurs, enseignants et représentants de la loi.

Ce même ministère fournit de plus une page Web (www.safekidsbc.ca/parent_child_safety.htm) portant sur la prévention d'abus d'enfants sans référence à Internet. Cependant, il offre des conseils très judicieux, précis et pratiques sur certains abus d'enfants comme l'intimidation (bullying), conseils qui pourraient se transposer facilement pour le monde d'Internet.

Pour sa part, le ministère de l'Éducation fournit une liste de conseils pour aider les parents à protéger leurs enfants lors de l'utilisation d'Internet[116]. De plus, il fournit des références à certains sites dont ceux-ci :

- Community Learning Network – www.cln.org : site des États-Unis destiné à aider les enseignants à intégrer la technologie dans leur enseignement. Ce site comprend une page Web portant sur les façons de faire face aux abus sur Internet et particulièrement ceux, personnels, s'adressant à la jeunesse;
- American Library Association (ALA) – la division Association for Library Service to Children (ALSC) y publie un guide pour aider les parents et les enfants dans l'utilisation d'Internet. (www.ala.org/ala/alsc/greatwebsites/greatsitesbrochure.pdf)

3.c Gestion de l'identité et authentification

Le gouvernement de la Colombie britannique a commencé à déployer une solution permettant d'identifier numériquement ses citoyens. Cette solution, l'authentification « BCeID » est présentement utilisée sur une base volontaire pour l'accès aux services gouvernementaux en ligne mais sera éventuellement rendue obligatoire pour tous ses citoyens, incluant les jeunes. Cette identification n'est pas conçue spécifiquement pour eux mais

[115] Consulter le document n° 49.1 du Cahier 4 *Internet Safety Tips for Parents* (www.bced.gov.bc.ca/resourcedocs/internet_safe/internet_safe.pdf)
[116] Consulter le document n° 49.1 du Cahier 4

elle a toute la potentialité pour être utilisée dans la protection de la jeunesse concernant certains contenus sur Internet[117].

---

[117] Consulter la page Web du blogue de Phillip J. Windley : www.windley.com/archives/2006/09/digital_identity_in_bc_government.shtml

5.2.7 Europe

Dans cette section, l'Europe va comprendre autant l'Union européenne (« Europe des 27 ») que le Conseil de l'Europe (« Europe des 46 »). L'évaluation de la gouvernance présentée se base sur les actions réalisées par l'Europe comme entité politique à part entière et non pas par l'ensemble des pays européens. Ainsi, certaines actions peuvent être recommandées par l'Europe mais réalisées de façon très variable d'un pays à l'autre. Nous verrons, dans des sections subséquentes comment la gouvernance s'établit de façon spécifique dans certains de ces pays.

Responsabilité et types de régulation

L'Europe a mis en place des mesures législatives ou des programmes concourant à la protection de la jeunesse par rapport à Internet et, notamment, son contenu audiovisuel. Bien que quelques mesures sont obligatoires et s'appliquent à l'ensemble des pays faisant partie de l'Europe sous forme de directives (telles que celles en matière de cybercriminalité et de pollupostage), la majorité des mesures sont des recommandations ou des programmes qui sont mis en oeuvre sur une base volontaire tel le programme « Safer Internet » ou « Programme pour un Internet plus sûr ».

L'Europe ne dispose pas d'organisme spécifique de catégorisation ou de classification du contenu audiovisuel sur Internet. C'est laissé à l'entière discrétion des états membres.

L'Europe, en matière de gouvernance de contenu audiovisuel, a recours principalement à l'autorégulation et à la régulation (les deux modes, soit recommandation et directive) mais en insistant davantage sur la régulation en mode recommandation et en la complétant de programmes incitatifs de financement ou d'aide technique (sous la forme de guides pratiques par exemple) pour aider à mettre en oeuvre les mesures volontaires recommandées, d'où la corégulation. Bien que l'Europe ne soit pas responsable des choix nationaux, par ses programmes incitatifs, elle parvient assez bien à faire en sorte que ses recommandations deviennent des réalités nationales. Il faut dire que les recommandations correspondent déjà à un consensus des nations européennes et qu'elles ont donc fait l'objet de débats autant sur les fondements des recommandations que sur les façons de les mettre en oeuvre. L'Europe fait assez bien la démonstration qu'une régulation en mode recommandation peut bien fonctionner si elle est appuyée de programmes incitatifs de mise en oeuvre.

Elle a recours à l'autorégulation en laissant l'industrie s'autoréguler concernant la catégorisation et le classement éventuel du contenu sur Internet, notamment en matière d'Internet et la téléphonie mobile.

L'Europe dispose donc d'un ensemble de principes, de normes, de lois et de programmes communs.

En 2005, l'Europe a adopté une recommandation relative à la protection des mineurs et de la dignité humaine dans le domaine de l'audiovisuel et de la société de l'information afin de s'adapter à l'évolution de l'univers médiatique concernant les contenus illicites et préjudiciables sur Internet pour les mineurs. Afin de protéger les enfants et les personnes les plus fragiles des contenus préjudiciables et illégaux, les actions doivent, selon ce texte, être menées à trois niveaux de responsabilité :

- responsabilité politique, par la mise en place de campagnes d'information auprès des citoyens sur les dangers et les risques de sanctions pénales encourues;
- responsabilité des industriels, avec la mise à disposition par les hébergeurs de logiciels de contrôle parental;
- responsabilité éducative et parentale, en inscrivant la société de l'information dans les programmes scolaires afin de garantir une meilleure utilisation d'internet.

1.a DNS

L'Europe recommande l'utilisation de logiciel de filtrage ou de contrôle parental dont la plupart a recours au DNS.

De plus, en 2004, l'Europe a émis un ensemble de recommandations relatives à la protection des mineurs et de la dignité humaine dans le domaine de l'audiovisuel et de la société de l'information. L'une d'elle portant sur la création d'un nom de domaine « .kid » qui serait réservé aux contenus pour enfants. Ceci permettrait d'avoir un espace Internet sécurisé qui leur serait consacré en créant, notamment, une « liste verte » de sites Web pour enfants.

1.b Serveurs racine

Il n'y a pas d'utilisation des serveurs racine pour gérer le contenu d'Internet.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

L'Europe a recours au multilinguisme pour ce qui est du contenu pour soutenir plusieurs des langues nationales européennes. De plus, l'Europe encourage le recours aux noms de domaines internationalisés (IDN – Internationalized Domain Names) pouvant contenir les accents propres aux langues européennes. Certaines autorités nationales le font.

2.a Création du contenu – catégorisation

L'Europe ne réalise pas de catégorisation de contenus de sites Web. Cependant, elle favorise cette catégorisation en soutenant financièrement l'ICRA.

2.b Création du contenu – classement

L'Europe ne réalise pas de classement de contenus de sites Web.

2.c Homologation du contenu

L'Europe ne réalise pas d'homologation de contenus de sites Web. Cependant, des initiatives nationales permettent de le faire.

2.d Contrôle du contenu – filtrage

L'Europe encourage l'utilisation de filtrage, selon les choix nationaux.

2.e Contrôle du contenu – lutte à la cybercriminalité

La lutte à la cybercriminalité est un des domaines où l'Europe a recours à la régulation en mode directive. Même s'il est difficile de convenir d'une définition de pornographie à l'échelle mondiale car ce qui acceptable dans

un pays peut ne pas l'être dans un autre[118], il a été possible pour l'Union européenne de convenir de balises communes dans une loi qui indique la nécessité d'une certaine adaptabilité aux différences nationales telles que l'âge de consentement comme adulte. Elle dispose maintenant d'une Convention sur la cybercriminalité liant tous les pays[119] ainsi que du réseau INHOPE, réseau international de lignes d'urgence ou de « points de contact » (INHOPE - International Association of Internet Hotlines ou Association internationale de services d'assistance en ligne) permettant de signaler toute manifestation possible de cybercriminalité à travers l'Europe et certains autres pays dont le Canada.

2.f Lutte au pollupostage

La lutte au pollupostage est l'un des autres domaines où l'Europe a recours à la régulation en mode directive. Elle a voté en 2002 la directive « Vie privée et communications électroniques » qui a introduit dans l'ensemble de l'Union européenne le principe dit « opt-in », c'est-à-dire le consentement préalable de la personne pour l'envoi de courriel à des fins commerciales. Ainsi, dans chacun des États membres, la prospection par courriel est interdite sauf si la personne a donné son consentement préalable[120]. Évidemment, cette obligation européenne reste sujette aux pratiques disparates des autres pays non européens.

2.g Pédagogie

L'Europe, comme stratégie de protection de la jeunesse, favorise énormément la sensibilisation et la formation à Internet, à ses risques et aux façons d'y faire face. Elle dispose notamment du programme « Safer Internet »[121] qui vient d'être reconduit[122]. Il a été considéré comme un succès, notamment en raison du bon fonctionnement :

---

[118] Consulter le document n° 9 du Cahier 1 *Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach* (www.cyber-rights.org/reports/governan.htm)

[119] Consulter le document n° 2 du Cahier 4 *Convention sur la cybercriminalité* (http://conventions.coe.int/Treaty/fr/Treaties/Word/185.doc)

[120] Consulter le document n° 32 du Cahier 4 *Directive Vie privée et Communications électroniques* (www.lexinter.net/UE/directive_vie_privee_et_communications_electroniques_du_12_juillet_2002.htm)

[121] Consulter le document n° 4 du Cahier 3 *A multiannual Community Programme on promoting safer use of the Internet and new online technologies* (http://europa.eu.int/information_society/activities/sip/call/proposals/index_en.htm et http://europa.eu.int/information_society/activities/sip/docs/call_2006/sip_work_programme_2006.pdf)

- du réseau européen INHOPE (association des 21 lignes directes nationales internet permettant aux utilisateurs de signaler de manière anonyme des contenus illicites sur Internet). Selon l'INHOPE, environ 65 000 rapports ont été transmis en 2005 aux organismes nationaux et internationaux chargés de faire respecter la loi, pour qu'ils enquêtent et prennent les mesures requises;
- du réseau de sensibilisation INSAFE (www.SaferInternet.org) composé de 23 nœuds nationaux visant à promouvoir une utilisation plus sûre d'Internet auprès des enfants, des parents et des enseignants.

Par ce programme, l'Europe organise beaucoup d'activités dont une journée annuelle de sensibilisation (Safer Internet Day). C'est par le biais de ce programme que l'Europe participe au financement de l'ICRA.

3.a Liberté d'expression

L'Europe respecte la liberté d'expression dans ses directives, recommandations et programmes relatifs à la protection de la jeunesse. Le Conseil de l'Europe dispose de la Déclaration sur la liberté d'expression sur Internet[123].

3.b Protection des données et de la vie privée

L'Europe dispose d'une directive générale rendant obligatoire la protection de la vie privée[124].

3.c Gestion de l'identité et authentification

L'Europe n'a pas de dispositif d'authentification commun à l'ensemble des pays. Cependant, elle est en réflexion sur ce dossier et déjà certains pays ont mis en place des initiatives d'authentification si bien qu'elle aura à faire face à l'interopérabilité des différents systèmes nationaux d'authentification

---

[122] Consulter le document n° 41.8 du Cahier 4 *Évaluation du programme « Safer Net »* (http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/1512&format=HTML&aged=0&language=EN&guiLanguage=en)

[123] Consulter le document n° 2 du Cahier 3 *Liberté d'expression sur Internet* (www.europarl.europa.eu/sides/getDoc.do?Type=TA&Reference=P6-TA-2006-032...)

[124] Consulter le document n° 41.10 *Directive sur la protection des données personnelles* (www.lexinter.net/UE/directive_du_24_octobre_1995_sur_la_protection_des_donnees_personnelles.htm)

afin d'offrir une approche commune ou compatible pour l'ensemble des pays de l'Europe[125].

5.2.8 Allemagne

L'Allemagne ne sera abordée que brièvement pour souligner deux des éléments plus différentiels de ce pays, soit le multilinguisme et la protection de la vie privée.

1.d Multilinguisme

Le gestionnaire du premier niveau du nom de domaine pour l'Allemagne, « .de », soit DENIC.De (www.denic.de), est l'un des plus avancés de l'Europe concernant le soutient de l'internationalisation des noms de domaine (IDN - Internationalized Domain Names). Ainsi, dès 2004, il avait déjà plus de 200 000 noms de domaine avec des caractères accentués propres à la langue allemande[126]. Et l'Allemagne sert actuellement d'inspiration à l'Autorité canadienne pour les enregistrements Internet (ACEI – www.ACEI.ca) pour mettre en place l'internationalisation des noms de domaine au Canada[127].

3.b Protection des données et de la vie privée

La protection de la vie privée est très importante en Allemagne. D'ailleurs, une étude publiée en novembre 2006 permettait de classer le Canada et l'Allemagne comme les meilleurs défenseurs de la vie privée[128].

---

[125] Consulter le document n° 39.2 du Cahier 4 *Contribution pour une Europe numérique* (www.industrie.gouv.fr/pdf/europnum.pdf).
[126] Consulter le document n° 50.1 du Cahier 4 *IDN Deployment in Germany* (www.ripe.net/ripe/meetings/ripe-48/presentations/ripe48-dns-idn-de.pdf)
[127] Information fournie lors de la conférence prononcée par le président de l'ACEI, monsieur Turcotte, à l'occasion de la rencontre avec l'ICANN organisée par ISOC Québec le 23 novembre 2006 (www.isoc.qc.ca/tiki-read_article.php?articleId=24)
[128] Consulter la page Web du journal *Globe and Mail* : (www.theglobeandmail.com/servlet/Page/document/v4/sub/MarketingPage?user_URL=http://www.theglobeandmail.com%2Fservlet%2Fstory%2FRTGAM.20061101.wpriv1101%2FBNStory%2FNational%2F%3Fpage%3Drss%26id%3DRTGAM.20061101.wpriv1101&ord=1163442966379&brand=theglobeandmail&force_login=true)

5.2.9 Belgique

La Belgique ne sera abordée que brièvement pour souligner un des éléments plus différentiels de ce pays, soit l'authentification des internautes.

3.c Gestion de l'identité et authentification

La Belgique a mis en place une carte d'identité numérique « eID » pour tous les citoyens belges. Elle a, de plus, commencé à l'utiliser spécifiquement pour la protection des jeunes sur Internet et notamment pour la vérification de l'âge pour les sites de clavardage des 12-15 ans[129].

5.2.10 Danemark

Responsabilité et types de régulation

La gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse s'effectue, au Danemark, selon un mode qui se concentre surtout autour de l'autorégulation et de la régulation en mode recommandation. Bien sûr, toujours en ce qui a trait au contenu illégal, le Danemark, comme les autres pays de l'Europe qui sont soumis à la Loi sur la cybercriminalité, a recours à une régulation en mode directive.

En 1997, le gouvernement danois a aboli l'organisme de classification des films (National Board of Film Censorship) et a élargi le mandat du Conseil des médias pour les enfants et les jeunes gens (Medierådet for Børn og Unge - Media Council for Children and Young People – MCCYP - http://portal.medieraadet.dk), rattaché au ministre de la Culture, afin de couvrir à la fois les films, les jeux et Internet, et ainsi tenir compte de l'évolution du paysage médiatique. Ce Conseil des médias a la tâche d'attribuer les classements aux films[130].

Il a revisité son site Web en 2005 afin de mieux soutenir cette mission auprès des parents et des enseignants. Il leur offre des occasions d'apprentissage en ligne sur différents sujets tels que la sûreté sur Internet,

[129] Consulter le document n° 50.2du Cahier 4 *Carte d'identité numérique* (http://eid.belgium.be/fr/navigation/documents/39743.html)
[130] La méconnaissance de la langue danoise nous empêche d'aller plus avant dans l'objet du classement (vidéo, jeux, etc.).

les jeux en ligne, les filtres, le clavardage, le partage de fichiers et la téléphonie mobile pour enfant[131].

Le Conseil des médias englobe des activités de sensibilisation qui incluent les 5 « C » :

- Contenu : sélection, éducation et filtrage;
- Contact : « hotlines », campagnes de sensibilisation;
- Commercial : autorégulation, choix;
- Configuration : recherche sur les médias;
- Compétence : expérience pratique avec les médias, exemple de modèle parental[132].

La loi danoise sur la télédiffusion (télévision et radio), sous la responsabilité de l'Agence nationale des technologies de l'information et des télécommunications (National IT and Telecom Agency) du ministère de la Science, de la Technologie et de l'Innovation, inclut aussi l'utilisation d'Internet pour la diffusion de radio ou télévision (TVIP)[133].

1.a DNS

Le Danemark a recours à des logiciels de filtrage et donc utilise le DNS.

1.b Serveurs racine

Pas d'utilisation des serveurs racine pour gérer le contenu d'Internet.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

[131] Consulter le document n° 48.5 du Cahier 4 *Rapport annuel du Media Council for Children and Yound People* (http://andk.medieraadet.dk/upload/d1_4_annual_report_andk.pdf)
[132] Consulter le document n° 48.5 du Cahier 4 (p. 11)
[133] Consulter la loi *Danish Radio and Television Broadcasting Act - ACT N° 1052* du 17 décembre 2002 (http://kum.dk/sw4498.asp).

Le Danemark a recours au multilinguisme pour ce qui est du contenu afin de soutenir l'anglais et le danois.

2.a Création du contenu – catégorisation

Le Danemark, à notre connaissance, n'effectue pas de catégorisation particulière du contenu des sites Web, bien que certains de ses sites utilisent le système d'étiquetage de l'ICRA.

2.b Création du contenu – classement

Le Danemark, à notre connaissance, n'effectue pas de classement du contenu des sites Web. Cependant, comme nous le verrons plus loin, il a des initiatives pour offrir aux jeunes un portail qui leur est destiné et d'effectuer une homologation de certains sites.

2.c Contrôle du contenu - homologation

Le Danemark considère que le clavardage constitue une des activités à risque pour les enfants et les jeunes gens. Le ministère de la Science, de la Technologie et de l'Innovation a donc lancé un projet visant à attribuer aux sites de clavardage un sceau de sûreté (Safe-chat smiley). À cette fin, un groupe de travail comprenant des professionnels, des représentants des FSI (association danoise des médias d'Internet - FDIM) et du Conseil des médias, dans une optique d'autorégulation, sont à développer les critères d'évaluation et d'attribution d'une telle homologation ainsi que les procédures afférentes. Ces critères vont inclure, notamment, les mécanismes de reportage et de blocage à l'intention des utilisateurs ainsi que la présence d'information sur le clavardage sécuritaire et la supervision (ou modération) des portails de clavardage.

Ce service d'homologation, prévu disponible à la fin de 2006, sera basé sur l'autorégulation et sera utilisé sur une base volontaire. La seule obligation des FSI sera de passer à travers du processus d'homologation s'ils désirent inscrire le sceau de sûreté sur leur portail de clavardage.

Le Conseil des médias insiste sur le fait que ce sceau ne sera qu'un outil pour la sûreté du clavardage des enfants et des jeunes gens et qu'il demeurera crucial de maintenir les efforts de sensibilisation tant auprès des parents et enseignants qu'auprès des enfants et des jeunes gens afin de

s'assurer d'un clavardage sécuritaire. L'initiative d'homologation doit donc être accompagnée de formation[134].

2.d Contrôle du contenu – filtrage

Le principe qui gouverne le filtrage au Danemark peut se résumer dans cette phrase :

The « gate keeper » days are over !

« L'Internet est comme un diamant aux milles facettes »

« The gate keeper days are over »

En effet, auparavant, la protection de la jeunesse se basait sur la censure appliquée sur des produits tangibles et faisait office de gardienne dans les salles de cinéma et à la maison. Cependant, Internet a introduit le concept de société en réseau où le choix des enfants n'est plus limité par le temps et l'espace et où d'énormes possibilités d'apprentissage, de communications et de développement sont apparues pour la jeunesse[135]. Internet, tout en représentant des situations potentiellement dangereuses ou désagréables, offre un haut potentiel d'expériences positives.

C'est pourquoi le Danemark s'est tourné de façon très importante vers l'éducation afin d'augmenter l'alphanétisation des jeunes, de leurs parents et de leurs éducateurs.

Cependant, le filtrage n'est pas délaissé pour autant.

Ainsi, pour ce qui est de l'accès à Internet par la téléphonie mobile, le Conseil des médias recommande la disponibilité de filtre mais une non-activation automatique afin de ne pas faire perdre de vue la responsabilité première des parents d'éduquer leurs enfants et éviter ainsi de leur donner un faux sentiment de sécurité[136].

De plus, depuis juin 2006, le ministre de la Culture offre à toutes les bibliothèques danoises la disponibilité de filtres d'Internet afin de leur permettre; sur une base volontaire, d'empêcher l'accès à des sites pornographiques aux jeunes qui fréquentent leur bibliothèque. Encore ici, l'Union des bibliothécaires insiste sur l'importance d'accompagner la solution de filtrage par celle d'éducation des jeunes vers un comportement sécuritaire sur Internet et sur l'importance de ne pas bloquer les sites ayant une valeur d'éducation sexuelle[137].

---

134 Consulter le document n° 48.4 du Cahier 4 *Sceau pour les sites de clavardage* (www.saferinternet.org/ww/en/pub/insafe/news/articles/1006/dk.htm)
135 Consulter le document n° 48.5 du Cahier 4 *Rapport annuel du Media Council for Children and Yound People* (http://andk.medieraadet.dk/upload/d1_4_annual_report_andk.pdf)
136 Consulter le document n° 48.3 du Cahier 4 *Questionnaire sur la téléphonie mobile* (http://europa.eu.int/information_society/activities/sip/docs/public_consultation/results/mccyp_a337786.pdf) ainsi que le document n° 48.5 du Cahier 4 (p. 10)
137 Consulter le document n° 21 du Cahier 3 *Danish Minister of Culture offers Danish libraries internet filters* (www.saferinternet.org/ww/en/pub/insafe/news/articles/0606/dk.htm)

2.e Contrôle du contenu – lutte à la cybercriminalité

Le Danemark, comme tout autre pays de l'Europe, est soumis à la loi européenne sur la cybercriminalité.

Au Danemark, le Code juridique concernant la pornographie enfantine a été modifié en 1999 pour prendre en compte la propagation de la pornographie infantile via Internet. En 1998, l'organisation internationale Red Barnet a mis en place au Danemark (www.redbarnet.dk) une « hotline » afin de faire progresser la lutte contre la pornographie enfantine. Red Barnet collabore avec l'autorité judiciaire danoise et l'organisation danoise des fournisseurs Internet. La police danoise (www.politi.dk) offre aussi une « hotline » où tout comportement illégal sur Internet peut être rapporté.

2.f Lutte au pollupostage

Le Danemark réalise, comme tous les pays européens, sa partie de lutte contre le pollupostage. L'envoi de pourriels est illégal au Danemark mais tant qu'il reste des pays où cela ne l'est pas, il reste une lutte à poursuivre.

Ainsi, en décembre 2004, le Danemark a lancé sa stratégie nationale antipollupostage. En 2005, les FSI ont lancé une solution technique commune contre le pollupostage[138]. De plus, en janvier 2006, les FSI ont mis en œuvre un code de conduite relatif au pollupostage qui les oblige à utiliser un filtre central contre les pourriels ou d'offrir une solution qui leur est propre contre les pourriels. Les FSI doivent aussi indiquer à leurs clients le potentiel de filtrage et ses limites. Ce code de conduite inclut des dispositifs lorsque des pourriels sont effectivement envoyés. Le code de conduite est le résultat de collaboration entre les FSI faisant partie du Forum sur la sûreté (ISP Safety Forum - ISP Sikkerhedsforum)[139].

Le site Web du Conseil des médias couvre aussi les sujets du pollupostage et des filtres et fournit des conseils pour éviter le pollupostage.

[138] Consulter la page Web d'INSAFE : www.saferinternet.org/ww/en/pub/insafe/news/articles/0305/dk_newcamp.htm

2.g Pédagogie

La stratégie de sensibilisation et d'éducation afin d'augmenter l'alphanétisation des jeunes, de leurs parents et de leurs éducateurs est au cœur de la gouvernance du contenu audiovisuel au Danemark afin de protéger la jeunesse.

Le **Conseil des médias** joue un rôle prédominant dans la stratégie d'alphanétisation des jeunes, de leurs parents et de leurs éducateurs.

Il ne recommande généralement pas d'avoir recours uniquement à des solutions techniques pour répondre aux risques soulevés par l'utilisation d'Internet par les jeunes. Il attribue la responsabilité première aux parents et par la suite aux enseignants d'éduquer les enfants à l'utilisation d'Internet. Il souligne aussi l'importance d'adopter des stratégies différentes selon le groupe d'âge. Le Conseil des médias recommande de dialoguer avec leurs enfants sur leurs expériences en ligne. Plutôt que d'empêcher l'accès à Internet, il recommande que les parents permettent à leurs enfants d'acquérir les compétences nécessaires pour distinguer entre la fiction et la réalité (en matière de pornographie par exemple). Il offre une aide aux parents en fournissant une « Liste de vérification » sur la façon de discuter de l'utilisation d'Internet avec leurs enfants.

Une étude récente intitulée « Boys » et réalisée auprès des garçons de 12 à 17 ans, est assez révélatrice : la majorité des garçons interviewés avaient déjà vu de la pornographie sur Internet. L'auteure de l'étude résume ainsi :

> « In the long term, you don't get anything out of saying, 'Don't'. You need to teach them to choose. Tell them that they only need to see what they want to see and that they also need to remember to tell each other when they think something is unpleasant. »[140]

Le Conseil des médias représente le nœud danois du réseau européen « Safer Internet ». Il regroupe au Danemark près d'une trentaine de membres représentant le gouvernement, les parents, les enseignants, le secteur éducationnel, l'industrie et la recherche[141].

Le Conseil des médias collabore avec le ministère de la Science, de la Technologie et de l'Innovation et le Centre des technologies de l'information pour l'Éducation et la Recherche (IT Centre for Education

---

[139] Consulter le document n° 48.6 du Cahier 4 *Lutte au spam* (www.saferinternet.org/ww/en/pub/insafe/news/articles/1005/dk.htm)
[140] Consulter le document n° 19 du Cahier 3 *Danish parents prepare children for harmful content* (www.saferinternet.org/ww/en/pub/insafe/news/articles/0505/dk_parents.htm)
[141] Consulter le document n° 48.3 du Cahier 4 *Questionnaire sur la téléphonie mobile* (http://europa.eu.int/information_society/activities/sip/docs/public_consultation/results/mccyp_a337786.pdf)

and Research - UNI-C), afin de rendre disponibles des articles sur le portail danois d'apprentissage (www.emu.dk) permettant d'informer les enseignants et les enfants (7 à 10 ans) des mesures à prendre pour naviguer de façon sécuritaire sur Internet[142].

Le Conseil des médias souligne l'urgence de l'alphanétisation des jeunes avec la venue d'Internet par la téléphonie mobile.

Une étude auprès des parents réalisée en 2006 par SAFT, dont le Conseil des médias en est le représentant au Danemark[143], révèle certaines caractéristiques intéressantes :

- Les parents danois sont les parents scandinaves qui présentent le degré de confiance le plus élevé dans les capacités de leurs enfants à faire face à des expériences désagréables sur Internet;
- 91 % des parents croient que les bénéfices dépassent largement les aspects négatifs d'Internet;
- La principale préoccupation des parents est la somme de temps que le jeune passe sur Internet (pour 23 % des parents) et la seconde (pour 15 % des parents) concerne la pornographie;
- Seulement 11 % des parents ont installé un logiciel de filtrage.

SAFT - Safety, Awareness, Facts and Tools est un consortium européen dans lequel le Danemark, par le biais du Conseil des médias, y participe et qui fait la promotion de l'utilisation d'Internet avec sûreté de la part des jeunes. Ce consortium vise à réduire les comportements à risque sur Internet et à rendre les jeunes utilisateurs d'Internet responsables, notamment en matière d'information inexacte, de matériel nuisible, de publicité intrusive, de harcèlement et d'intimidation en ligne, tout en mettant l'accent sur les aspects positifs de l'utilisation d'Internet. SAFT intervient aussi auprès des parents, des enseignants et de l'industrie d'Internet pour qu'ils puissent à leur tour aider les jeunes[144].

Le Conseil des médias réalise de plus différentes activités de formation destinées aux enseignants, parents, à l'industrie des TI et aux représentants

---

[142] Consulter le document n° 48.2 du Cahier 4 (p. 28) *IT and Telecommunications Policy Report 2006* (http://itst.dk/image.asp?page=image&objno=203180229)

[143] Consulter le document n° 48.8 du Cahier 4 *SAFT - Safety, Awareness, Facts and Tools – Parental survey 2006* (www.saftonline)

[144] Les quatre autres pays sont : la Norvège (*The Norwegian Board of Film Classification* - http://film.medietilsynet.no, *ICT Norway* - www.ikt-norge.no, *MMI Norway* - www.synovate.no), l'Islande (*Home and School* - http://heimiliogskoli.is), la Suède (*Council on Media Violence* - www.medieradet.se) et l'Irlande (*National Centre for Technology in Education* - www.ncte.ie). Consulter le document n° 48.8 du Cahier 4 *SAFT – Safety, Awareness, Facts and Tools*

gouvernementaux sur les nouveaux médias eux-mêmes et sur l'utilisation dont les jeunes en font[145].

L'organisation « Red Barnet » (www.redbarnet.dk/Default.aspx?ID=983) est la division danoise de l'organisation « International Save the Children Alliance » qui a des unités dans 29 pays et des programmes dans une centaine. Cette organisation lutte pour les droits des enfants et l'amélioration de leur vie à l'échelle mondiale.

Le Centre de l'éducation supérieure de la Copenhagen Business School (Center for Higher Education – CHE - www.cbs.dk) a participé à l'étude universitaire Mediappro (Media Appropriation), dont il est fait référence sous la section « Canada – Québec ».

Un projet qui se distingue beaucoup des autres projets d'alphanétisation de par la participation active des jeunes est le projet Cyberhus (Cybermaison - www.cyberhus.dk). Cette *Maison danoise en ligne pour les enfants* est créée par et pour les jeunes qui décident du texte, des images, des graphiques, de la navigation et de l'étendue des activités qui y sont conduites. Les jeunes sont tour à tour critiques, écrivains, rappeurs, consultants en TIC et aussi chercheurs de conseils. Le concept derrière ce projet est de donner un sens d'appartenance aux jeunes utilisateurs et de générer leur participation active. De plus, les jeunes acquièrent les habiletés nécessaires pour devenir des citoyens actifs[146]. C'est un des rares projets relevés où les jeunes ont l'occasion d'apprendre à créer du contenu en ligne.

3.a Liberté d'expression

La liberté d'expression constitue un des principes fondamentaux dans la gouvernance d'Internet au Danemark[147].

3.b Protection des données et de la vie privée

[145] Consulter le document n° 48.5 du Cahier 4 *Rapport annuel du Media Council for Children and Young People* (p. 17) (http://andk.medieraadet.dk/upload/d1_4_annual_report_andk.pdf)
[146] Consulter le document n° 48.7 du Cahier 4 *Cyberhus* (www.saferinternet.org/ww/en/pub/insafe/news/articles/0705/dk.htm)
[147] Consulter la page Web du ministère de la Culture : http://kum.dk/sw2991.asp

Le Danemark respecte le principe de la protection de la vie privée comme tout autre pays membre de l'Union européenne.

3.c Gestion de l'identité et authentification

Nous n'avons pas pu observer de gestion de l'identité ou d'authentification spécifique aux jeunes. Cependant, depuis 2003, le gouvernement danois a mis en place la signature électronique disponible gratuitement auprès de tous les citoyens. Ceci place le Danemark comme leader mondial de la signature électronique pour le gouvernement en ligne. Il est rapporté que plus de 50 % des Danois utilisent cette signature électronique à chaque mois[148]. Cette signature électronique n'est pas nécessairement conçue expressément pour les besoins des jeunes et leur protection sur Internet. Mais la présence d'une telle infrastructure technologique pourrait inspirer des solutions spécifiques pour les jeunes.

5.2.11 Espagne

Responsabilité et types de régulation

L'Espagne a principalement recours à la corégulation et à la régulation en mode directive.

L'institut de la cinématographie et des arts visuels (Instituto de la Cinematografía y de las Artes Audiovisuales[149]) qui relève du ministère de la Culture, est chargé de classer les films selon un système de classement national. Les classements n'ont qu'une valeur informative, sauf la classe pour les « 18 ans et plus » qui est restrictive. Les communautés autonomes (comme la Catalogne) peuvent réviser ce classement tout en conservant le même système national de classement[150]. Il n'y a pas de loi ou d'organisme gouvernemental qui exerce une régulation du contenu sur Internet.

---

[148] Consulter le document n° 48.2 du Cahier 4 *IT and Telecommunications Policy Report 2006* (p. 21) (http://itst.dk/image.asp?page=image&objno=203180229)

[149] Consulter le site Web de l'institut www.mcu.es/cine/CE/InfGeneral/GestionMinisterio.html

[150] Consulter les documents n° 40.5 *Accord concernant la protection de la jeunesse à la télévision* (www.audiovisualcat.net/decisions/accord117-2004.pdf) et 40.6 *Loi sur la communication audiovisuelle en catalogne* (www.audiovisualcat.net/information/loicatalane.pdf) du Cahier 4 portant sur la régulation de la production audiovisuelle diffusée à la télévision en Catalogne et où le classement des films est réalisé par l'industrie selon un système défini par le gouvernement. Le Conseil de l'audiovisuel de la Catalogue (www.audiovisualcat.net),

Cependant, l'organisme gouvernemental espagnol, Red.es (www.red.es), qui dépend du ministère de l'Industrie, du Tourisme et du Commerce, a pour fonction, outre d'assumer celle de registre du nom de domaine « .es », d'agir comme observatoire des TIC et d'Internet. À cet effet, il publie régulièrement des statistiques sur l'utilisation d'Internet[151]. Il est intéressant de noter qu'une étude sur Internet a été réalisée en 2002 par l'association PROTEGELES, pour le compte de l'instance gouvernementale *Défense des mineurs de la communauté de Madrid* (DEFENSOR DEL MENOR - www.dmenor-mad.es). Cette étude présente des statistiques sur l'usage d'Internet par les jeunes (10 – 17 ans), dégage des problèmes majeurs et propose des pistes de solution en fonction du contexte de l'Espagne. Cette étude a servi de base aux actions de toutes les parties prenantes relatives à la protection de la jeunesse et de son contenu[152].

De plus, en 2005, toutes les parties prenantes de la société de l'information, y incluant les instances gouvernementales, ont signé une déclaration[153] déterminant les objectifs en ce qui a trait à l'évolution de la régulation du contenu audiovisuel :

- respect obligatoire de la législation nationale et internationale (Directive communautaire de la Télévision sans Frontières[154]) et, plus particulièrement, sur tout ce qui se rapporte à la « protection, la promotion et la défense » des

---

propose une autorégulation de l'industrie en matière de contenu audiovisuel. Ce conseil dispose cependant d'une loi (www.audiovisualcat.net/information/loicatalane.pdf) qui permet d'encadrer cette autorégulation incluant, notamment, la protection des mineurs et de pouvoir sévir, le cas échéant. Un système de classification des films y est indiqué. Cependant, ce Conseil ne se préoccupe pas de la diffusion audiovisuelle sur Internet. En Andorre (Conseil de l'audiovisuel de l'Andorre - www.caa.ad/eng/index.html) et en Navarre (Conseil de l'audiovisuel de Navarre (www.consejoaudiovisualdenavarra.es), le gouvernement a la mission de s'assurer, notamment, que les droits des minorités et des mineurs sont respectés mais n'exerce pas de rôle de régulation directe dans le contenu audiovisuel sur Internet.

[151] Pour plus de détails sur les nombreuses études sur l'utilisation et les dangers d'Internet, consulter les documents n° 40.7 *Profil d'utilisation d'Internet* (http://observatorio.red.es/estudios/documentos/magnitudes_sociodemograficas_sep.pdf) et 40.8 *Profil comparatif de l'utilisation d'Internet* (http://observatorio.red.es/estudios/documentos/uso_perfil.pdf) du Cahier 4 et le site Web de Red.es (www.Red.es) pour consulter les autres études.

[152] Consulter le document n° 40.1 du Cahier 4 *Étude sur l'utilisation d'Internet par les mineurs* (www.protegeles.com/internet.doc)

[153] Consulter le document n° 40.2 du Cahier 4 *Déclaration de Madrid* (www.protegeles.com/internet.doc)

[154] Il est à noter qu'une proposition de révision de la Directive (déc. 2005) est en cours d'examen (voir http://europa.eu/scadplus/leg/fr/lvb/l24101.htm). Cette révision vise à moderniser les règles existantes de manière à tenir compte de l'évolution technologique et commerciale du secteur audiovisuel européen. Elle propose, notamment, d'opérer une distinction entre les services "linéaires" (télévision traditionnelle, Internet, téléphonie mobile) et "non linéaires" (télévision et informations à la demande) mais de soumettre tous les services de contenu audiovisuel à des obligations fondamentales (notamment la protection des mineurs et de la dignité humaine).

droits de l'enfant et de l'adolescent de la part des États mais également des entreprises privées;

- création d'un Conseil de l'Audiovisuel à niveau étatique, indépendant, de composition plurielle, chargé de contrôler le respect de la législation tout en pouvant appliquer des mesures répressives. Un Conseil qui renforcerait l'autorégulation, défendrait la liberté d'expression, protégerait les enfants et qui serait à l'écoute des citoyens;
- mise en place d'un plan d'éducation concernant les technologies de l'information, particulièrement auprès des enfants, adolescents et adultes dans l'entourage scolaire et familial, et intégration de cette éducation dans les programmes scolaires;
- renforcement d'une politique de communication de la part des gouvernements garantissant, entre autres, la production et la diffusion de contenus de qualité pour les enfants, incluant la mise en place de programmations spécifiques pour eux, découpées par tranches d'âge, qui permettent l'amélioration du respect des droits des jeunes garçons, des jeunes filles et des adolescents dans ce domaine.

1.a DNS

L'Espagne a recours à des logiciels de filtrage et donc utilise le DNS.

1.b Serveurs racine

Pas d'utilisation des serveurs racine pour gérer le contenu d'Internet.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

L'Espagne a recours au multilinguisme pour ce qui est du contenu pour soutenir, entre autres, la langue espagnole.

2.a Création du contenu – catégorisation

L'Espagne n'effectue pas de catégorisation particulière du contenu des sites Web.

2.b Création du contenu – classement

L'Espagne n'effectue pas de classement du contenu des sites Web. Cependant, comme nous le verrons ci-après, elle offre une possibilité d'homologation des sites Web espagnols.

2.c Contrôle du contenu - homologation

L'Espagne, par le biais de l'agence Internet Quality Agency (IQUA – www.iqua.net), s'est dotée d'un organisme qui fait la promotion de l'autorégulation[155] par la certification, sur une base volontaire, des sites Web espagnols. Cette agence est composée de milliers de membres, propriétaires de sites Web espagnols désirant obtenir le sceau de qualité de l'IQUA et ainsi certifier leurs sites Web. Chaque analyse de qualité de site Web coûte à son propriétaire environ 250 $. La certification, attribuée pour un an, est basée sur un ensemble de règles décrites dans un code de conduite[156] et portant, notamment, sur les éléments suivants :

- Respect de la loi espagnole sur les « Services de la société de l'information et le Commerce électronique »;
- Protection des mineurs;
- Discrimination.

2.d Contrôle du contenu – filtrage

L'association espagnole des mères et pères internautes (AEMPI) recommande l'utilisation de deux logiciels de filtrage : **CANGURONET** commercialisé par Telefónica et celui de la firme espagnole **OPTENET**.

---

[155] Consulter le document n° 40.3 du Cahier 4 décrivant quelque peu les activités de l'IQUA *Introduction à l'IQUA* (www.iqua.net/Quality_seal/Explanation/?go=WWiW6aWP3cIUyUj7fiM3LUP2TCqO0m3NphIdSAiqOiarm/tZ3hXnGk01).

[156] Consulter le document n° 40.4 du Cahier 4 *Critères de l'IQUA* (www.iqua.net/Codes_of_conduct/Code_of_conduct/?go=WWiW6aWP3cIUyUj7fiM3LUP2TC6K0m3NphIdSAiqOiapl/pU2RbkFEc8)

2.e Contrôle du contenu – lutte à la cybercriminalité et

2.g Pédagogie

Ces deux aspects, soit la lutte à la cybercriminalité et la pédagogie visant à l'alphanétisation, sont très imbriqués en Espagne, comme d'ailleurs dans plusieurs autres pays, et seront abordés simultanément.

L'Espagne, par le biais de Safenet, fait partie du réseau européen INHOPE, de cybersurveillance et de cybersignalement. C'est PROTEGELES, association visant à dénoncer la pornographie infantile sur Internet (www.protegeles.com/historiayobj.asp), qui fait office de nœud espagnol du réseau INHOPE de cybersignalement. Cette association a été fondée par la firme OPTENET et l'association ACPI. PROTEGELES exerce son rôle en collaboration avec la firme Terra Networks, qui est le plus grand fournisseur d'accès Internet en Espagne.

L'association PROTEGELES a ceci de particulier par rapport au réseau INHOPE, c'est qu'il a ajouté des objets particuliers de surveillance et de signalement, soit :

- le cyberharcèlement (ou cyber-bullying) avec un site Web spécifique (www.acosoescolar.info);
- la cyberapologie de l'anorexie et de la boulimie (www.masqueunaimagen.com);

tout en ajoutant des fonctions d'éducation et de sensibilisation.

PROTEGELES réalise son travail en collaboration avec plusieurs organisations espagnoles, dont :

- Association espagnole des mères et pères internautes - Asociación Española de Madres y Padres Internautas (**AEMPI -** www.aempi.com), qui a pour mission de faire d'Internet un espace plus sûr et pratique pour les enfants. Elle est membre associé du ECPAT - International (End Child Prostitution, Child Pornography and the trafficking of Children for sexual purpose - Mettre fin à la prostitution enfantine, la pornographie enfantine et le trafic d'enfants à des fins sexuelles)**;**
- Ministère de l'Industrie et du Commerce de l'Espagne dont dépend l'organisme « Red.es »;
- Défense des mineurs de la communauté de Madrid (www.dmenor-mad.es) DEFENSOR DEL MENOR (Défense du mineur de la communauté de Madrid);
- Association « Action contre la pornographie infantile » (ACPI - ACCION CONTRA LA PORNOGRAFIA INFANTIL www.asociacion-acpi.org/queesacpiespanol.htm);

- La firme OPTENET, qui produit le logiciel de filtrage (www.optenet.com).

D'autres organismes participent au rôle de protection des mineurs sur Internet, tels que :

- Observatoire des contenus télévisuel et audiovisuel (Observatorio de Contenidos Televisivos y Audiovisuales – OCTA - www.iniciativaocta.org/modules.php?name=Portada) : organisme de la société civile ayant comme mission de garantir les droits de l'enfance et de la jeunesse dans leur relation avec les différents médias et systèmes de communication;
- Site de sensibilisation et d'éducation destiné aux mineurs (www.portaldelmenor.es) ou aux parents (www.ciberfamilias.com).

2.f Lutte au pollupostage

L'Espage respecte la directive européenne contre le pollupostage.

3.a Liberté d'expression

La liberté d'expression constitue un des principes fondamentaux dans la gouvernance d'Internet en Espagne.

3.b Protection des données et de la vie privée

L'Espagne respecte le principe de la protection de la vie privée comme tout autre pays membre de l'Union européenne.

3.c Gestion de l'identité et authentification

L'Espagne n'offre pas de services de gestion de l'identité et d'authentification destinés aux jeunes.

5.2.12 France

Responsabilité et types et moyen de régulation

La gouvernance du contenu audiovisuel sur Internet en France, à des fins de protection de la jeunesse, a recours principalement à la corégulation et à la régulation en mode directive.

La France dispose d'un organisme de classification des films destinés à leur exploitation en salle, soit la Commission de classification des œuvres cinématographiques, faisant partie du Centre national de la Cinématographie (CNC) lui-même rattaché au ministère de la Culture. Elle ne traite pas la production audiovisuelle sur Internet.

Cependant, le gouvernement français a élaboré un ensemble de mesures destinées à protéger la jeunesse du contenu audiovisuel potentiellement nocif sur Internet. Ces mesures entraînent la participation des trois parties prenantes concernées, soit les différents ministères du gouvernement français (y incluant les institutions d'enseignement), le secteur privé (fournisseurs d'accès Internet et producteurs de logiciel de filtrage) et la société civile (enfants, parents et organismes de protection de l'enfance). Certaines de ces mesures s'inscrivent dans un programme européen, notamment celui pour un Internet plus sûr (INSAFE - Internet Safer). Ces mesures peuvent se résumer ainsi :

- Mise à disposition gratuite d'un logiciel de contrôle parental;
- Mise en place d'un « Plan CONFIANCE »;
- Mise en place de mesures de sensibilisation et d'éducation;
- Mise en place de mesures relatives à la téléphonie mobile;
- Lutte au pollupostage;
- Lutte à la cybercriminalité.

1.a DNS

La France a recours à des logiciels de filtrage et donc utilise le DNS.

1.b Serveurs racine

Pas d'utilisation des serveurs racine pour gérer le contenu d'Internet.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

La France a recours au multilinguisme pour ce qui est du contenu cependant elle n'a pas mis en place l'internationalisation des noms de domaine (IDN) pour les sites Web génériques « .fr ».

2.a Création du contenu – catégorisation

La France n'effectue pas de catégorisation de contenu de sites Web.

2.b Création du contenu – classement et

2.c Contrôle du contenu – homologation

La France n'effectue pas de classement de contenu de sites Web. Cependant, elle s'apprête à mettre en place un classement pour le contenu Internet accessible par les mobiles et une homologation de sites Web.

En effet, le gouvernement français a confié à l'organisation **Forum des droits sur Internet** deux rôles portant sur le « label citoyen » et sur la téléphonie mobile. Ce forum est un organisme créé avec le soutien des pouvoirs publics et composé de près de 70 membres provenant d'organismes publics, d'associations de protection de l'enfance et d'entreprises privées. Il a pour mission d'informer le public et d'organiser la concertation entre les pouvoirs publics, les entreprises et les utilisateurs sur les questions de droit et de société liées à Internet. Ces rôles sont :

- **Développement, mise en œuvre et mise à jour d'un « label citoyen »**. Ce label[157], prévu début 2007, permettra de distinguer; parmi les fournisseurs d'accès à Internet et de services en ligne, ceux qui s'engagent pour une plus grande sécurisation des usages. Ce « label citoyen » est destiné à localiser les contenus Web ne présentant pas de risques pour l'enfant, soit une « liste verte » de sites Web. Cela devrait permettre aux parents de

[157] Lire à cet effet l'article de l'UNAF *Familles, fractures et usages numériques : décisions gouvernementales.*. Document n° 34.2 du Cahier 4 (www.unaf.fr/articleimprim.php3?id_article=3865)

repérer facilement sur Internet les services et les contenus sans risque et de désigner les outils, services et contenus en ligne les plus appropriés au public familial et respectueux de la protection de l'enfant;

- Une « **marque de confiance** » sera créée pour distinguer les fournisseurs d'accès ou de services sur Internet qui respecteront une charte de 70 engagements pour la sécurisation d'Internet et le développement de la confiance sur les réseaux;
- **Développement d'une approche de classification des contenus multimédias mobiles** qui a été déposée sous forme de recommandation en octobre 2006[158]. Il est à noter que 66 % des jeunes entre 12 et 17 ans utilisaient un téléphone portable en 2005[159]. Avec l'arrivée des portails multimédia sur les téléphones mobiles et l'ajout récent du nom de domaine générique « .mobi », l'utilisation d'Internet Mobile est exponentielle. Le gouvernement français aura à statuer sur cette recommandation qui comprend, notamment, un système de classification similaire à celui utilisé pour le classement des films par la Commission de classification des œuvres cinématographiques, l'exclusion de la classification du contenu illégal et une proposition d'ajout d'un nouveau nom de domaine générique de premier niveau (gTLD), soit « .kid ». Incidemment, cette proposition de nom générique présente davantage de chances d'être acceptée au niveau international et par ICANN que la proposition de « .xxx ». Elle servirait à produire une « liste verte » de sites Web mais exigerait une gouvernance particulière afin de s'assurer de sa cohérence. Le cheminement de cette proposition sera intéressant à suivre.

2.d Contrôle du contenu – filtrage

Le gouvernement français a mis un accent particulier sur les logiciels de contrôle parental. Depuis 2006, tous les fournisseurs français d'accès à Internet (FAI) proposent un logiciel de contrôle parental gratuit, et ce, conformément à un accord avec le gouvernement français. Des études comparatives ont été réalisées concernant les logiciels de protection des enfants sur Internet[160]. Le logiciel de contrôle parental fonctionne généralement à l'aide de trois profils : **enfant** (moins de 10 ans), **adolescent** (plus de 10 ans) et **adulte**. De plus, l'organisme gouvernemental **Délégation aux usages de l'Internet** (DUI) a conclu un

[158] Consulter le document n° 36 du Cahier 4 *Classification des contenus multimédias mobiles* (www.foruminternet.org/telechargement/documents/reco-CCMM-20061017)
[159] Source : ARCEP – juin 2005
[160] Consulter le document n° 35.1 du Cahier 4 *Tests comparatifs sur logiciels de filtrage* (www.e-enfance.org/cote_parents/soft/test/) ainsi que le document n° 35.2 du Cahier 4 *Tests des logiciels des contrôles parentaux* qui fournit des essais sur un plus grand nombre de logiciels de contrôle parental (www.filtra.info/web/resultats.aspx?nav=3)

accord avec l'organisation sans but lucratif **Action Innocence**, qui a pour but de protéger les enfants mineurs des aspects négatifs d'Internet afin de lui permettre, notamment, de continuer à publier régulièrement une évaluation comparative des solutions de filtrage disponibles pour les particuliers et les entreprises[161]. Enfin, un accord a été conclu avec l'université de Toulouse 1 afin d'établir une « liste rouge » des sites Web pornographiques et un autre accord avec le programme européen INSAFE permettant d'établir une « liste rouge » des sites Web racistes.

Cependant, tel que souligné par les autorités françaises, il est important de rappeler que la meilleure sécurité pour les enfants réside dans le dialogue avec eux. Aucun logiciel de contrôle parental n'assurera une sécurité totale, et les enfants ont tendance à les contourner. Le logiciel de contrôle parental doit seulement être considéré comme un outil d'aide dans l'éducation sur Internet.

2.e Contrôle du contenu – lutte à la cybercriminalité

La France a mis en place un processus de signalement de sites Web par le biais d'un réseau de points de contact sur tout le territoire français. Ces points de contact sont concentrés autour de trois pôles :

- **Association des fournisseurs d'accès et de services internet** (AFA)[162], membre du réseau INHOPE. L'objectif du point de contact de l'AFA est :
  - d'aider l'internaute à identifier les sites potentiellement illégaux en matière de pornographie enfantine et d'incitation à la haine raciale et les acteurs qui peuvent recevoir le signalement ou la plainte;
  - d'obtenir la suppression des contenus illégaux en les transmettant, en fonction de leur localisation, soit à leur hébergeur membre de l'AFA soit à un « point de contact » du réseau INHOPE;
  - de permettre aux autorités répressives de réaliser rapidement des enquêtes, en signalant le contenu potentiellement illégal aux services de police français ou à un « point de contact » du réseau INHOPE, qui prend le relais avec ses propres autorités de police.
- **Délégation aux usages de l'Internet** (DUI), organisme du gouvernement français, qui permet aux internautes de signaler à partir du site Web de la DUI[163], tous contenus de pédophilie;
- **Fournisseurs d'accès Internet** (FAI) et **hébergeurs**. Depuis la *Loi pour la confiance dans l'économie numérique* du 21 juin 2004[164], ils doivent rendre

[161] Consulter le document n° 35.2 du Cahier 4 *Tests des logiciels des contrôles parentaux* (www.filtra.info/web/resultats.aspx?nav=3)
[162] Consulter le site Web de l'AFA (www.pointdecontact.net)
[163] Consulter le site Web www.internet-mineurs.gouv.fr

disponible un dispositif permettant à toute personne de porter à leur connaissance les infractions d'apologie des crimes contre l'humanité, d'incitation à la haine raciale ainsi que de pornographie enfantine.

2.f Lutte au pollupostage

La France dispose de lois permettant de se prémunir contre les courriels non sollicités[165]. De plus, la France est soumise à la directive européenne contre le pollupostage, soit « Vie privée et communications électroniques ».

La France a mis en place l'association « Signal Spam » (www.signal-spam.fr) qui réunit la plupart des associations françaises concernées par la lutte contre le pollupostage ainsi que des ministères du gouvernement français et des firmes privées. L'association, par le biais de son site Web vise les objectifs suivants :

- Fournir des informations permettant de se prémunir du pollupostage;
- Fournir un lieu de signalement de pollupostage;
- Fournir un lieu pour se désabonner (opt-out) des listes de diffusion connues.

2.g Pédagogie

Le gouvernement français, en collaboration avec les autres parties prenantes ont mis en place le « Plan CONFIANCE » (CONFiance dans un Internet sANs Crainte pour les Enfants), piloté par la DUI, rattachée au ministre de l'Éducation Nationale, de l'Enseignement supérieur et de la Recherche. À cet effet, un site Web rend disponible l'ensemble de la politique gouvernementale en faveur de la protection des mineurs sur

---

[164] Pour plus de détails, consulter la loi apparaissant sur le site Web du *Forum des droits sur Internet* (www.foruminternet.org/documents/lois/lire.phtml?id=733)

[165] *Loi informatique et libertés* du 6 janvier 1978 (article 226-16 et suivants du Code pénal) et de la *Loi relative aux atteintes aux systèmes de traitement automatisé de données* du 5 janvier 1988 (article 323-1 et suivants du Code pénal) voir www.cnil.fr/index.php?id=1534 de la Commission nationale de l'informatique et des libertés. De plus, depuis le 21 juin 2004, la France dispose d'une *Loi pour la confiance dans l'économie numérique*

Internet. Le « Plan Confiance »[166] et la DUI représente le noeud français du réseau européen INSAFE[167].

Ce plan a pour objectif de conduire des actions de sensibilisation auprès des enfants, parents, éducateurs et webmestres « à la sécurité et à la civilité de l'Internet », en impliquant l'ensemble des parties prenantes concernées, dont les institutions d'enseignement, les FAI et les producteurs de logiciels de filtrage (ou de contrôle parental). Ce plan a déterminé un ensemble de dangers à gérer pour mieux protéger les mineurs tels que :

- des contenus violents;
- des images choquantes (1 enfant sur 3 est confronté à des contenus choquants sur le Net[168];.
- des contenus incitant à la haine raciale;
- de la pédopornographie;
- des risques de conditionnement de type sectaire ou idéologique;
- des contenus détournés (sensibilisation sur les pratiques de manipulation des données et des images);
- des pressions psychologiques exercées sur les jeunes par des personnes malintentionnées, mineures ou majeures (incitation à l'anorexie, au suicide ou harcèlement sexuel…);
- des rencontres « clandestines » (les jeunes sont enclins à se rendre à un rendez-vous avec un inconnu à la suite d'un clavardage ou à des jeux en réseau - 1 enfant sur 3 qui clavarde se voit proposer une rencontre physique[169] et 1 enfant sur 12 a réellement rencontré quelqu'un connu d'abord en ligne[170]);
- des blogues diffamatoires[171];
- de la dépendance : notamment aux jeux;
- du pollupostage et des jeux d'argent.

---

[166] Consulter le site Web : www.mineurs.fr/confiance et celui de la Délégation aux usages de l'Internet (rattachée au ministre de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche (MENESR). http://delegation.internet.gouv.fr/confiance

[167] Le programme INSAFE est abordé sous la rubrique « Europe ». Pour plus de détails, consulter leur site Web, soit www.saferinternet.org/ww/en/pub/insafe/focus/france.htm

[168] Consulter le document n° 38.1 du Cahier 4 *Les usages d'Internet par les adolescents* produit par l'IFOP (l'Institut Français d'Opinion Publique) Mars 2005 (www.ifop.com/europe/sondages/opinionf/internetadosv2.asp) Consulter aussi le document n° 38.2 du Cahier 4 *Statistiques sur Internet et enfants* (www.innocenceindanger.org)

[169] Source : Enquête européenne SAFT de mai 2003

[170] Consulter le document n° 38.2 du Cahier 4 *Statistiques sur Internet et enfants*

[171] Près de 4 millions de français sont accros aux carnets Web de Skyrock en 2005 selon *Le Point* – 28 juillet 2005

Le gouvernement français, dans le cadre du « Plan CONFIANCE » a entrepris une importante campagne de sensibilisation auprès des enfants, des parents (Internet à la maison) et des éducateurs (Internet à l'école)[172] au moyen de spots publicitaires à la radio et à la télévision, de dépliants, de guides[173], de conférences et de congrès[174]. Les FAI, à leur tour, se doivent de mettre en œuvre des actions de sensibilisation.

Le secteur privé et, surtout, la société civile, par le biais de ses nombreuses organisations, ont mis en place plusieurs mesures de sensibilisation et d'éducation sur les dangers d'Internet pour la jeunesse, particulièrement par le biais de sites Web.

Mentionnons, entre autres, les sites Web suivants :

- www.decodeleweb.com : site d'éducation aux dangers d'Internet sous la forme d'un site ludique destiné aux jeunes. Sensibilisation au pollupostage, au hameçonnage, au vol d'identité, au harcèlement moral ou sexuel;
- www.e-enfance.org : site de l'association à but non lucratif **E-Enfance** ayant pour mission de permettre aux enfants et adolescents de se servir des nouvelles technologies de communication (Internet, téléphone mobile, jeux en réseau) avec un maximum de sécurité. E-Enfance remplit à la fois un rôle de sensibilisation sur les risques d'Internet et un rôle de conseiller auprès des parents afin de leur permettre d'exercer une autorité en tant que « cyberparent ». Le site fournit notamment une liste de sites Web à des fins ludiques ou pédagogiques pour enfants et adolescents.

Téléphonie mobile

En matière d'Internet par la téléphonie mobile, la France y a investi beaucoup d'efforts. Des actions concertées entre le gouvernement français

[172] Consulter les documents n° 33.1 *La sécurité des mineurs à la maison* (www.ia05.ac-aix-marseille.fr/tice/Fichemineursmaison.pdf), 33.2 *La sécurité des mineurs à l'école* (www.ia05.ac-aix-marseille.fr/tice/Fichemineursecole1.pdf) et 33.3 *Première semaine nationale de la sécurité informatique* (www.protegetonordi.com) du Cahier 4 portant sur la sécurité des mineurs par rapport à Internet.

[173] Consulter les documents n° 34.1 du Cahier 4 *La parentalité à l'ère du numérique* (www.unaf.fr/IMG/pdf/Guide_parents_Unaf_MS-2.pdf) et le document n° 28 du Cahier 4 *Votre enfant et le téléphone mobile* (www.afom.fr/guideparents/Guide_Enfance_20051004.pdf)

[174] Ainsi, en avril 2006, le Congrès *Enfance en ligne – La parentalité à l'ère du numérique* était organisé en collaboration avec divers partenaires privé (Microsoft France) et de la société civile (tels que l'Union Nationale des Associations Familiales - UNAF et le Collectif Interassociatif Enfance et Médias - CIEM). Pour plus de détails, consulter le document n° 33.4 du Cahier 4 *Congrès Enfance en ligne* (www.microsoft.com/france/apropos/enfance-en-ligne/default.mspx)

et les opérateurs de téléphonie mobile ont été prises ou le seront bientôt concernant la lutte à la cybercriminalité, la pédagogie et l'homologation.

Les contenus sensibles étant accessibles par le biais de la téléphonie mobile, une *Charte d'engagements* [175] a été signée, en janvier 2006, entre le gouvernement français et des opérateurs membres de l'Association française des opérateurs mobiles (AFOM) afin de renforcer l'encadrement sur les réseaux mobiles et accentuer la lutte contre les contenus illicites. Cette charte définit les cinq engagements suivants :

- renforcer et harmoniser la démarche déontologique encadrant le développement des contenus multimédias mobiles dans les kiosques et portails;
- informer et proposer de manière systématique aux parents un système gratuit de contrôle parental;
- renforcer la lutte contre les contenus illicites;
- informer le grand public sur les actions menées et participer à l'éducation pour tous aux bons usages de la téléphonie mobile;
- évaluer, informer et consulter régulièrement l'ensemble des parties concernées par cette démarche déontologique.

Cette charte s'appuie sur plusieurs dispositifs :

- l'outil de contrôle parental qui bloque l'accès à certains sites et est activable dès l'ouverture de la ligne;
- l'absence de contenus réservés aux adultes sur le portail des opérateurs;
- la modération des parties publiques des sites de clavardage et de blogues;
- un outil de cybersignalement des contenus susceptibles de porter atteinte à la dignité humaine.

Le gouvernement français, sur la base de la recommandation d'octobre 2006 du *Forum des droits sur Internet*, devrait éventuellement mettre en place le concept de « label citoyen » qui servira aussi à la téléphonie mobile.

3.a Liberté d'expression

La France respecte le principe de la liberté d'expression comme tout autre pays membre de l'Union européenne.

[175] Consulter le document n° 37 du Cahier 4 *Charte d'engagements des opérateurs sur le contenu multimedia mobile* (www.famille.gouv.fr/com_pr/charte_multimedia20060110.pdf)

3.b Protection des données et de la vie privée

La France respecte le principe de la protection de la vie privée comme tout autre pays membre de l'Union européenne.

3.c Gestion de l'identité et authentification

Nous n'avons pas détecté de gestion d'identité ou d'authentification particulière pour la protection de la jeunesse.

5.2.13 Royaume-Uni

Responsabilité et types de régulation

La gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse s'effectue, au Royaume-Uni, principalement au moyen d'autorégulation et de corégulation.

Le Bureau britannique de classification des films (**British Board of Film Classification** - **BBFC** - www.bbfc.co.uk/about/index.php), organisme indépendant non gouvernemental, classifie, selon une loi britannique, les films, vidéo, DVD ainsi que des jeux par ordinateur ou par consoles de jeux. Cependant, le BBFC n'a pas autorité sur le contenu audiovisuel sur Internet, même s'il en a exprimé son intérêt[176].

Pour ce qui est du contenu sur Internet, sans égard au mode d'accès (que ce soit par exemple par « mobile » ou par ordinateur), on se retrouve davantage à un mode d'autorégulation. Ainsi, la centaine de membres de l'Association des fournisseurs de services Internet (**Internet Services Providers' Association ISPA UK** - www.ispa.org.uk) s'engagent, sur une base volontaire, à respecter le code de pratiques de l'association[177]. Mais ce code n'inclut aucune disposition relative à la protection des mineurs, du fait des trois principes suivants qui y sont énoncés :

- Encouragement des technologies permettant le filtrage du contenu mais sans engagement financier;
- Attribution de la responsabilité entière du contenu à l'utilisateur ou au propriétaire du site Web qui fournit ce contenu;
- Reconnaissance de la responsabilité entière au gouvernement pour toute action de filtrage ou de censure.

Cette association remplit son rôle d'autorégulation en plus de celui de promotion de la compétition et du développement de l'industrie d'Internet.

La participation gouvernementale à la gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse s'effectue principalement, outre la lutte à la cybercriminalité qui y occupe une place très importante, au niveau des études sur les usages d'Internet et sur l'éducation des jeunes,

[176] Consulter le document n° 25.4 du Cahier 3 *Who's reading your e-mail* (http://news.bbc.co.uk/1/hi/technology/5132512.stm)
[177] Consulter le document n° 44.1 du Cahier 4 *ISPA Code of practice* (www.ispa.org.uk/about_us/page_16.html)

de leurs parents et de leurs éducateurs à ces usages, à leurs périls et aux façons d'y faire face. Cette éducation est généralement assez imbriquée dans la lutte à la cybercriminalité de façon à permettre aux jeunes, aux parents et aux éducateurs de savoir quoi faire lorsqu'il se produit des situations qui exigent de faire appel à de l'aide qui est soit du ressort du cybersignalement (comme pornographie infantile ou la séduction - « grooming ») soit du soutient social ou psychologique (comme l'intimidation ou l'accès à du contenu non approprié à un jeune public). Les organismes gouvernementaux, par le financement accordé à des initiatives de protection de la jeunesse, influencent l'industrie d'Internet.

Ainsi, l'organisme gouvernemental **Home Office** (www.homeoffice.gov.uk) joue un grand rôle dans la protection de la jeunesse concernant la lutte à la cybercriminalité et l'éducation à l'utilisation d'Internet. Il présente d'ailleurs une page de son site Web une liste assez exhaustive des outils et références pour protéger les mineurs[178].

De même, l'Office des communications (**Office of Communications - OFCOM** - www.ofcom.org.uk), organisme de régulation gouvernemental[179] ayant autorité en matière de compétition concernant l'industrie des communications au Royaume-Uni (télévision, radio, télécommunications et services de communication sans fil), a approuvé le Code de pratiques élaboré pour ce secteur par l'**Independent Committee for the Supervision of Standards of Telephone Information Services** (**ICSTIS** - www.icstis.org.uk), régulateur indépendant financé par l'industrie sur les services tarifés en télécommunications. L'OFCOM ne couvre pas directement le contenu sur Internet accédé par la téléphonie mobile mais il réalise des études et observations sur l'alphanétisation des utilisateurs auprès des enfants et des parents. Le Code de pratiques sur les services tarifés de télécommunications comporte des dispositions permettant à l'ICSTIS de forcer son respect dans le cas de déviation. Ce code de pratiques fortement orienté vers la protection des consommateurs comporte quelques considérations concernant le contenu où il est requis d'exclure tout matériel ou services incitant à la violence, de nature répulsive, utilisant un langage grossier ou causant des préjudices graves. Ce code ne comprend aucune exigence de catégorisation ou d'étiquetage des services.

Aussi, afin de compléter la régulation du contenu accessible sur Internet par téléphone mobile, le gouvernement britannique et le secteur privé, ont

[178] Consulter le document n° 44.2 du Cahier 4 *Politique opérationnelle et protection des mineurs* (http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce?version=4)

[179] Selon selon l'article121 du *Communications Act 2003*

développé un système de classification du contenu par le biais de l'Independant Mobile Classification Body (IMCB - www.imcb.org.uk). L'IMCB offre de l'aide pour l'application de ce système de classification du contenu audiovisuel disponible sur les « mobiles » (cela peut inclure d'autres appareils que les téléphones mobiles). Le système de classification a été établi conformément au Code de pratique britannique d'autorégulation des nouvelles formes de contenu sur les « mobiles » (UK Code of Practice for the self-regulation of new forms of content on mobiles) publié par les opérateurs de mobiles en janvier 2004. Le système de classification retenu est binaire. Il s'agit de déterminer tout contenu réservé ou non aux 18 ans et plus[180]. Le contenu couvert comprend :

- Images fixes;
- Matériel audiovisuel et video;
- Jeux pour mobiles, incluant les jeux basés sur Java.

Le système de classification demeure compatible avec celui utilisé pour les films au Royaume-Uni, du moins pour la catégorie « 18 ans et plus ». De plus, le système de classification comprend des critères explicatifs additionnels (tels que les thèmes, le niveau de langage, le sexe, la nudité, la violence et les drogues).

Cependant, ce système de classification exclut plusieurs contenus et services dont ceux couverts par l'ICSTIS, le contenu généré par les abonnés, incluant les blogues ainsi que le contenu accédé par Internet où l'opérateur de « mobiles » ne fournit qu'un service de connexion[181]. Dans ce dernier cas, l'industrie du « mobile » se fie sur la sensibilisation de la communauté et la disponibilité éventuelle de technologies de filtrage afin de protéger la jeunesse de matériel inapproprié. Chaque fournisseur de contenu est responsable de classifier lui-même son contenu « 18 ans et plus ou non » selon cette structure de classement. Mais l'IMCB ne dispose d'aucun pouvoir légal pour renforcer le système de classification dans le cas de dérogations[182].

---

[180] Consulter le document n° 44.6 du Cahier 4 *Système de classification du contenu pour téléphonie mobile* (www.imcb.org.uk/assets/documents/ClassificationFramework.pdf)

[181] Les exclusions comprennent :

- Services texte, audio et voix, incluant ceux tarifés et régulés par l'ICSTIS;
- Services de pari;
- Salles de clavardage modéré ou non (les salles de clavardage commerciales non modérées sont réservées aux 18 ans et plus);
- Services basées sur de la location, qui sont assujettis à un autre code de pratiques;
- Contenu généré par les abonnés, incluant les carnets Web;
- Contenu accédé par Internet ou WAP où l'opération de téléphonie cellulaire ne fournit qu'un service de connexion.

[182] Consulter le document n° 16 du Cahier 3 *Final Convergent Devices Report* (www.dcita.gov.au/__data/assets/pdf_file/39890/Final_Convergent_Devices_Report.pdf)

Il est intéressant de noter qu'en Europe, une consultation est en cours sur la téléphonie mobile et que Childnet International a produit un avis très étoffé sur les différentes questions soulevées par la téléphonie mobile et la protection des mineurs[183].

Le Ministère du Commerce et de l'Industrie du Royaume-Uni (Department of Trade & Industry - www.dti.gov.uk), bien qu'il possède un rôle d'aide au développement de l'industrie d'Internet, offre souvent son soutien financier pour la réalisation d'études et d'éducation en ce qui a trait à la protection de la jeunesse.

1.a DNS

La technologie du filtrage est utilisée au Royaume-Uni et donc le DNS est mis à contribution. De plus, des initiatives privées d'authentification en cours au Royaume-Uni font appel au DNS.

1.b Serveurs racine

Ils ne sont pas utilisés pour la protection de la jeunesse.

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

Le Royaume-Uni a recours au multilinguisme pour ce qui est du contenu.

2.a Création du contenu – catégorisation

[183] Consulter le document n° 44.8 du Cahier 8 *A response by Childnet international to the European Commission public consultation on the protection of minors using mobile phones* (http://europa.eu.int/information_society/activities/sip/docs/public_consultation/results/childnet_international_a337660.pdf)

Partielle par le biais de la catégorisation de certains contenus Internet accessibles par les « mobiles ».

2.b Création du contenu – classement

Partielle par le biais du classement de certains contenus Internet accessibles par les « mobiles ».

2.c Contrôle du contenu - homologation

Aucune initiative d'homologation n'a été détectée.

2.d Contrôle du contenu – filtrage

Sur une base volontaire, il est prévu, par le Home Office, qu'à la fin de 2007, tous les FSI offrant la connexion à Internet à large bande va avoir mis en oeuvre des mesures techniques (particulièrement basées sur les filtres) pour empêcher l'accès à des images d'abus d'enfants[184].

Ainsi, un FSI a décidé d'offrir récemment un service de filtrage à tous ses abonnés à Internet à large bande[185] qui comporte, notamment, une préoccupation concernant la protection de la jeunesse. Son service a déjà catégorisé le contenu de près de 10 millions de domaines selon une cinquantaine de rubriques. Il est impossible cependant, de pouvoir apprécier la qualité de cette catégorisation.

2.e Contrôle du contenu – lutte à la cybercriminalité

La cybersurveillance englobe plusieurs domaines de préoccupation dont celui relatif à la pornographie et particulièrement la pornographie infantile. Le Royaume-Uni a complété la loi européenne pour prendre en charge cette question particulièrement exacerbée sur Internet.

La cybersurveillance et le cybersignalement sont des activités de gouvernance très importantes au Royaume-Uni. Elles sont dirigées ou

[184] Consulter le document n° 25.4 du Cahier 3 *Who's reading your e-mail* (http://news.bbc.co.uk/1/hi/technology/5132512.stm)
[185] Consulter le document n° 44.10 du Cahier 4 *Service de filtrage Cleanfeed* (www.cleanfeed.co.uk)

soutenues autant de la part d'organismes gouvernementaux que par des organismes de la société civile.

Le Royaume-Uni est membre du réseau européen **INHOPE**.

Du côté gouvernemental, le **Home Office** exerce un rôle majeur qui est à la fois de cybersurveillance et d'alphanétisation. Il dispose en son sein d'une unité spécifique à Internet, soit l'**Internet Task Force** (ITF). Il supporte, par exemple, des sites Web d'éducation / cybersurveillance comme WebSafe Crackers et des projets tels que le projet Internet Safety Content Agent (ISCA) décrit plus loin. Il prévoit, tel que mentionné précédemment la disponibilité, de la part des FSI offrant la connexion à Internet à large bande, de mesures techniques pour empêcher l'accès à des images d'abus d'enfants[186].

L'autre organisme, celui de la société civile, qui exerce un rôle majeur est la fondation de surveillance d'Internet (**Internet Watch Foundation** - IWF - www.iwf.org.uk/public/page.35.htm)[187]. Cet organisme ne dispose d'aucune autorité légale bien que soutenu par plusieurs ministères du gouvernement du Royaume-Uni. Il collabore avec les organismes d'application de la loi et les fournisseurs de services Internet au Royaume-Uni pour éliminer d'Internet le contenu illégal (particulièrement la pornographie infantile) et promouvoir l'étiquetage et le filtrage du contenu légal que certains peuvent considérer comme offensant[188]. Ainsi, il fournit un « point de contact » pour permettre de rapporter des cas visuels d'abus d'enfants et œuvre avec les corps policiers pour éliminer ces images des sites Web concernés. Évidemment, cet organisme, comme la plupart des organismes de cette nature à travers le monde, œuvre en aval du phénomène, c'est-à-dire une fois que les images abusives sont déjà sur le Web. La gouvernance actuelle mondiale des sites Web ne permet pas de détecter de telles images dès qu'elles sont publiées sur le Web et la gestion de la criminalité mondiale ne permet de contrer la création même de telles images. IWF œuvre donc à minimiser la disponibilité de contenu potentiellement illégal sur Internet concernant les images d'abus d'enfants, le contenu obscène criminel et le contenu incitant à la haine raciale[189].

---

[186] Consulter le document n° 25.4 du Cahier 3 *Who's reading your e-mail* (http://news.bbc.co.uk/1/hi/technology/5132512.stm)

[187] Consulter le document n° 44.9 du Cahier 4 *Internet Watch Foundation* (www.iwf.org.uk)

[188] Consulter le document n° 43.1 du Cahier 4 *Le contenu illégal et offensant diffusé dans Internet* (http://cyberwise.ca/epic/internet/incyby-cybj.nsf/fr/h_uz00054f.html)

[189] IWF joue donc trois grands rôles :

- Favoriser la confiance auprès des utilisateurs d'Internet;
- Assister les FSI pour éviter l'utilisation de leurs systèmes pour la propagation de contenu criminel et ce, selon le Memorandum of Understanding concerning Section 46 Sexual Offences Act 2003;

Un autre organisme de la société civile important est l'unité de recherche sur Internet de l'université Lancashire (**Cyberspace Research Unit** du Department of Forensic and Investigative Science à University of Central Lancashire **UCLAN/CRU** - www.fkbko.co.uk). Sa mission est double :

- Fournir aux enfants et jeunes personnes des outils, connaissance et habiletés nécessaires pour naviguer de façon sûre sur Internet;
- Explorer la façon dont les criminels utilisent Internet et examiner l'impact sur les stratégies d'enquête[190].

Ainsi, le CRU est l'organisation responsable de la participation du Royaume-Uni à la compétition mondiale de « story-telling » « Safer Internet Magic and Friendship » du programme européen du réseau INSAFE.

Il est intéressant de noter une étude, qui apparaît fort originale, réalisée par le *Department of Media and Communications* du London School of Economics and Political Science et commanditée[191] par plusieurs organismes britanniques concernant le contenu illégal et l'éducation des utilisateurs. Elle a permis de dégager des informations intéressantes concernant les quatre sujets suivants :

- Accès, inégalités et fracture numérique;
- Formes indésirables de contenu et de contact;
- Éducation, apprentissage informel et alphanétisation;
- Communication, identité et participation[192].

Certains des résultats confirment d'autres études ou fournissent un éclairage différent sur les usages d'Internet par la jeunesse (9-19 ans) de la part d'une société qui peut ressembler beaucoup à celle du Québec :

- Plus de 50 % des jeunes ont vu de la pornographie en ligne;
- La plupart de la pornographie est vue par accident (pop-up, recherche d'autre chose ou pollupostage);

- Participer au renforcement de la loi dans la lutte contre le contenu criminel sur Internet.

[190] Consulter le document n° 1 du Cahier 3 *Insafe* (www.saferinternet.org/ww/en/pub/insafe/focus/uk/uk_node_info.htm#target)
[191] Cette étude était principalement commanditée par une subvention du Economic and Social Research Council dans le cadre du *e-Society Programme*, et de la participation financière des organisations suivantes : AOL UK, BSC, Childnet-International, Citizens Online, ITC and Ofcom.
[192] Consulter le document n° 44.7 du Cahier 4 *UK Children Go Online Report* (http://personal.lse.ac.uk/bober/UKCGOfinalReport.pdf)

- Près de 50 % des jeunes de 18-19 qui ont vu de la pornographie sont d'avis qu'ils étaient trop jeunes lorsqu'ils en ont vu pour la première fois;
- Près de 25 % ont accédé par accident à des images violentes ou dégradantes et 9 % à des sites hostiles ou haineux;
- Près de 50 % ont fourni leur information d'identification personnelle à quelqu'un rencontré en ligne;
- Les parents sous-estiment les expériences négatives des enfants : les enfants ont reçu du contenu sexuel non sollicité ou ont fait l'objet de menaces dans une proportion de 31 %[193] et 33 % respectivement alors que les parents pensent que ce pourcentage n'est que de 7 % et 4 % respectivement;
- 63 % des enfants (12-19 ans) ont pris des actions pour cacher de leurs parents leurs activités en ligne.

Le rapport comprend un ensemble d'actions proposées dont :

Du côté des parents :

- Régulation plus stricte concernant les lois relatives à la pornographie en ligne et les services en ligne;
- Davantage d'éducation tant dans les écoles que pour les parents;
- Meilleur contenu destiné aux enfants;
- Technologie améliorée concernant les logiciels de filtrage, de contrôle parental et de surveillance.

Du côté des jeunes :

- Meilleur contenu conçu pour eux;
- Sites interactifs qui interagissent à leurs contributions;
- Meilleure aide pour la création de contenu[194];

---

[193] Plusieurs études confirment le chiffre de 30 à 33 % des enfants ou jeunes qui ont été en contact avec du contenu pornographique non désiré. Voir notamment à la page 22 du document n° 3 du Cahier 3 *Projet de résolution législative du parlement européen concernant la protection des mineurs* où une étude en Europe du Nord est relatée (www.europarl.europa.eu/meetdocs/2004_2009/documents/pr/558/558297/558297fr.pdf).

[194] Ce besoin exprimé par les jeunes confirme la tendance du Web participatif où l'utilisateur devient un coproducteur de contenu. L'article sur les blogues texte, vidéo ou mobile du programme Safe Internet (www.saferinternet.org/ww/en/pub/insafe/news/articles/0106/uk.htm) renforce cette tendance où il est mentionné que les jeunes sont de plus en plus des consommateurs, créateurs et producteurs de contenu. De plus, à la suite d'une étude au Royaume-Uni, il ressort qu'environ 33 % des jeunes publient du contenu sur les blogues ou sur des sites

- Meilleure protection de contenu non sollicité;
- Meilleure considération de leurs besoins de protéger leur vie privée, incluant de la part de leurs parents.

2.f Lutte au pollupostage

Le Royaume-Uni, comme les autres pays de l'Union européenne, lutte contre le pollupostage. Il a mis sur pied le Plan d'action de Londres (*London Action Plan* – LAP - www.londonactionplan.org/?q=node/22) afin de promouvoir la coopération internationale contre le pollupostage et ses problèmes connexes à la cybercriminalité (tels que la fraude en ligne, l'hameçonnage ou « phishing » et la propagation de virus).

Le Plan d'action de Londres a été adopté par 62 agences de lutte antipourriel dans plus de 30 pays, dont les États-Unis, la Chine et le Canada (par le biais de Industrie Canada et du Commissariat à la protection de la vie privée du Canada). Ces agences oeuvrent à la protection de la vie privée, à la protection des consommateurs ou à la réglementation des télécommunications. De nombreuses sociétés d'envergure internationale ont également rejoint le Plan.

Les activités concrètes du Plan d'action de Londres peuvent être résumées ainsi :

- **Sensibilisation** des grandes entreprises et des FAI à travers le monde, notamment grâce aux opérations d'éducation;
- **Échange de bonnes pratiques** pour identifier les origines des pourriels reçus, par l'intermédiaire de conférences périodiques;
- **Facilitation et mise en place de procédures de coopération** entre les régulateurs et l'industrie et ce, notamment en collabaration avec le réseau européen des autorités antipourriel, le Contact Network of Spam Authorities - CNSA;
- **Opérations conjointes** de lutte antipourriel telles que le « Global Spam Sweep » (février 2005), en association avec le réseau international de protection des consommateurs (ICPEN)[195].

Web (d'après le document n° 7 du Cahier 3 *First global 'blogathon' for safer internet* - www.saferinternet.org/ww/en/pub/insafe/news/insafe20060118.htm et www.saferinternet.org/shared/data/saferinternet.org/blogathon/organisations_events%20060126.pdf).

[195] Lors de cette opération, les participants ont étudié plus de 130 000 courriels circulant lors d'une journée spécifique, et ont échangé des informations sur l'origine du pourriel reçu. À la suite de cet exercice, plus de 3 000 enquêtes approfondies ont été lancées contre les pourriels les plus sérieux

2.f Pédagogie

Le Royaume-Uni a recours à plusieurs approches de sensibilisation et de formation à l'utilisation d'Internet, à ses périls et aux façons d'y faire face. Il est intéressant de constater que s'il est sensible aux périls et donc à ses risques, il essaie aussi de les contrebalancer avec les possibilités énormes que représente Internet pour la jeunesse.

Le Royaume-Uni participe au programme « Safer Internet » qui soutient deux réseaux à l'échelle nationale :

- Hotlines : pour signaler le contenu illégal sur Internet. Réseau soutenu par le Internet Watch Foundation (www.uk.inhope.org);
- Nœud de sensibilisation : pour réaliser des actions d'information sur l'utilisation sûre d'Internet. Ce réseau est soutenu par l'University of Central Lancashire (UCLAN) (www.internetsafetyzone.co.uk).

On retrouve l'organisation sans but lucratif de la société civile Childnet International (www.childnet-int.org) qui vise à rendre Internet une « place formidable et sûre pour les enfants ». Elle intervient sur les trois sujets suivants :

- Accès : par la promotion du contenu de qualité et de l'utilisation d'Internet de façon constructive;
- Sensibilisation : en aidant les enfants à acquérir les habiletés d'alphanétisation et en fournissant des conseils à l'industrie, aux organisations et aux enseignants concernant la sûreté sur Internet et les « mobiles »;
- Protection et politique : en aidant à protéger les enfants de leur exploitation sur les environnements en ligne et en prenant l'initiative des changements de politiques afférentes.

La Commission européenne finance présentement le **projet Internet Safety Content Agent** (**ISCA**)[196] dirigé par Cyberspace Research Unit (CRU) de University of Central Lancashire (UCLAN) en partenariat avec le Home Office Internet Task Force (HO ITF – sous-groupe G – Public

[196] Consulter le site Web de l'UCLAN : www.uclan.ac.uk/host/cru/isca_overview.htm et le document n° 44.2 du Cahier 4 *Politique opérationnelle et protection des mineurs* (http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce)

Awareness)[197]. Ce sous-groupe, présidé par le CRU, comprend des membres du secteur de l'éducation, des organismes relatifs aux enfants, des agences gouvernementales, des fournisseurs de services Internet et de téléphonie mobile. L'objectif du projet est d'augmenter les niveaux de sensibilisation et d'éducation à la sûreté sur Internet auprès de clientèles variées et particulièrement les enseignants, les parents et les jeunes gens.

Ce projet a ceci de particulier : il vise à fournir, sans frais pour les fournisseurs de contenu ou de services, du matériel de sensibilisation par le biais d'un réseau de sites Web de tierce partie afin d'atteindre une couverture maximale, plutôt que par le biais d'un seul site Web. Ce projet apparaît très structurant et fédérateur pour toutes les activités de sensibilisation et de formation reliées à la protection des mineurs lors de leur navigation sur Internet[198].

Un autre projet, soit COMPANIONS (www.oii.ox.ac.uk/research/project.cfm?id=4), vient de débuter en novembre 2006. Il est dirigé par l'Oxford Internet Institute (www.oii.ox.ac.uk), organisme qui réalise des études périodiques sur l'utilisation d'Internet. Ce projet vise, à terme, à offrir un environnement d'accès au Web personnalisé selon l'utilisateur, en langue naturelle, et dont une version pourrait éventuellement être développée par la suite pour la jeunesse.

Il existe plusieurs autres sites Web oeuvrant à la sensibilisation et l'éducation aux dangers d'Internet. En voici quelques uns :

- Chat Danger : www.chatdanger.com - site Web géré par Childnet International, qui offre de la sensibilisation sur les dangers possibles des services interactifs en ligne tels que le clavardage, la messagerie instantanée, les jeux, le courriel et les mobiles;
- Kidsmart : www.kidsmart.org.uk - site Web géré par Childnet International qui offre un programme pratique de sûreté d'Internet destiné aux enfants, aux enseignants et aux parents;

---

[197] Consulter le document n° 44.2 du Cahier 4 *Politique opérationnelle et protection des mineurs* (http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce)

[198] Ce projet, à terme, devrait produire les éléments suivants :
- Ensemble cohérent de matériel approuvé relatif à la sûreté sur Internet;
- Site Web central permettant de télécharger ce matériel et indiquant les firmes ou sites Web expérimentant ou utilisant déjà ce matériel;
- Outils de promotion du matériel;
- Réseau établi de « formation des formateurs » (train the trainers) auprès des éducateurs et des parents;
- Détermination des différentes activités, campagnes, projets entourant la sûreté sur Internet à travers tout le Royaume-Uni.

- Think U Know : www.thinkuknow.co.uk - site Web géré par le Child Exploitation and Online Protection (CEOP) Centre qui fournit des informations sur la façon de se protéger sur Internet;
- Le Child Exploitation and Online Protection (CEOP : www.ceop.gov.uk - membre du Virtual Global Taskforce. Tient des ateliers sur les risques à utiliser les réseaux sociaux (http://publicaffairs.linx.net/news/?cat=10) tels que MySpace, Bebo et Facebook.;
- BBC Chat Guide : www.bbc.co.uk/chatguide - site Web dédié au clavardage destiné aux enfants, adolescents, parents et enseignants;
- NetSmartz : www.netsmartz.org - site Web du **National Center for Missing & Exploited Children**;
- WebSafe Crackers : (www.websafecrackerz.com/bbb.aspx) supporté par Microsoft, Internet Watch Foundation, Home Office, Cyberspace Research Unit, BBC, NSPCC, Virtual Global Taskforce et Childnet International (www.childnet-int.org);
- Internet Safety Zone : (www.internetsafetyzone.co.uk/root/default.htm) : ce site offre aussi aux jeunes et leurs parents la façon pour faire du cybersignalement et ce, pour de nombreux sujets de préoccupations dont l'intimidation, le contenu raciste, l'abus d'enfants.

3.a Liberté d'expression

Le Royaume-Uni respecte le principe de la liberté d'expression comme tout autre pays européen, membre de l'Union européenne.

3.b Protection des données et de la vie privée

Le Royaume-Uni respecte le principe de la protection de la vie privée comme tout autre pays européen, membre de l'Union européenne.

3.c Gestion de l'identité et authentification

Des initiatives tant gouvernementales que privées sont à souligner en ce qui a trait à la gestion de l'identité.

Du côté gouvernemental, le Royaume-Uni est à déployer sa solution d'authentification *UK Government Authentication Gateway*[199] pour l'accès à tous ses services en ligne. Déjà, 8 millions de Britanniques l'ont adopté. Ce n'est pas une solution orientée spécifiquement pour la protection de la jeunesse. Cependant, elle présente toutes les potentialités pour s'y adapter.

Du côté du secteur privé, une firme du Royaume-Uni, Net-ID (www.netidme.com/netidme.asp) offre un nouveau système d'authentification et d'identification dans le contexte du clavardage, particulièrement destiné aux jeunes. Le Net-ID est une carte d'identité électronique sécurisé, genre de passeport électronique, qui affiche seulement le prénom, l'âge, le genre et la localisation générale afin de permettre de vérifier les personnes avec lesquelles on clavarde. Ce système, additionné du logiciel ChatShield (www.chatshield.com), offre une façon sûre de clavarder, avec Messenger par exemple, avec les personnes dont l'identité a été assurée et permet entre autres, d'éviter le piège du jeune qui se retrouve à clavarder avec un inconnu adulte qui usurpe l'identité d'un enfant par exemple. Les parents peuvent aussi intervenir pour établir la liste de contacts permis. Ce nouveau service, unilingue anglais pour le moment, apparaît cependant dispendieux[200]. Actuellement, ce système est offert dans 4 pays, soit le Royaume-Uni, le Canada, l'Australie et les États-Unis. Il est cependant prévu une version multilingue au début de 2007.

---

[199] Le gouvernement du Royaume-Uni vient de recevoir le prix de la meilleure initiative 2006 à ce chapitre octroyé par Liberty Alliance en raison principalement de son interopérabilité et du respect de la vie privée, rencontrant ainsi les spécifications de services du Liberty Federation and Liberty Web. Pour plus de détails, consulter la page suivante : www.xml.org/xml/news/archives/archive.09142006.shtml#2.

[200] Il en coûte au Canada 40 $ pour l'acquisition du logiciel ChatShield et de 20 $ par année pour l'utilisation du système d'authentification.

5.2.14 États-Unis d'Amérique

Responsabilité et types de régulation

Les États-Unis ont recours, pour la gouvernance du contenu audiovisuel sur Internet, principalement à l'autorégulation pour le contenu pouvant être nocif pour la jeunesse et à la régulation en mode directive, pour le contenu illégal. Ils ont aussi recours, à l'occasion, à la corégulation (relativement à la protection de la vie privée des enfants).

Aux États-Unis, aucune loi ne régit le classement des films, y compris ceux sur support vidéo, et, lorsque celui-ci se retrouve sur un produit, les spectateurs, de même que les exploitants, sont libres de le respecter ou non. Un organisme émanant de l'industrie cinématographique, la **Motion Picture Association** (www.mpaa.org) a toutefois pour mission de classer les produits dans le but d'informer le public. Il n'y a pas non plus de loi concernant le contenu audiovisuel sur Internet.

Cependant, l'organisme de régulation, soit Federal Communications Commission (FCC) a récemment « recommandé » (régulation, mode recommandation), à l'association des télécommunications et d'Internet (CTIA - US Cellular Telecommunications & Internet Association - www.ctia.org), de mettre en place davantage de mesures pour décourager les enfants d'accéder du contenu pour adulte par le biais de leurs appareils mobiles, à savoir :

- Former les parents sur les options servant à protéger leurs enfants, incluant le blocage d'accès à Internet;
- Former les parents sur les mesures que l'industrie a mis en place pour protéger leurs enfants d'un accès à du contenu inapproprié;
- Prévoir changer le code de pratiques des membres de la CTIA afin de faire la promotion de l'autorégulation de l'industrie dans ce domaine;
- Considérer les mesures déployées par d'autres gouvernements et industries dont le Royaume-Uni et l'Australie.

Depuis 2005, la CTIA prévoit une classification binaire du contenu audiovisuel permettant de détecter si le contenu est accessible ou non pour les moins de 18 ans[201]. Les critères pour déterminer si le contenu est accessible aux moins de 18 ans seront les mêmes que ceux utilisés par l'industrie des films, de la musique et des vidéos.

---

[201] Consulter le document n° 16 du Cahier 3 *Review Of The Regulation Of Content Delivered Over Convergent Devices* (p. 86) (www.dcita.gov.au/__data/assets/pdf_file/39890/Final_Convergent_Devices_Report.pdf).

Le gouvernement américain a mis en place en 2000 une loi de protection des enfants par rapport au contenu offensant sur Internet (Children's Internet Protection Act - CIPA) destinée aux écoles et bibliothèques. La CIPA exerce un certaine corégulation par l'entremise de son pouvoir de financement. En effet, par le biais de la CIPA, le gouvernement fournit un certain financement à ces entités à la condition qu'elles répondent aux exigences suivantes :

- Mise en place de politique relative à la sûreté sur Internet et de mesures technologiques de protection. Ces mesures incluent le blocage ou le filtrage d'images obscènes ou nuisibles pour les mineurs et de pornographie infantile;
- Adoption et suivi d'une politique de surveillance des mineurs concernant leurs activités en ligne;
- Adoption et mise en place d'une politique relative à l'accès par les mineurs de contenu inapproprié sur Internet, à la sûreté et la sécurité des mineurs dans l'utilisation du courriel, des salles de clavardage et d'autres formes de communications électroniques directes, aux accès non autorisés ou illégales par les mineurs, à la divulgation, l'utilisation et la diffusion de renseignements personnels sur les mineurs ainsi qu'à l'accès restreint des mineurs à du contenu nuisible[202].

1.a DNS :

Le gouvernement américain encourage fortement, par le biais de financement des écoles et des bibliothèques, le recours à la technologie de filtrage et de blocage de contenu, notamment audiovisuel, dont la plupart des solutions technologiques utilisent le nom de domaine. De plus, en matière d'Internet par mobiles, son industrie privilégie la caractérisation du contenu et des sites Web et se base, en partie sur le DNS. Enfin, certaines solutions privées d'authentification, telles que SenderID proposée par Microsoft pour contrer le pollupostage et favorisée par le gouvernement des États-Unis, utilisent les enregistrements du DNS pour vérifier l'authenticité de l'émetteur.

1.b Serveurs racine

Aucune utilisation des serveurs racine n'a été détectée pour la gouvernance du contenu audiovisuel.

[202] Consulter le document n° 52.1 du Cahier 4*Children's Internet Protection Act* (www.fcc.gov/cgb/consumerfacts/cipa.pdf)

1.c Normes ou standards

Les normes et standards d'Internet sont utilisés.

1.d Multilinguisme

Les États-Unis ont recours au multilinguisme pour ce qui est du contenu.

2.a Création du contenu – catégorisation

Les États-Unis, selon l'approche proposée par l'une ou l'autre des deux organisations proposant l'étiquetage du contenu, soit ICRA ou SafeSurf[203], ont recours à la catégorisation du contenu sur Internet, sur une base volontaire.

2.b Création du contenu – classement

Les États-Unis n'ont pas recours, du moins au niveau fédéral, au classement du contenu sur Internet. Cependant, en matière de contenu Internet accessible par mobile, l'industrie prévoit une autorégulation très bientôt, à la suite de l'insistance du gouvernement des États-Unis.

2.c Contrôle du contenu - homologation

Il n'y a pas d'homologation obligatoire générale de contenu aux États-Unis.

Cependant, il existe une organisation, ChildSafe International, qui offre la possibilité d'homologuer le contenu d'un site Web qui a été catégorisé par l'une des approches de catégorisation de contenu en usage (ICRA ou SafeSurf), soit la « ICCS™ Certification »[204] L'homologation permet aussi de déterminer de façon claire la présence de contenu pour adultes et de l'afficher de façon claire sur le site Web correspondant à ce contenu. De plus, depuis novembre 2006, l'ICRA offre un service d'homologation semblable.

---

[203] Consulter le document n° 12 du Cahier 5 *SafeSurf: The Basics* (www.Safesurf.com)
[204] Consulter le site Web IwatchDog : www.iwatchdog.org

Il existe plusieurs autres homologations de firmes privées ou d'organismes sans but lucratif. On retrouve, par exemple, celle offerte par le Better Business Bureau (BBB Online), financé par l'industrie et le gouvernement des États-Unis (Department of Commerce – DoC). Elle offre ainsi un sceau de confiance délivré spécifiquement aux sites sûrs pour les enfants (Safe Harbor). Cette homologation se base sur une obligation légale pour protéger la vie privée des jeunes de moins de 13 ans.

2.d Contrôle du contenu – filtrage

Tel que mentionné précédemment, le gouvernement des États-Unis encourage fortement le recours aux logiciels de filtrage dans les écoles, les bibliothèques et pour l'accès à Internet par le biais de mobiles. L'industrie des logiciels et services de filtrage aux États-Unis est très active et présente une offre très variée dans ce domaine.

2.e Contrôle du contenu – lutte à cybercriminalité

Le gouvernement fédéral dispose d'un ensemble de mesures légales pour mener la lutte contre la cybercriminalité. Elle est actuellement à étudier un projet de loi (*Internet Safety and Child Protection Act*), qui vise à, notamment, exiger la vérification adéquate de l'âge et à percevoir une taxe de 25 % sur tout produit pornographique vendu par Internet. Cette taxe servira, si le projet de loi est adopté, à financer la protection des enfants contre les contenus pour adultes[205].

Le gouvernement américain, par le biais principalement du Federal Bureau of Investigation (FBI), fournit un centre de signalement de cybercriminalité : Internet Crime Complaint Center (IC3 - www.ic3.gov) et finance un centre de cyberenquêtes (www.fbi.gov/cyberinvest/cyberhome.htm).

L'organisation sans but lucratif **National Center for Missing and Exploited Children** (NCMEC - www.missingkids.com) est l'organisation la plus importante aux États-Unis concernant la lutte à la cybercriminalité auprès des enfants. Ce centre a pour mission d'aider à prévenir l'abus et l'exploitation sexuelle d'enfant, d'aider les victimes, leurs familles et les professionnels qui les aident. Au delà du travail concernant les enfants disparus, le NCMEC fournit, notamment, une ligne servant au cybersignalement de cybercriminalité relative aux enfants (CyberTipline), des ressources concernant l'abus d'enfants, de la formation auprès des

[205] Consulter le document n° 52.7du Cahier 4 *Internet Safety and Child Protection Act* (http://thomas.loc.gov/cgi-bin/query/z?c109:h3479)

professionnels du domaine, de la coordination d'efforts de la protection de la jeunesse avec le secteur privé et de l'information auprès des gouvernements pour s'assurer d'une législation appropriée pour protéger les enfants. Le NCMEC représente le canal de communication le plus important pour signaler des cas de cybercriminalité. À cet effet, il fournit la liste des catégories de crimes possibles, tous couverts par des dispositions légales, ainsi que la façon de les signaler :

- Pornographie infantile (tout enfant de moins de 18 ans);
- Encouragement des enfants à commettre des actes sexuels;
- Prostitution d'enfants;
- Tourisme sexuel impliquant des enfants;
- Abus sexuel d'enfant;
- Envoi à un enfant (moins de 16 ans) de matériel obscène non sollicité (par le biais de pourriels principalement);
- Leurre par le biais du nom de domaine afin d'inciter l'enfant à visiter un site Web contenant du matériel nuisible.

2.f Lutte au pollupostage

Les États-Unis, au niveau fédéral, possède une loi entourant le pollupostage gérée par le Federal Trade Commission (FTC) (CAN-SPAM Law[206]) et offre un site Web fort complet sur le sujet[207]. Cette loi inclut, notamment, l'exigence de fournir une option de désabonnement (opt-out) à toute personne qui reçoit un courriel non sollicité et offre une adresse électronique pour signaler tout pourriel (spam@uce.gov), particulièrement ceux qui semblent illégaux. À cette adresse, plus de 10 millions de signalements de courriel ont été transmis[208]. De plus, chacun des États peut légiférer dans ce domaine[209]. La FTC, sur son site OnGuard Online, fournit l'information pour déposer une plainte auprès des organismes responsables de son traitement selon le type de problème, dont celui concernant le pollupostage.

---

[206] Consulter le document n° 52.9 du Cahier 4 *The CAN-SPAM Act: Requirements equirements for Commercial Emailers* (www.ftc.gov/bcp/conline/pubs/buspubs/canspam.pdf)

[207] Consulter les pages Web suivantes : www.ftc.gov/spam et www.ftc.gov/bcp/conline/edcams/spam/index.html

[208] Consulter le document n° 52.3 du Cahier 4 *Spam Report* (http://cc.uoregon.edu/cnews/fall2002/spamreport.html)

[209] Consulter le site Web fournissant les références aux états ayant légiféré en matière de pollupostage : www.spamlaws.com/state/index.html

Certaines initiatives privées sont mises en place pour lutter contre le pollupostage. Une de celles-ci est l'approche développée par Microsoft (et favorisée par la FTC) et rendue disponible gratuitement récemment, soit Sender ID. Cette approche semble être utilisée par plus de 2,5 millions de compagnies, y incluant certaines provenant du logiciel libre (tel que SendMail) et se retrouve à être utilisée par plus de ½ milliard d'utilisateurs[210]. Elle permet d'augmenter la fiabilité de l'authenticité de l'émetteur d'un courriel et ainsi permettre un filtrage des pourriels.

2.g Pédagogie

Toutes les parties prenantes (gouvernements, entreprises et société civile) participent à la sensibilisation et la formation des enfants, des parents, des éducateurs et des personnes chargées d'appliquer la loi. Il existe énormément d'organisations qui font oeuvre de pédagogie. Nous n'en faisons état que de quelques-unes d'entre elles qui apparaissent prendre une place plus importante sur le territoire des États-Unis.

Du côté gouvernemental, on retrouve la FTC (Federal Trade Commission) qui maintient un site Web afin de faire la promotion d'une navigation plus sûre sur Internet et notamment pour la protection de la jeunesse (OnGuard Online - http://onguardonline.gov) et ce, en partenariat avec plus d'une vingtaine d'organisations des secteurs gouvernemental, privé et associatif[211]. Il est avant tout destiné aux adultes et aux parents. Il couvre les sujets suivants :

- Réseautage social (par le biais de clavardage notamment);
- Pollupostage;
- Commerce électronique;
- Partage de fichiers (P2P);
- Téléphonie par Internet (VoIP – Voice over Internet Protocol);
- Fraudes transfrontières.

Il fournit, de plus, une liste d'organisations choisies des États-Unis oeuvrant à l'alphanétisation et à la protection des internautes et particulièrement des jeunes. Enfin, il fournit l'information pour déposer

[210] Consulter le document n° 60.2 du Cahier 4 *Cadre de fonctionnement de Sender ID* (http://download.microsoft.com/download/9/c/f/9cf82def-4e0e-42f9-8629-bc5120043fef/en_sidf.pdf) ou le site Web de Sender ID : www.microsoft.com/senderid

[211] Consulter le document n° 52.5 du Cahier 4 *Onguard Online - Social Networking* (http://onguardonline.gov/socialnetworking.html)

une plainte auprès des organismes responsables de son traitement selon le type de problème, dont celui concernant le pollupostage.

Du côté des secteurs privés et associatifs, on retrouve les quatre organisations suivantes :

- I-SAFE (www.iSafe.org);
- National Institute on Media and the Family (www.mediafamily.org);
- Center for Media Literacy (CML - www.medialit.org);
- Parent-Teacher Association (PTA – www.PTA.org).

i-SAFE est une organisation sans but lucratif de la Californie, fondée en 1998 et soutenue par le Congrès des États-Unis. Elle a une présence dans tous les États des États-Unis ainsi que dans les écoles du Department of Defense. Elle a pour mission de faire en sorte que les expériences des jeunes sur Internet soient sûres et responsables. À cette fin, elle a mis en place un curriculum de formation (programme i-LEARN Online et le i-Mentor Network) destiné aux différentes clientèles cibles, soit les jeunes, les enseignants, les parents, les représentants de la loi et les adultes concernés par le sujet. Microsoft est un des partenaires de cette organisation pour la partie formation en ligne. Depuis trois ans, près de 300 000 étudiants et 10 000 parents ont suivi le programme de formation. Cette formation touche à des sujets tels que :

- Cybercitoyenneté;
- Sûreté personnelle;
- Cybersécurité;
- Propriété intellectuelle;
- Cyberintimidation;
- Identification des prédateurs.

Ce programme est dispensé autant à l'intérieur des écoles qu'auprès des communautés. D'où certaines déclinaisons de leurs programmes de formation telles que Student Mentors (destiné aux étudiants plus âgés qui servent de mentors aux plus jeunes, à leurs pairs, leur famille et leur communauté); le programme i-PARENT (destiné à réduire la fracture numérique entre les parents et leurs enfants) et leur programme i-SHIELD (destiné aux représentants de la loi sur la cybercriminalité).

i-SAFE fait partie du réseau européen INSAFE.

L'Institut national sur les médias et la famille (**National Institute on Media and the Family**) est un des organismes de la société civile à faire

oeuvre de pédagogie. Sa vision est de « faire en sorte que des familles et des communautés soient en santé par l'usage avisé des médias ». Sa mission est de maximiser les bénéfices et minimiser les dommages des médias sur les enfants au moyen de la recherche, de la formation et de la sensibilisation. Cet institut offre une liste assez exhaustive d'organisations oeuvrant à des missions similaires[212].

Le **Center for Media Literacy** (CML) est un autre organisme de la société civile qui fait oeuvre de pédagogie non pas sur Internet en particulier mais sur tous médias. Ce centre fournit de la formation publique, du développement professionnel et des ressources éducatives afin de développer l'aisance avec les médias. Ceci afin d'aider les citoyens et particulièrement les jeunes, à développer une pensée critique et des habiletés pour produire des contenus. Plusieurs de ses ressources, bien que non ciblées pour Internet, peuvent être utilisées pour être appliquées à l'alphanétisation des jeunes, de leurs parents et de leurs éducateurs.

L'organisation Parent-Teacher Association (PTA – www.PTA.org), bien qu'ayant une mission beaucoup plus large que l'alphanétisation, couvre très bien ce volet[213]. Sa vision consiste à développer l'habileté à communiquer de façon compétente dans toutes les formes de médias, tant imprimés qu'électroniques, aussi bien pour accéder, comprendre, analyser et évaluer les images, mots et sons véhiculés par les médias.

3.a Liberté d'expression

La liberté d'expression est une des valeurs fondamentales des États-Unis et inscrite dans sa Constitution. C'est sur cette base qu'une loi votée à la fin des années 1990 par le Congrès et le Sénat portant sur la protection des enfants sur Internet, a été invalidée par la Cour suprême des États-Unis car elle allait à l'encontre de la liberté d'expression, telle que formulée.

3.b Protection des données et de la vie privée

L'approche des États-Unis pour la protection de la vie privée des jeunes est un bon exemple de corégulation. Le gouvernement, par le biais de la FTC,

[212] Consulter le document n° 52.4 du Cahier 4 *Liste d'organisations* (www.mediafamily.org/links/index.shtml)
[213] Consulter la page Web de la PTA fournissant sa vision sur la protection de la jeunesse par rapport au contenu sur Internet : www.pta.org/archive_article_details_1117655691078.html

a adopté et mis en oeuvre une loi pour protéger la vie privée des enfants de moins de 13 ans (Children's Online Privacy Protection Act de 1998 ou COPPA - www.coppa.org)[214]. Les organisations privées et de la société civile ont eu la responsabilité de mettre en place une approche pour certifier ou homologuer les sites Web en matière de protection des renseignements personnels auprès des jeunes (concept de Safe Harbor – « port sûr »). Ainsi, le Better Business Bureau (www.bbbonline.org), partiellement financé par la FTC, a été la première organisation des États-Unis à mettre en place un programme de régulation[215] conforme aux exigences de cette loi. D'autres organismes tels que l'organisme de classement des jeux en Amérique du Nord, le ESRB, offrent aussi une telle homologation. Les organisations qui obtiennent une certification basée sur une approche approuvée par le FTC, se retrouvent épargnées des actions coercitives que le FTC pourrait exercer contre elles.

3.c Gestion de l'identité et authentification

Plusieurs initiatives privées sont disponibles pour l'authentification. Certaines sont spécialisées selon le type d'interaction (comme le courriel ou les blogues). Ainsi, Microsoft présente une initiative pour le courriel en utilisant le DNS, soit Sender ID et une autre nommée CardSpace[216] qui offre un métasystème d'identité permettant de prendre en compte plusieurs identités numériques pour une même personne. De même, la communauté du logiciel libre présente une approche en cours de développement pour les blogues avec Open ID[217]. Cette initiative est ouverte, décentralisée et gratuite.

Cependant, ces approches, purement technologiques, ne garantissent pas l'authenticité des personnes possédant cette identité numérique. Elles permettent de garantir la protection de cette identité numérique et les renseignements personnels rattachés à cette identité numérique.

---

[214] Consulter le document n° 52.5 du Cahier 4 *OnGuard Online - Social Networking* (http://onguardonline.gov/docs/onguardonline_socialnetworking.pdf)
[215] Consulter le programme sur la vie privée CARU (Children's Advertising Review Unit) : www.caru.org/program/index.asp
[216] Consulter le site Web de Microsoft sur le sujet : http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx
[217] Consulter le document n° 60.1 du Cahier 4 *Authentification - OpenID* ou le site Web de Open ID : http://openid.net ou www.eweek.com/print_article2/0,1217,a=184700,00.asp

Tableaux récapitulatifs

Dans ces tableaux, on utilise quatre caractères distincts :

- « - » pour indiquer l'absence de l'élément pour ce pays;
- « X » pour indiquer la présence de l'élément pour ce pays;
- « x » pour indiquer la présence partielle de l'élément pour ce pays;
- « * » pour indiquer la présence planifiée imminente de cet élément pour ce pays;
- « n.d. » pour indiquer l'absence d'information sur cet élément pour ce pays.

Pays	**Responsabilité**			
	Org. semblable à la RCQ	**Org. gouv. autre**	**Org. du secteur privé**	**Org. non gouv. (ONG)**
Australie	x	X	X	X
Canada	-	-	-	X
Québec	-	-	-	X
Ontario	-	-	-	X
Colombie britannique	-	-	-	X
Nouveau-Brunswick	-	-	-	X
Europe	-	X	X	X
Danemark	X	-	X	X
Espagne	-	X	X	X
France	-	X	X	X
Royaume-Uni	-	X	X	X
États-Unis	-	X	x	X

Tableau 5.5 – Tableau relatif à la répartition de la responsabilité de la gouvernance du contenu audiovisuel sur Internet

Pays	Type de régulation			
	Autorégulation	**Corégulation**	**Régulation – mode recommandation**	**Régulation – mode directive**
Australie	x [218]	X	X	X
Canada	X	x [219]		X
Québec	X			X
Ontario	X			X
Colombie britannique	X			X
Nouveau-Brunswick	X			X
Europe	X	X	X	X
Danemark	X		X	X [220]
Espagne		X	X	x
France		X		X
Royaume-Uni	X	X	X	X
États-Unis	X	X	X	X

Tableau 5.6 – Tableau relatif aux types de régulation

[218] Seuls les volets « pédagogie » et « authentification » sont en mode d'autorégulation.
[219] Participation et financement du volet « pédagorie »
[220] En matière de cybercriminalité et de pollupostage seulement.

Pays	**Moyens de régulation**		
	Principes	**Lois, directives, règles et normes**	**Programme commun**
Australie	X	X	X
Canada	X	X	X
Québec	X	X	X
Ontario	X	X	X
Colombie britannique	X	X	X
Nouveau-Brunswick	X	X	X
Europe	X	X	X
Danemark	X	X	X
Espagne	X	X	X
France	X	X	X
Royaume-Uni	X	X	X
État-Unis	X	X	X

Tableau 5.7 – Tableau relatif aux moyens de régulation

Pays	**1. Questions relatives à l'infrastructure et à la gestion de ressources Internet critiques**			
	a. DNS	**b. Serveurs racine**	**c. Normes ou standards**	**d. Multi-linguisme[221]**
Australie	X	-	X	x
Canada	X	-	X	x
Québec	X	-	X	x
Ontario	X	-	X	x
Colombie britannique	X	-	X	x
Nouveau-Brunswick	X	-	X	x
Europe	X	-	X	x
Allemagne	n.d.	n.d.	n.d.	X
Danemark	X	-	X	x
Espagne	X	-		x
France	X	-	X	x
Royaume-Uni	X	-	X	x
États-Unis	X	-	X	x

Tableau 5.8 – Tableau relatif à l'infrastructure et à la gestion des ressources critiques

[221] x : multilinguisme de contenu seulement
X : multilinguisme de contenu et de nom de domaine (IDN)

Pays	**2. Questions relatives à l'utilisation d'Internet**				
	a. Catégori-sation	**b. Classe-ment**	**c. Homo-logation**	**d. Filtrage**	**Fourniture de filtrage obligatoire[222]**
Australie	X	X	-	X	Oui
Canada	-	-	-	X	Non
Québec	-	-	-	X	Non
Ontario	-	-	-	X	Non
Colombie britannique	-	-	-	X	Non
Nouveau-Brunswick	-	-	-	X	Non
Europe	x [223]	-	-	X	Non
Danemark	-	-	* [224]	X	Partiel [225]
Espagne	-	-	X	X	?
France	-	* [226]	-	X	Oui
Royaume-Uni	x [227]	X	-	X	Non [228]
États-Unis	x [229]	x [230]	-	X	Non

Tableau 5.9.1 – Tableau relatif à l'utilisation d'Internet

[222] Obligation par le FAI/FSI de fournir un logiciel de filtrage/contrôle parental

[223] L'Europe favorise l'utilisation d'un système de catégorisation de contenu en soutenant l'ICRA

[224] Le Danemark se prépare à offrir une homologation des sites de clavardage pour les enfants.

[225] Il est recommandé aux opérateurs de mobiles d'offrir des possibilités de filtrage
Les bibliothèques et les écoles peuvent disposer gratuitement de logiciel de filtrage, sur une base volontaire
Un filtrage contre les pourriels doit être mis en place par les FSI.

[226] Il est prévu, début 2007, offrir une homologation des sites Web (« label citoyen ») et des FAI/FSI (« marque de confiance »).

[227] Catégorisation partielle pour le contenu Internet accessible par les mobiles.

[228] Il est prévu qu'à la fin de 2007, les FAI à large bande auront implanté un service de filtrage.

[229] Les États-Unis s'apprêtent à adopter un système volontaire de catégorisation pour le contenu sur Internet accessible par mobile.

[230] Les opérateur de mobiles s'apprêtent à adopter un système de classement binaire (pour ou non les moins de 18 ans) pour le contenu sur Internet.

Pays	**2. Questions relatives à l'utilisation d'Internet**		
	e. Lutte à la cybercriminalité	**f. Lutte au pollupostage**	**g. Pédagogie**
Australie	X	X	X
Canada	X	X	X
Québec	X	X	X
Ontario	X	X	X
Colombie britannique	X	X	X
Nouveau-Brunswick	X	X	X
Europe	X	X	X
Danemark	X	X	X
Espagne	X	X	X
France	X	X	X
Royaume-Uni	X	X	X
États-Unis	X	X	X

Tableau 5.9.2 – Tableau relatif à l'utilisation d'Internet

Pays	**3. Questions relatives à la liberté d'expression ainsi qu'à la protection des données et de la vie privée**		
	a. Liberté d'expression	**b. Protection des données et de la vie privée**	**c. Gestion de l'identité et de l'authentification**
Australie	X	X	-
Canada	X	X	-
Québec	X	X	-
Ontario	X	X	-
Colombie britannique	X	X	x [231]
Nouveau-Brunswick	X	X	-
Europe	X	X	* [232]
Allemagne	n.d.	X	n.d.
Belgique	n.d.	n.d.	X
Danemark	X	X	x [233]
Espagne	X	X	-
France	X	X	-
Royaume-Uni	X	X	x [234]
États-Unis	X	X	

Tableau 5.10 – Tableau relatif à la liberté d'expression et la protection de la vie privée

[231] Système d'authentification disponible pour tous les citoyens mais pas d'utilisation spécifique pour la protection de la jeunesse.
[232] Les systèmes d'authentification sont présentement à l'étude en Europe.
[233] Signature électonique disponible pour tous les citoyens mais pas d'utilisation spécifique pour la protection de la jeunesse.
[234] Solution d'authentification nationale en cours de déploiement.

Pays	**Taxonomie du contenu sur Internet par pays**					
	Film et Vidéo		**Internet**		**Mobile**	
	Classes d'âge	Types de contenu	Classes d'âge	Types de contenu	Classes d'âge	Types de contenu
Australie	6	-	6	-	6 [235]	-
Canada	5	-	-	-	-	-
Québec	4	5	-	-	-	-
Ontario	5	15	-	-	-	-
Colombie britannique	6	32	-	-	-	-
Nouveau-Brunswick	6	14	-	-	-	-
Europe	-	-	-	-	-	-
Danemark	4	n.d.	n.d.	n.d.	n.d.	n.d.
Espagne	6	-	-	-	-	-
France	4	n.d.	-	-	4	n.d. [236]
Royaume-Uni	8	8	-	-	2	8
États-Unis	5	-	2 [237]	-	2 [238]	-

Tableau 5.11 – Comparaison de la taxonomie par pays

[235] Exigence de preuve d'âge pour accéder à du contenu destiné aux 18 ans et plus.
[236] Un projet de taxonomie est à l'étude en France pour les mobiles.
[237] Sur une base volontaire.
[238] Sur une base volontaire.

5.3 Conclusion sur la gouvernance par pays

Les tableaux récapitulatifs présentés à la fin de la section précédente ont permis de faire ressortir les approches les plus fréquemment utilisées et celles ignorées. Dans cette section, nous aborderons la gouvernance par pays en comparant, élément par élément, la situation au Québec (et au Canada) avec celle d'autres pays en faisant ressortir les similitudes et les différences concernant cette gouvernance. Cependant, il ne faudra pas interpréter ces différences comme des recommandations de pratiques pour le Québec. Nous réserverons notre jugement ou nos recommandations lors de la conclusion du présent rapport. De plus, il est important de retenir que lorsque nous nous référons aux pays, nous nous référons à l'échantillon de pays étudiés.

Attribution de la responsabilité

Rôle gouvernemental

Les gouvernements interviennent dans la gouvernance du contenu audiovisuel pour la protection de la jeunesse de diverses façons que l'on peut regrouper ainsi :

- Législation;
- Participation directe à la gouvernance (classement du contenu et coordination de la gouvernance);
- Participation indirecte à la gouvernance par le biais du financement d'organismes associatifs sur la gouvernance ou de programmes conjoints.

Législation

Tous les pays possèdent une législation directe ou indirecte en matière de gouvernance de contenu audiovisuel sur Internet. Tous les pays disposent, par exemple, de législation concernant la cybercriminalité et notamment en matière de pornographie infantile. La plupart des pays (sauf le Canada et ses provinces et territoires) disposent aussi de législation concernant l'accès et le classement de contenu Internet pour adulte accessible par mobile.

D'autres législations générales s'appliquent aussi à la gouvernance du contenu sur Internet, comme esquissée au chapitre précédent. Il s'agit de rappeler la *Déclaration universelle des droits de l'homme* (concernant notamment la liberté d'expression), la *Déclaration universelle de l'UNESCO sur la diversité culturelle* (concernant notamment la protection des diverses langues nationales) et la *Convention relative aux droits de l'enfant* (concernant

notamment la liberté d'expression et d'accès à l'information[239] reconnue aux enfants et la responsabilité première des parents dans l'éducation des enfants).

Participation directe à la gouvernance

En général, très peu de pays ont attribué la responsabilité de la gouvernance du contenu audiovisuel d'Internet à l'organisme partageant une mission semblable à celle de la Régie du cinéma, soit le classement des films. À ce jour, aucun pays n'effectue de classement de contenu audiovisuel sur Internet de façon aussi systématique que pour les films. Lorsqu'il y a un classement de contenu audiovisuel sur Internet, c'est réalisé sur une base volontaire (et donc très peu fréquent) et davantage systématique concernant le contenu accessible avec les mobiles.

En effet, la seule situation où on commence à constater le classement davantage systématique de contenu audiovisuel sur Internet, c'est lors de l'accès au moyen de mobiles où l'industrie a commencé à effectuer un classement binaire minimal (accessible ou non pour les moins de 18 ans). Et cela est dû au fait que la plupart des pays (sauf le Canada et ses différentes provinces et territoires) ont légiféré pour que le contenu pour adulte (pornographie, jeux, etc.) ne soit pas accessible aux moins de 18 ans par le biais des mobiles. Habituellement, les façons pour le faire sont laissées à la discrétion de l'industrie (et quelquefois en collaboration avec la société civile comme en France).

En fait, un seul pays, soit le Danemark, a réellement intégré la gouvernance de contenu audiovisuel sur Internet avec les autres médias audiovisuels (tels que les films, vidéos et jeux vidéo ou par ordinateur). En effet, le ministère Danois de la Culture a intégré en un seul organisme gouvernemental, soit le Conseil des médias pour les enfants et les jeunes gens (Medierådet for Børn og Unge - Media Council for Children and Young People – MCCYP), cette responsabilité. Ce Conseil effectue le classement des films projetés en public et exerce un leadership pour que l'industrie effectue un certain classement sur une base volontaire en recourant, notamment au système de catégorisation proposé par l'Internet Content Rating Association (ICRA). De plus, ce Conseil réalise un travail important de sensibilisation et de formation visant à augmenter l'alphanétisation et ainsi l'habileté de la jeunesse à naviguer de façon sûre sur Internet. C'est le seul pays qui a intégré en un seul organisme gouvernemental la responsabilité classique de

[239] L'article 13.1 stipule : « L'enfant a droit à la liberté d'expression. Ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen du choix de l'enfant. »

classement des films et celle d'alphanétisation des jeunes et des personnes gravitant autour d'eux (tels que parents et éducateurs).

Un autre pays qu'il convient de souligner est l'Australie[240] qui, tout en conservant intact l'organisme qui s'acquitte de la mission de classement des films semblable à celle de la Régie du cinéma, soit l'Office de classification des films et de la littérature (Office of Film and Literature Classification – OFLC), a créé un autre organisme, soit l'Autorité australienne des communications et des médias (Australian Communications and Media Authority - ACMA), responsable de la régulation des autres médias dont Internet. L'ACMA, qui relève du ministre des Technologies de l'information, des Communications et des Arts, utilise, pour le contenu sur Internet, le même système de classification défini pour les films. La classification du contenu sur Internet s'effectue sur une base volontaire par l'industrie.

Tous les pays ont attribué à un organisme gouvernemental un certain rôle dans la gouvernance du contenu sur Internet. Très souvent, ce rôle se situe au niveau de l'alphanétisation que nous verrons plus loin sous la section « pédagogie ».

Participation indirecte à la gouvernance

Tous les gouvernements des pays jouent un rôle indirect dans la gouvernance d'Internet pour la protection de la jeunesse en contribuant au soutien des organisations de la société civile qui exercent un rôle de pédagogie ou de lutte à la cybercriminalité. Ce soutien peut prendre la forme de soutien technique et surtout de soutien financier.

Rôle du secteur privé

En général, le secteur privé participe à la gouvernance à deux niveaux : en offrant des produits ou services de filtrage et en offrant une collaboration dans le contrôle du contenu.

L'industrie s'est activée à élaborer une offre abondante et variée en matière de logiciels permettant le blocage ou le filtrage de contenu. On a assisté, depuis quelque temps, à une association entre les fournisseurs d'accès ou de services Internet (FAI/FSI) avec des producteurs de logiciels de filtrage afin de rendre disponibles aux internautes des solutions de filtrage. Certains de ces services sont accessibles en supplément aux services d'abonnement à

[240] Il est à noter que l'Australie sera l'hôtesse en février 2007 de la conférence internationale sur la classification du contenu : International Ratings Conference. Consulter le site Web : www.ratingsconference2007.com

Internet comme c'est le cas souvent le cas au Québec et d'autres ont commencé à l'intégrer directement dans leur abonnement (comme un fournisseur Internet au Royaume-Uni pour le service à haute vitesse). Nous verrons plus en détail cet aspect dans le chapitre suivant.

L'industrie du logiciel a commencé à oeuvrer dans la protection de la jeunesse sur Internet à la suite de l'insistance des gouvernements. Ainsi, on peut constater que le secteur privé est à peu près absent de cet aspect de la gouvernance d'Internet au Canada et au Québec car les gouvernements canadiens et québécois n'ont pas fait pression sur l'industrie à cet effet. Les gouvernements qui ont légiféré ou fait pression sur l'industrie (par des menaces de législation ou par du financement, par exemple), ont vu l'industrie s'investir dans la protection de la jeunesse. C'est le cas des pays européens et de l'Australie. Il est intéressant de noter la participation d'une firme privée, soit Microsoft, dans l'élaboration d'un logiciel pour la lutte à la cybercriminalité à la suite de l'initiative d'un policier du Service de police de Toronto. Même si on peut louanger l'apport technique et financier du secteur privé, il faut quand même souligner le soutien insuffisant des gouvernements pour faire respecter une loi et combattre un des aspects les plus néfastes d'Internet, soit la pornographie infantile. C'est symptomatique du sous financement, du moins au Canada, de la protection de la jeunesse sur Internet. Si les policiers ne se sentent pas suffisamment appuyés pour effectuer la lutte à la cybercriminalité, il est loin d'être assuré que les parents et éducateurs ainsi que les jeunes eux-mêmes sont suffisamment épaulés pour permettre une utilisation d'Internet de façon sûre chez les jeunes.

Rôle de la société civile

Le rôle de la société civile est majeur dans la gouvernance du contenu audiovisuel pour la protection de la jeunesse. Elle intervient de façon très importante, en plus de la lutte à la cybercriminalité[241], en matière d'alphanétisation. Il existe plusieurs organisations très actives en Europe, en Australie et aux États-Unis et qui font oeuvre de pédagogie tant auprès des jeunes qu'auprès des parents, des éducateurs, des représentants de la loi et de tout autre adulte concerné par la question. De plus, on peut constater une grande collaboration entre ces organisations et le gouvernement ainsi qu'une implication du secteur privé par le biais de soutien technique (comme le soutien technologique de la prestation de cours en ligne) ou financier. En fait, dans ces pays, on peut noter un défi de coordination de toutes ces organisations afin de rejoindre adéquatement les personnes concernées sans duplication.

[241] Le FBI estime qu'il y a environ 20 nouveaux enfants apparaissant à chaque mois dans du contenu pornographique sur Internet.

Au Canada, seul le gouvernement fédéral semble être présent dans le soutien des très peu nombreuses organisations canadiennes de la société civile vouées à la protection de la jeunesse sur Internet. Les gouvernements des provinces semblent presque absents ou peu sensibilisés à la question, du moins jusqu'à présent. Seuls les ministères provinciaux relatifs à la sécurité publique en lien avec la cybercriminalité semblent s'investir dans cette question. Nous n'avons pu noter la présence d'organisations provinciales de la société civile oeuvrant à la protection de la jeunesse sur Internet.

La présente étude commandée par la Régie du cinéma qui relève de la ministre de la Culture du gouvernement du Québec dénote cependant un intérêt à porter attention à ce dossier et éventuellement y investir les ressources nécessaires.

Type de régulation

Le mode de régulation privilégié par la plupart des pays est l'autorégulation associée à une régulation classique en mode directive. Généralement, les gouvernements des pays ont recours à cette dernière régulation dans le contexte de la cybercriminalité. La seule exception retrouvée se situe en Espagne où les contraintes légales en cette matière se limitent à celles qui se retrouvent édictées par l'Union européenne avec sa Convention sur la cybercriminalité.

Pour ce qui a trait à la corégulation ou la régulation en mode recommandation, seul le Canada, incluant ses provinces et territoires, n'a pas recours à une de ces formes de régulation. Au Canada, la primauté des principes de la non-intervention de l'État dans la régulation d'Internet afin de permettre à l'industrie d'Internet de croître et de la liberté d'expression explique principalement cette situation.

Tel que mentionné précédemment, la plupart des gouvernements des pays, à l'exclusion du Canada, sont intervenus, selon l'un de ces deux derniers modes de régulation, pour ce qui a trait au contenu pour adultes sur Internet accessible par les mobiles. Seuls l'Australie et le Royaume-Uni y sont allés d'une régulation en mode directive concernant ce contenu. Habituellement, les opérateurs de mobiles se sont dotés de « codes de pratique » plus ou moins élaborés à la suite d'exigence ou de fortes recommandations de la part des gouvernements.

Il est intéressant de souligner l'initiative des États-Unis concernant la protection des renseignements personnels, en mode corégulation, pour les jeunes de moins de 13 ans avec le concept de « Safe Harbor ». Ainsi, le gouvernement a établi l'obligation de les protéger et a laissé à l'industrie et

la société civile le soin d'établir le moyen de le faire le plus adéquatement, tout en conservant le droit d'approuver l'approche retenue et en fournissant un financement adéquat pour permettre à la société civile de mettre en place cette approche.

Lorsque la régulation se base sur des obligations légales associées à des pénalités importantes, le gouvernement n'a pas nécessairement besoin d'offrir un soutien (technique ou financier) pour la mise en oeuvre des mesures légales par l'industrie. Cependant, pour une lutte efficace, par exemple, en matière de cybercriminalité, les gouvernements y ont dédié des ressources techniques ou financières. Aussi, il est important de souligner que les gouvernements ont apparié leur approche de régulation avec un financement de la société civile ou du secteur privé afin de permettre la mise en oeuvre des éléments de la gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse. Ainsi, si l'autorégulation n'est pas appuyée d'une volonté gouvernementale, l'autorégulation ne se fera pas. À preuve, la catégorisation du contenu sur Internet : il existe au moins une approche reconnue au niveau mondial (soit celle de l'ICRA), basée sur des normes de l'IETF, mais elle est très peu utilisée dans les faits. À moins d'exception comme au Danemark, même les sites gouvernementaux ne sont pas étiquetés selon les critères de l'ICRA. Cette approche de catégorisation du contenu n'a pas été appariée de soutien technique ou financier suffisant[242].

Moyens de régulation

Principes

Les parties prenantes à la gouvernance d'Internet des différents pays partagent tous les principes de gouvernance reconnus lors du Sommet Mondial sur la Société de l'Information (SMSI). Rappelons ceux qui s'appliquent particulièrement au contenu audiovisuel pour la protection de la jeunesse :

- Droit à la liberté d'opinion et d'expression;
- Reconnaissance et respect des droits et libertés d'autrui;

[242] L'Europe finance déjà l'existence de l'ICRA par le biais de son programme « Safer Internet ». Mais ce financement ne semble pas suffisant pour inciter l'industrie à utiliser l'approche d'ICRA. D'ailleurs, un des fureteurs les plus utilisés, soit Internet Explorer de Microsoft, ne reconnaît pas les étiquettes produites par l'ICRA, version 2005, et supporte plutôt une version périmée depuis 2000. L'évolution technologique de Microsoft sur la question est de déplacer la prise en charge du contrôle parental du fureteur vers le système d'exploitation de sorte que ce contrôle ne sera plus dépendant du fureteur (de sa version ou de son fournisseur) et que ce contrôle pourra s'appliquer à tout accès à Internet (comme les courriels ou le clavardage). De plus, la firme semble délaisser la version périmée d'étiquette pour choisir non pas la récente version de l'ICRA mais plutôt la catégorisation et le classement selon le Entertainment Software Ratings Board (ESRB). Pour plus de détails, consulter le site Web suivant : www.microsoft.com/windowsvista/community/parentalcontrols.mspx

- Égalité souveraine de tous les états;
- Protection des enfants et de la famille;
- Prise en compte de minorités dont les peuples autochtones;
- Participation de toutes les parties prenantes à la société de l'information;
- Établissement, rétablissement ou renforcement du climat de confiance et de sécurité dans l'utilisation des technologies de l'information et des communications (TIC), particulièrement en matière d'authentification, de protection de la vie privée et du consommateur, de cybersécurité, de cybercriminalité et de pollupostage;
- Importance de la normalisation internationale et de la contribution des organisations internationales;
- Respect de la diversité culturelle et linguistique;
- Utilisations éthiques des TIC.

À ces principes généraux, les pays ont ajouté, de façon explicite ou non, un certain nombre de principes qui peuvent expliquer l'évolution de la gouvernance du contenu audiovisuel sur Internet pour la protection de la jeunesse.

Ainsi, au Canada, on retrouve le principe de la non-intervention de l'État dans la régulation d'Internet, ce qui explique en partie le recours privilégié à l'autorégulation.

On retrouve dans la plupart des pays le principe de la non-tolérance de contenu illégal sur Internet et particulièrement concernant la pornographie infantile.

Le principe de l'alphanétisation de tous les acteurs de la gouvernance du contenu audiovisuel comme une des meilleures mesures de protection de la jeunesse, se retrouve mis de l'avant de façon très importante en Europe et particulièrement en France et au Danemark.

Lois, directives, recommandations, règles, normes

Tous les pays partagent un corpus minimal de régulation sous la forme de loi, directives, recommandations (particulièrement en Europe), règles et normes.

Cette communauté de régulation gravite principalement autour de la cybercriminalité et particulièrement la pornographie infantile où on y retrouve une gouvernance qui s'exerce aux niveaux tant local, national, régional et mondial. Un autre domaine commun de régulation concerne la protection de la vie privée ou plus particulièrement des renseignements personnels. Tous les pays ont mis en place des mesures de protection des

renseignements personnels basées sur la Directive de l'OCDE en la matière et présentent beaucoup de cohérence légale. L'application spécifique pour la protection de la jeunesse sur Internet est cependant relativement nouvelle. À cet effet, seuls les États-Unis ont pris des mesures concrètes pour protéger les renseignements personnels des jeunes en ayant voté deux lois dans ce sens dont une exige une homologation des sites Web pour démontrer qu'ils sont sûrs pour les jeunes (le sceau « Safe Harbor »). Il faut aussi souligner qu'en Belgique, cette protection des renseignements personnels peut aussi s'appliquer grâce à l'authentification numérique disponible à tous les Belges, incluant particulièrement les jeunes et les sites de clavardage.

Fait intéressant à souligner, c'est la volonté dans la plupart des pays, sauf au Canada, d'imposer une régulation du contenu pour adulte sur Internet accessible par le biais de mobile. Le mode de régulation qui semble se dessiner est de classifier au moins de façon binaire les contenus (pour adulte ou non), alors que l'Australie y va avec une approche beaucoup plus dirigée et détaillée : la catégorisation des contenus accessibles sur Internet

Programme commun

Tous les pays disposent de programmes communs, que ce soit au niveau de leur pays ou au niveau international.

On retrouve principalement des programmes communs tant national qu'international en ce qui a trait à la lutte à la cybercriminalité et à l'alphanétisation.

La pornographie infantile occupe beaucoup l'espace de la lutte à la cybercriminalité. Le programme européen « Safer Internet » inclut une dimension de lutte à la cybercriminalité par le réseau international de cybersignalement INHOPE. Le Canada fait partie de ce réseau.

Les programmes de sensibilisation et de formation visant à augmenter l'alphanétisation se retrouvent dans tous les pays. L'Europe possède un programme particulièrement bien étoffé, soit « Safer Internet » qui a mis en place un réseau international de sensibilisation et de formation à l'utilisation sûre et responsable d'Internet. Au programme commun européen, chacun des pays y a ajouté un programme spécifique à sa culture et à sa langue.

1.a DNS

Tous les pays ont recours au DNS dans leur gouvernance par le biais des logiciels de filtrage ou de système d'authentification. Ce recours au DNS peut mettre en péril une partie de la gouvernance étant donné la menace de la balkanisation du DNS, menace dont pour certains est actuellement une réalité. Cette menace provient principalement de l'internationalisation trop

lente de l'organisme anglo-saxon de gestion du DNS, soit ICANN, et du malaise international face à l'hégémonie du gouvernement des États-Unis sur le DNS pourtant considéré comme bien commun au niveau mondial.

1.b Serveurs racine et autres intermédiaires du DNS

Aucun pays n'a recours aux serveurs racine pour la gouvernance de contenu. Ceci s'explique par le principe de neutralité de l'architecture d'Internet : on n'intervient qu'aux extrémités du réseau et à l'intérieur du réseau, on ne fait que transiter l'information sans autre questionnement.

De plus, étant donné que les serveurs racine sont sous le contrôle d'ICANN et du gouvernement des États-Unis, il est compréhensible que les pays n'aient pas inséré de la gouvernance de contenu à ce niveau.

Cependant, devant l'importance des pourriels (au moins 50 % du trafic des courriels) et l'inadmissibilité d'utilisation des ressources critiques d'Internet à des fins criminelles, il pourrait être intéressant de se questionner sur la non-utilisation des serveurs racine pour réduire l'utilisation indue ou illicite des ressources critiques d'Internet. Au delà des serveurs racine, il pourrait y avoir une intervention au niveau des cinq registres régionaux d'Internet (RIR - Regional Internet Registry) pour aborder cette situation. Sachant que le pollupostage sert notamment à la sollicitation sexuelle et que la pornographie infantile est absolument inadmissible sur Internet, il serait intéressant de les bannir à la source.

De plus, cela pourrait réduire sensiblement l'utilisation de la bande passante en bloquant très tôt dans son cycle de vie cette activité inappropriée ou illégale. Cela pourrait éventuellement éviter aux firmes de télécommunication supportant cette bande passante de vouloir remettre en cause le principe de neutralité à cause de la trop grande utilisation de la bande passante.

1.c Normes ou standards

Tous les pays ont recours aux normes internationales ou standards de l'industrie pour permettre la gouvernance du contenu, que ce soit au niveau des normes d'ISO, de l'ITU, de IETF et de W3C. Ainsi, l'ICRA utilise une norme de W3C pour permettre la catégorisation des contenus sur Internet. Certaines approches d'authentification, comme SenderId, utilisent une norme de l'IETF. Cependant, la norme concernant l'internationalisation des noms de domaine provenant de l'IETF et d'ICANN exige une évolution pour s'assurer de la prise en compte plus adéquate des besoins d'internationalisation.

1.d Multilinguisme

Tous les pays supportent le multilinguisme quant au contenu des sites Web. Les normes internationales permettent le soutien adéquat du contenu sur Internet exprimé en l'une ou l'autre des langues nationales.

Par contre, en ce qui a trait de l'internationalisation des noms de domaine (IDN – Internationalized Domain Names), même s'il existe une norme de l'IETF permettant de le faire depuis plusieurs années, peu de pays ont mis en place le soutien des langues nationales dans le nom de domaine. Ainsi, la France et le Canada ne l'offrent pas encore. Cependant, au Canada, l'organisme responsable du nom de domaine « .ca », soit l'Autorité canadienne pour les enregistrements Internet - ACEI, a décidé de l'offrir dans un avenir approché à la suite d'une demande officielle du gouvernement du Québec. Seule l'Allemagne, chef de file dans ce domaine, l'offre depuis plusieurs années. Et c'est d'ailleurs le processus développé par l'Allemagne qui inspirera la proposition de soutien de l'IDN par l'ACEI.

On peut constater, qu'en général, les responsables de noms de domaine par pays ne sont pas très proactifs pour offrir un tel service d'IDN. De plus, les détenteurs de noms de domaine sont généralement peu sensibilisés à l'existence même de la possibilité de disposer de noms de domaine dans une langue autre que l'anglais et encore moins à qui demander un tel service! Il faut cependant noter que la mise en place de l'IDN n'est pas uniquement un défi technique (l'ICANN travaille encore à tenter d'améliorer le processus relatif à l'IDN et à éviter la balkanisation du DNS) mais aussi un défi administratif : les organisations qui offrent le service doivent aussi pouvoir disposer de personnel habile dans les différentes langues soutenues. Ainsi, est-ce qu'au Canada, l'IDN signifie le soutien du français et de l'anglais uniquement ou bien le soutien des autres langues des différentes communautés ethniques du Canada comme l'arabe, le chinois, l'espagnol, le russe, etc. De plus, l'enregistrement des noms de domaine avec des caractères accentués soulève des défis techniques, financiers et légaux pour les détenteurs de noms de domaine : devront-ils payer pour la réservation de leur nom de domaine autant de fois qu'il peut y avoir de variation dans le nom comme dans cet exemple : www.montréal.québec.org, www.montreal.quebec.org, www.montréal.quebec.org et www.montreal.québec.org ?

Il reste qu'avec l'accroissement de la popularité des noms de domaine par pays (ccTLD) comme « .ca » par rapport une diminution des noms de domaine générique (gTLD) comme « .com », les autorités nationales

responsables des noms de domaine de leur pays subiront une pression accrue pour soutenir l'IDN.

3.1.a Création du contenu – catégorisation

Au Canada, il n'y a pas d'initiative de catégorisation du contenu sur Internet ni même pour le contenu accessible par les mobiles.

Seuls l'Australie et le Royaume-uni présentent des initiatives de catégorisation du contenu. L'Australie est le seul pays à assurer une cohérence entre les films et le contenu audiovisuel sur Internet en ayant recours à un même système de catégorisation. De son côté, le Royaume-Uni effectue une catégorisation de certains des contenus audiovisuels accessibles sur Internet par mobiles.

3.1.b Création du contenu – classement

La situation du classement est à peu près similaire à celle pour la catégorisation du contenu. Cependant, on note que pour le contenu sur Internet accessible par les mobiles, l'approche du classement y est nettement plus répandue, à tout le moins pour un classement binaire, soit pour moins de 18 ans ou non. Aucune initiative n'est détectée au Canada à cet égard.

3.1.c Homologation

L'homologation du contenu ou de site Web est peu répandue et non uniforme. Les initiatives sont, à l'heure actuelle, toutes d'envergure nationale.

Seule l'Espagne, par le biais de l'Agence de la qualité d'Internet (IQUA), offre une telle homologation, sur une base volontaire, pour les sites Web espagnols. Elle semble avoir un certain succès de par le nombre de sites Web espagnols homologués. Le processus d'homologation actuel se base sur, notamment, le respect des lois espagnoles et ne peut être étendu à l'extérieur de l'Espagne dans son état actuel.

D'autres pays offrent (États-Unis) ou sont sur le point d'offrir (Danemark et France) une homologation partielle du contenu audiovisuel. Ainsi, au Danemark, on prévoit mettre en place à la fin de 2006 une homologation permettant de décerner un sceau « Safe-chat smiley » pour les sites Web de clavardage destinés aux jeunes. En France, on prévoit au début de 2007 mettre en oeuvre une homologation avec un sceau « Label citoyen » permettant de distinguer les sites Web adéquats pour les jeunes. Aux États-Unis, on note une homologation pratiquement obligatoire (basée sur une

loi) des sites Web concernant la protection des renseignements personnels pour les jeunes de moins de 13 ans avec le sceau « Safe Harbor ».

3.1.d Contrôle du contenu - filtrage

Tous les pays offrent, par le biais des producteurs de logiciels de filtrage, la possibilité d'avoir recours, selon une tarification variable ou nulle, à des filtres du contenu audiovisuel afin de protéger la jeunesse. L'Espagne y va même à recommander deux logiciels de filtrage.

En France, un accord a été signé en 2006 entre le gouvernement français et les FAI afin de rendre disponible gratuitement, des logiciels de contrôle parental fonctionnant généralement sur la base de trois profils d'âge : enfant, adolescent et adulte.

Le gouvernement de l'Australie s'apprête à déployer une solution de filtrage accessible gratuitement à toute famille australienne en y investissant plusieurs millions $ AU pour offrir ce choix à ses citoyens. Leur logique de protection de la jeunesse par les filtres s'illustre par cette phrase :

> "You wouldn't send your child out to ride their bike without a helmet, or let them travel in a car without a seatbelt, so why would we let them surf the Internet without the protection of an effective filter? "[243]

Certains pays imposent une obligation ou non auprès des FAI/FSI pour offrir une solution de filtrage. Ainsi, en Australie et en France, ils y sont obligés alors qu'au Canada, au Danemark, Royaume-Uni et aux États-Unis, c'est laissé à leur discrétion. Cependant, au Danemark, on dénote des initiatives non obligatoires : le gouvernement offre gratuitement des solutions de filtrage à toutes les bibliothèques publiques et recommande aux opérateurs de mobiles d'offrir à leurs abonnés une solution de filtrage. Au Royaume-Uni, sans le rendre obligatoire, le gouvernement a fait des pressions sur les FAI pour qu'ils intègrent à leurs services haute vitesse l'accès à un logiciel de filtrage. On dénote, par cette initiative, une certaine fracture numérique favorisée entre les riches et les pauvres car l'accès au service à haute vitesse est plutôt dispendieux au Royaume-Uni.

3.1.e Contrôle du contenu – lutte à la cybercriminalité

La lutte à la cybercriminalité est un des aspects de la gouvernance d'Internet pour la protection de la jeunesse le plus partagé entre tous les pays. Cette gouvernance s'effectue à tous les niveaux possibles de la

[243] Bien que les mesures de protection sont importantes, si on utilise la métaphore de la bicyclette, il faut comprendre que la protection préalable est d'apprendre à monter en bicyclette et apprendre les mesures de prudence en bicyclette (respect de la signalisation, vitesse, pistes utilisées, etc.).

gouvernance : mondial, multilatéral, régional, national, local et auprès de tous les intervenants possibles, à partir du jeune jusqu'aux autorités policières internationales (comme Interpol), en passant par les parents et les autorités policières locales.

La lutte à la cybercriminalité s'effectue à partir de cybersurveillance d'Internet effectuée par les autorités policières et aussi à la suite de cybersignalement de cybercriminalité reçus par ces autorités. Une grande collaboration s'est mise en place entre les autorités policières et autres représentants de la loi tant au niveau local qu'au niveau International.

Ainsi, l'Europe s'est dotée d'une Convention sur la cybercriminalité liant tous les pays[244] et a mis en oeuvre le réseau INHOPE, réseau international de lignes d'urgence ou de « points de contact » (INHOPE - International Association of Internet Hotlines ou Association internationale de services d'assistance en ligne), permettant la cybersurveillance et le cybersignalement. Le Canada fait partie de ce réseau et aussi du réseau international anglophone de cybersignalement Virtual Task Force (par le biais de l'organisme sans but lucratif Cyberaide.ca, financé par le gouvernement du Canada). Cette implication du Canada s'insère dans la « Stratégie nationale pour la protection des enfants contre l'exploitation sexuelle sur Internet ». De plus, en 2002, le Canada a inséré dans son code criminel le leurre d'enfants (luring) comme autre crime.

L'Australie, les États-Unis et le Royaume-Uni font aussi partie du réseau Virtual Task Force.

Au Québec, le Module de la cybersurveillance et de la vigie (MCV) de la Sûreté du Québec s'acquitte de la lutte à la cybercriminalité sur le territoire du Québec en collaboration, notamment, avec la Gendarmerie royale du Canada (GRC) et les services de police locaux.

Une attention particulière est accordée en cybersurveillance aux sites de clavardage car c'est un des lieux les plus périlleux pour les jeunes à cause de la possibilité pour des adultes étrangers avec des intentions malveillantes d'entrer en contact avec des jeunes.

L'objet de la lutte se concentre bien sûr sur la pornographie infantile. Cependant, selon les pays, d'autres formes de cybercriminalité sont ciblées.

On peut mentionner les formes suivantes[245] :

---

[244] Consulter le document n° 2 du Cahier 4 *Convention sur la cybercriminalité* (http://conventions.coe.int/Treaty/fr/Treaties/Word/185.doc)

[245] Plusieurs de ces formes de cybercriminalité sont récentes et ne comportent pas de termes recommandés par l'Office québécois de la langue française et ISOC Québec en propose un terme français non officiel.

- Cyberintimidation / cyberharcèlement (cyber bullying);
- Cyberséduction (cyber grooming);
- Leurre (« luring » - une personne adulte qui se fait passer pour un enfant afin d'inciter un enfant à commettre des actes sexuels, particulièrement lors du clavardage) (Canada);
- Leurre par le biais du nom de domaine afin d'inciter l'enfant à visiter un site Web contenant du matériel nuisible (États-Unis);
- Cyberapologie de l'anorexie et de la boulimie (Espagne);
- Envoi à un enfant de matériel obscène non sollicité (États-Unis).

De plus, un des aspects importants de la lutte à la cybercriminalité est le soutien offert aux victimes de cybercriminalité. Ainsi, on retrouve en Ontario, la présence d'une organisation ayant un rayonnement au niveau mondial, soit le Cyber Law Enforcement Organization (CLEO), qui offre aussi une assistance en ligne aux victimes de la cybercriminalité. Il en va de même aux États-Unis avec l'organisme National Center for Missing & Exploited Children (NCMEC).

Très fréquemment, les organisations qui luttent contre la cybercriminalité font aussi oeuvre de pédagogie afin d'aider à l'alphanétisation des jeunes et des personnes concernées par la protection de la jeunesse.

3.1.f Pédagogie

La pédagogie représente un des éléments de gouvernance d'Internet les plus communs d'un pays à l'autre.

Bien que les gouvernements y interviennent directement pour effectuer la sensibilisation et la formation des éléments relatifs à la cybercriminalité, ils interviennent aussi indirectement en fournissant les moyens financiers aux organisations de la société civile.

Ainsi, l'Europe a mis en place un réseau international de sensibilisation et de formation à Internet, à ses dangers et aux moyens d'y faire face, soit le réseau INSAFE dans le cadre du programme européen « Safer Internet ». C'est le réseau de formation de loin le plus important étudié. Il déborde même l'Europe car l'Australie et le Canada (par le biais de l'organisme Réseau Éducation-Médias) y participent. Il faut souligner la mobilisation importante de la France et du Danemark, qui ont investi énormément d'efforts et d'argent pour mettre en place des mécanismes d'alphanétisation orientés vers la protection de la jeunesse et assurer une certaine pérennité à ces mécanismes.

La société civile est particulièrement active dans ce programme et on y retrouve une pléthore d'organisations sans but lucratif et d'activités plus ou

moins communes. De plus en plus, les organisations qui oeuvrent à l'alphanétisation dans un contexte de protection de la jeunesse segmentent leur programme de sensibilisation et de formation en fonction de l'âge des jeunes. Ainsi, le réseau canadien de sensibilisation et de formation « Web Averti », soutenu par le gouvernement du Canada, la société civile et les entreprises canadiennes, segmente ses interventions selon cinq groupes d'âge (2 à 4, 5 à 7, 8 à 10, 11 à 13 et 14 à 17 ans) afin de tenir compte du développement de l'enfant. En France, on a tendance à segmenter les jeunes en deux groupes d'âge, soit enfant (moins de 10 ans) et adolescent (plus de 10 ans). Cela apparaît une voie importante d'intervention auprès des jeunes, particulièrement pour tenir compte de résultats de sondage auprès des jeunes et aussi pour s'assurer de l'efficacité des programmes de sensibilisation et de formation.

Certains pays ont développé des programmes de formation spécifiques aux secteurs de l'éducation. Ainsi, la France a adapté le curriculum de certains programmes pour y inclure l'acquisition des connaissances et habiletés nécessaires pour naviguer sur Internet d'une façon sûre et responsable. Aux États-Unis et au Canada, deux organismes offrent sur demande des modules de formation pouvant être intégrés dans les écoles ou dans la communauté (selon des frais pour ce qui est du Canada ou gratuitement pour ce qui est des États-Unis). Les États-Unis offrent un programme structuré selon les différentes clientèles possibles (enfants, parents, éducateurs, représentants de la loi et autres adultes concernés) et apparaissent comme un modèle de couverture de clientèle à cet égard. Ils semblent les seuls qui ont un programme destiné spécifiquement pour les représentants de la loi (policiers, etc.) dans le cadre d'un programme intégré. Souvent, les représentants de la loi possèdent une formation spécifique interne ou dans le cadre de leur formation régulière (comme les instituts de formation policière en Ontario).

Un des volets de la pédagogie, qui est ressorti comme besoin de la part des jeunes et qui est, jusqu'à maintenant, très peu couvert, est l'apprentissage de création de contenu par les jeunes, tel qu'exprimé à l'occasion de l'étude MediAppro Europe-Québec. Ce besoin est renforcé par le résultat d'une autre étude au Royaume-Uni où on a constaté que 33 % des jeunes créent déjà du contenu sur Internet. Certaines initiatives ont été détectées mais elles sont rares et encore plus pour ce qui est du contenu audiovisuel ayant recours aux technologies dont les jeunes sont friands, telles que le jeu, la musique et le vidéo. Il est intéressant de souligner le projet Cyberhus du Danemark (« Maison danoise en ligne pour les enfants ») où les jeunes décident du texte, des images, des graphiques, de la navigation et de l'étendue des activités qui y sont conduites. Ce projet leur fournit un sens

d'appartenance et une occasion de participation active comme le veut la tendance d'Internet participatif[246] et ainsi devenir des citoyens actifs.

La consultation de sites Web destinés à l'alphanétisation des jeunes a permis de constater que l'interface utilisateur de tels sites n'était pas toujours adaptée pour intéresser vraiment la clientèle visée tant par sa forme graphique, sa navigation que le vocabulaire adulte ou parental choisi. Certains organismes ont réussi cependant à proposer une interface apparaissant fort bien appropriée, comme le site du Conseil des médias du Danemark ou son projet de Cyberhus.

Si la société civile est très active et présente dans ce volet de la gouvernance, cela s'explique par le financement obtenu à la fois des gouvernements et du secteur privé. Souvent, lorsque les gouvernements font appel à la corégulation ou à la régulation en mode recommandation, ils complètent leur intervention en finançant la réalisation de projets ou d'activités spécifiques d'alphanétisation des personnes concernées par la protection de la jeunesse sur Internet. De plus, les entreprises du secteur privé, souvent regroupées en associations de FAI ou FSI, offrent du soutien technique (par exemple sous la forme de logiciel ou d'hébergement de sites Web d'association) ou des contributions aux organisations sans but lucratif afin de contribuer à l'alphanétisation. La motivation générale du secteur privé provient habituellement de la nécessité de donner suite aux « recommandations » gouvernementales (ou menaces de législation des gouvernements) ou pour répondre à des exigences légales, mais rarement dans le contexte de l'autorégulation.

Il est intéressant de souligner l'existence de deux projets de recherche actuellement en cours au Royaume-Uni pouvant avoir une incidence sur la protection de la jeunesse, soit « Internet Safety Content Agent (ISCA) » et « COMPANIONS ». Le projet ISCA vise à fournir, sans frais pour les fournisseurs de contenu ou de services, du matériel d'alphanétisation permettant ainsi d'atteindre une couverture maximale, plutôt que de tenter de réaliser l'alphanétisation par le biais d'un seul site Web comme c'est souvent le cas à l'heure actuelle. Cette approche aurait plus de chances de rejoindre les jeunes lors de la visite de leurs sites préférés. Le projet COMPANIONS, quant à lui, vise à offrir un environnement d'accès au Web personnalisé selon l'utilisateur, en langue naturelle (qui sera l'anglais) et qui pourrait éventuellement être adapté (mais non prévu au projet) spécifiquement pour les jeunes.

---

[246] Pour plus de détails sur l'Internet participatif, consulter le site Web d'ISOC Québec concernant sa conférence tenue sur le sujet le 3 mars 2006 : www.isoc.qc.ca/tiki-read_article.php?articleId=3

3.1.g Lutte contre pollupostage

Nous l'avons vu, le pollupostage constitue, avec le clavardage, une des plus importantes occasions de risques pour la jeunesse et il nécessite donc une grande attention.

Tous les pays, particulièrement les gouvernements, y ont investi temps et argent. Il est cependant difficile de pouvoir conclure sur l'efficacité de cette lutte, comme d'ailleurs la plupart des autres mesures de protection de la jeunesse, car il y a rarement d'étude de performance avant et après la mise en place d'un programme de lutte contre le pollupostage et, aussi, car le pollupostage est un phénomène évolutif, en ce sens que les polluposteurs affinent leurs techniques et inventent d'autres approches de pollupostage, de sorte qu'il représente une cible mouvante qui rend difficile d'y associer de façon sûre l'efficacité d'un programme. L'OCDE a produit un outil de lutte antipourriel fort complet qui permet de faire le tour de la question et de proposer de multiples pistes de solution[247].

Certains gouvernements ont légiféré pour rendre illégal le pollupostage. C'est le cas de l'Australie (Spam Act), qui y a inclus la défense de collecte des adresses de courriel (farming) ainsi qu'un code de pratiques auprès des FAI/FSI.

---

[247] Pour plus de détails sur l'approche proposée par l'OCDE, consulter le document n° 61 du Cahier 4 *OCDE - ANTI-SPAM TOOLKIT* (www.oecd.org/dataoecd/63/28/36494147.pdf)

C'est le cas aussi de l'Union européenne qui dispose d'une loi (Directive « Vie privée et communications électroniques ») qui rend illégale la prospection par courriel sans consentement préalable (opt-in). Évidemment, cette obligation européenne reste sujette aux pratiques disparates des autres pays non européens. L'Europe dispose de plus d'un réseau des autorités antipourriel (Contact Network of Spam Authorities – CNSA) permettant une certaine coordination entre les pays.

Chacun des pays européens, au-delà de cette directive, peut ajouter un programme national. Ainsi, le gouvernement du Danemark a déployé une stratégie antipollupostage qui a permis, entre autres, d'élaborer et mettre en oeuvre un code de conduite des FSI en matière de pollupostage qui prévoit une obligation d'offrir à leurs abonnés une solution de filtrage de pourriels et une certaine formation inhérente. La France y a ajouté des dispositions concernant le pollupostage dans une loi plus générale sur le commerce électronique (Loi pour la confiance dans l'économie numérique) et a mis en place une association de lutte au pollupostage (Signal Spam) qui réunit les associations, les ministères et les firmes privées. Le site Web de l'association fournit ainsi la possibilité de cybersignalement du pollupostage et de désabonnement (opt-out). Cette possibilité n'est pas répandue dans tous les pays et absente au Canada. Enfin, le Royaume-Uni a mis sur pied une action concertée internationale (Plan d'action de Londres adopté dans plus de 30 pays dont le Canada) visant à promouvoir la coopération internationale sur ce sujet et ses problèmes connexes de cybercriminalité (tels que la fraude en ligne et l'hameçonnage).

Du côté des États-Unis, le gouvernement fédéral a adopté une loi contre le pollupostage (CAN-SPAM Law[248]) rendant obligatoire l'option de désabonnement (opt-out) avec tout pourriel et soutenant un mode de cybersignalement de pourriel par le biais d'une adresse électronique (spam@uce.gov) offert au site Web correspondant, géré par le Federal Trade Commission (FTC). De plus, certains États ont ajouté une législation spécifique.

Du côté du Canada, le gouvernement s'est abstenu de toute législation et recourt à l'autorégulation. Cependant, il a investi de façon importante afin d'offrir des outils de sensibilisation et de formation permettant de se prémunir des risques associés au pollupostage avec le programme « Arrêtez le pourriel ici » (Stop SPAM Here).

[248] Consulter le document n° 52.9 du Cahier 4 *The CAN-SPAM Act: Requirements equirements for Commercial Emailers* (www.ftc.gov/bcp/conline/pubs/buspubs/canspam.pdf)

3.2.a Liberté d'expression

C'est un droit fondamental enchâssé au niveau international et respecté par tous les pays étudiés.

3.2.b Protection des données et de la vie privée

La protection de la vie privée et surtout la protection des renseignements personnels dans tous les pays étudiés s'inscrivent dans les lignes directrices émises par l'OCDE à ce sujet. Chacun des pays dispose d'une loi conforme à ces lignes directrices. Le Canada et le Québec possèdent des lois à cet effet qui sont considérées comme compatibles entre elles et avec celles de l'Union européenne. L'Allemagne et le Canada ont été considérés comme les meilleurs défenseurs de la vie privée selon une étude internationale publiée en novembre 2006. Fait intéressant à signaler, les États-Unis sont le seul pays étudié qui a, sous un mode de corégulation, ajouté une législation spécifique pour protéger la vie privée des enfants de moins de 13 ans (Children's Online Privacy Protection Act) qui est assortie d'une homologation des sites Web (« Safe Harbor »), établie par la société civile et l'industrie, destinée à rassurer cette clientèle du respect de cette loi.

3.2.c Gestion de l'identité et authentification

Le recours à l'authentification de l'internaute pour protéger la jeunesse est un des moyens les moins utilisés. Cette situation n'est pas étrangère aux défis énormes de concilier liberté d'expression, protection de la vie privée et authentification. Même que vouloir implanter une authentification systématique des citoyens a provoqué la chute du gouvernement en Australie à la fin des années 1980[249]. Il y a donc une méfiance de la part des gouvernements et de la société civile à travers le monde sur l'authentification nationale.

Il existe tout de même des initiatives intéressantes à souligner dans certains des pays étudiés[250]. La plus intéressante pour la protection de la jeunesse

[249] Pour plus de détails sur l'expérience vécue en Australie, consulter le document n° 60.4 du Cahier 4 *Arguments contre un système d'identification national* produit par l'organisme « Privacy international » (www.privacyinternational.org/article.shtml?cmd[347]=x-347-61882&als[theme). De plus, l'organisme « Canadian Internet Policy and Public Interest Clinic (CIPPIC) » a produit un état sur la question fort complet et disponible au document n° 60.3 du Cahier 4 *CIPPIC - National ID Cards* (www.cippic.ca/en/faqs-resources/national-id-cards)

[250] L'étude sur les pourriels réalisée par l'OCDE et publiée en 2006 fournit aussi une analyse d'un certain nombre d'approches d'authentification concernant le pourriel. Pour plus de détails, consulter le document n° 61du Cahier 4 *OCDE - ANTI-SPAM TOOLKIT* (www.oecd.org/dataoecd/63/28/36494147.pdf)

sur Internet se situe en Belgique[251]. En effet, la Belgique a mis en place une carte nationale d'identité numérique (« eID ») et a commencé à l'utiliser spécifiquement pour la vérification de l'âge pour les sites de clavardage des jeunes, un des endroits sur Internet où les jeunes sont les plus à risques. L'Europe n'a pas de dispositif d'authentification commun à l'ensemble des pays. Elle aura à faire face à des défis d'interopérabilité à concilier si elle désire une solution commune ou compatible au niveau de toute l'Europe.

Deux autres entités politiques ont mis en place des solutions d'authentification pour tous leurs citoyens et qui pourraient éventuellement être utilisées dans le contexte de la protection de la jeunesse sur Internet si les gouvernements le décident. Il s'agit du Royaume-Uni, avec sa solution d'authentification *UK Government Authentication Gateway*, et de la Colombie britannique, avec sa solution d'authentification « BCeID ».

Du côté du secteur privé, certaines solutions sont proposées ou sont déjà en usage et visent un créneau d'Internet tel que le courriel, le clavardage ou les blogues. Cependant, elles ne présentent pas la même valeur d'authentification : elles permettent de garantir la protection de l'identité numérique en cause et les renseignements personnels rattachés à cette identité numérique mais sans pour autant garantir l'authenticité des personnes possédant cette identité numérique.

L'approche la plus utilisée présentement est Sender ID (développée par Microsoft et libérée récemment des contraintes de droits d'auteur) qui permet, en utilisant les enregistrements du DNS selon une norme de l'IETF, de s'assurer d'une certaine authenticité des courriels reçus et d'ainsi réduire sensiblement les pourriels. Une autre solution proposée par Microsoft est le métasystème d'identité numérique CardSpace qui permet de prendre en compte plusieurs identités numériques pour une même personne. De même, la communauté du logiciel libre présente une approche ouverte, décentralisée et gratuite et qui est en cours de développement pour les blogues avec Open ID.

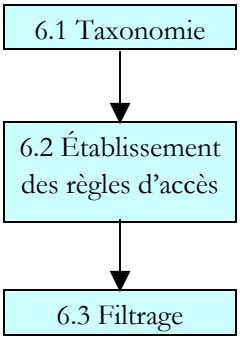
[251] L'Europe étudie actuellement la question et considère d'un bon oeil l'exemple belge.

Enfin, une firme du Royaume-Uni vient de lancer, Net-ID, un nouveau système d'authentification dans le contexte du clavardage, particulièrement destiné aux jeunes. Le Net-ID est une carte d'identité électronique sécurisé, genre de passeport électronique, qui affiche seulement le prénom, l'âge, le genre et la localisation générale afin de permettre de vérifier les personnes avec lesquelles on clavarde. Il est compatible avec les sites de clavardage.

Ceci complète la section sur la gouvernance par pays du contenu audiovisuel sur Internet afin de protéger la jeunesse.

Nous avons traité, durant ce chapitre, du filtrage du contenu, comme un des moyens pour atteindre cette protection. Il a été convenu, au début de l'étude, d'en faire un chapitre spécifique. Étant donné la couverture du sujet dans ce chapitre-ci, le chapitre sur les filtres va davantage porter sur les aspects techniques du filtrage.

6. Codification et filtrage des contenus numériques : inventaire et évaluation



Afin d'établir l'inventaire des filtres et des stratégies actuelles de codification et de classement du contenu sur Internet et d'en réaliser leur évaluation, nous découperons ce chapitre en trois parties.

Tout d'abord, la **taxonomie** (ou structure de codification) des contenus numériques sur Internet, comprenant le **classement selon l'âge** et le **classement selon le type de contenu**, sera examinée et comparée avec celle présentement utilisée par la Régie du cinéma du Québec pour ce qui est des films et vidéos diffusés en public.

Par la suite, nous aborderons l'**établissement des règles d'accès** (ou codification) et le processus de **filtrage** utilisant ces règles d'accès. L'**établissement des règles d'accès** consiste à caractériser le contenu numérique ou l'internaute qui désire accéder à ce contenu. Le résultat de cette phase est désigné par le terme « filtres » ou « règles d'accès » et correspond, globalement aux critères régulant l'accès au contenu sur Internet. Le **filtrage** consiste à appliquer cette caractérisation, principalement, lors de la demande d'accès par l'internaute au contenu numérique. Le résultat de cette phase consiste en l'accès ou non au contenu demandé. Il faut cependant préciser que ce découpage en deux phases (établissement des règles d'accès et filtrage) ne présuppose pas pour autant que le filtrage s'effectue de façon statique, soit une fois seulement pour l'ensemble d'un site Web. Il peut tout aussi bien s'effectuer dynamiquement, soit à chaque fois que l'accès à une page ou un site Web est demandé par un internaute.

.

6.1 Taxonomies et systèmes de codification des contenus

La codification des films et vidéos au Québec repose avant tout sur un classement selon l'âge, accompagnée de quelques éléments de classement selon le type de contenu, alors que la codification des contenus sur Internet a recours davantage à un classement selon le type de contenu, tout en recourant aussi au classement selon l'âge ou aux deux.

Pour des fins de rappel, le système de classement de la Régie du cinéma du Québec est le suivant :

- Visa général – public de tout âge;
- 13 ans et plus;

- 16 ans et plus;
- 18 ans et plus.

Ces classes d'âge peuvent être accompagnées d'indications supplémentaires permettant de préciser la caractéristique dominante du film, soit :

- Pour enfants;
- Déconseillé aux jeunes enfants;
- Langage vulgaire;
- Érotisme;
- Violence;
- Horreur;
- Sexualité explicite.

Si on examine ces indications, on constate que les deux premières se rapportent à l'âge et constituent un détail du « Visa général – public de tout âge », alors que les cinq autres indications, soit langage, érotisme, violence, horreur et sexualité explicite, fournissent des informations sur le type de contenu du film ou vidéo. Ces cinq dernières « indications supplémentaires » correspondent à des types de contenu qui portent, dans le monde d'Internet, diverses désignations telles que étiquettes, descripteurs, catégories et classes. Ainsi, l'Internet Content Rating Association (ICRA) désigne ces types de contenu comme des étiquettes ou des catégories. En fait, dans le monde actuel d'Internet, on n'utilise pas toujours de terme différent pour distinguer le classement selon l'âge et le classement selon le type de contenu et on réfère plutôt au terme « catégorie ».

En général, une taxonomie d'un système de codification basée sur le type de contenu est relativement neutre et peut s'appliquer dans toute culture de tout pays car elle repose essentiellement sur une description factuelle sans autre jugement. Par exemple, attribuer un type spécifique de contenu afin de signifier que le document audiovisuel comporte un démembrement de personne réelle est très factuel. Par contre, même si un type spécifique de contenu est neutre, l'ensemble des types (ou catégories) d'une taxonomie d'un système de codification peut l'être moins selon les critères reliés à chaque type. Ainsi, si on prend le terme « avortement », il pourrait se voir attribuer une catégorie relative à la « sexualité » de façon différente selon les critères retenus par les différents systèmes de codification qui sont influencés par les valeurs sociétales propres au pays où ces systèmes ont été conçus. Ce terme pourrait même se voir attribuer un tout autre type de contenu comme la « santé ». Malgré tout, il y a davantage de chances d'obtenir une certaine objectivité avec une taxonomie basée sur le type de

contenu, si on réussissait à établir un consensus autour d'une telle taxonomie mondiale. Les types, étant davantage factuels, pourraient donc être identiques à travers le monde. Et dans le monde d'Internet, toute codification de contenus numériques pouvant faire l'objet de consensus mondial constitue un grand avantage pour la gouvernance des contenus. C'est donc admettre tout de suite qu'il n'y a pas, actuellement, de taxonomie et de système de codification qui a fait l'objet à la fois d'un consensus mondial **et** d'un large déploiement à l'échelle mondiale.

Une taxonomie basée sur l'âge, quant à elle, est davantage subjective car elle exige un jugement selon les valeurs ou le consensus social (ou étatique selon certaines régions du monde moins démocratiques) du pays, de la province, de l'État ou de toue autre entité politique ou territoriale concernée. Ainsi, un document audiovisuel numérique pourrait se voir attribuer la classe « 16 ans et plus » dans un pays et « 13 ans et plus » ou « 18 ans et plus » dans un autre pays. Il est fort compréhensible donc que l'attribution d'une classe d'âge s'effectuera selon le territoire de l'entité politique concernée. Il n'est cependant pas exclu qu'il puisse exister une certaine collaboration entre États / provinces ou pays qui partagent les mêmes valeurs. Ainsi, au Canada, on observe déjà que les provinces de l'Atlantique partagent le même système de classement des films et il en est de même pour deux provinces de l'Ouest canadien. Il est possible d'envisager certains autres regroupements à travers le monde, tels que les pays nordiques européens qui pourraient s'appliquer aux contenus numériques sur Internet.

Le système de codification est constitué d'un ensemble de systèmes hétéroclites que l'on pourrait regrouper ainsi :

- Systèmes propriétaires;
- Systèmes du « domaine public » ou ayant fait l'objet de consensus;
- Systèmes relatifs à un type particulier de contenu numérique;
- Systèmes relatifs à un type particulier de mode d'accès au contenu numérique;
- Systèmes relatifs aux « listes vertes » et aux « listes rouges ».

6.1.1 Systèmes propriétaires

Les systèmes de codification propriétaires sont les plus nombreux. Ils sont la propriété des producteurs de logiciel de filtrage du contenu sur Internet et leur taxonomie constitue souvent un avantage compétitif. Généralement, le système de codification repose sur une base de données intégrée au logiciel et qui demeure sous le contrôle du producteur de logiciel. Le

nombre de catégories varie énormément. À titre d'illustration, parmi les logiciels les plus populaires, soit de moins de 100 $ CDN, qui s'installent généralement sur un ordinateur personnel et disposent de leurs propres systèmes de codification, on en retrouve dont le nombre de types de contenu varie de 13 à 41 pour ce qui a trait aux logiciels de filtrage des sites Web[252] et de 2 à 18 pour ce qui a trait aux logiciels de filtrage de pourriels[253]. De plus, ces types de contenu, très souvent désignés comme « catégories » par les fournisseurs de logiciel, ne sont pas du domaine public et donc pas toujours accessibles de façon détaillée à des fins d'analyse.

Par contre, les logiciels plus dispendieux et qui s'installent généralement sur un serveur (d'un FAI/FSI, d'une école, bibliothèque ou entreprise) rendent généralement public la taxonomie de leur système de codification.

Ainsi, le logiciel de filtrage Cleanfeed intégré à l'offre d'un FSI du Royaume-Uni rend disponible une telle information. La taxonomie retenue comprend une cinquantaine de types de contenu[254] auquel elle attribue un classement binaire selon l'âge (adulte ou non, soit 18 ans et plus ou non). Ces types de contenus comprennent, par exemple, les catégories « publicité » (pour tous), « alcool » (pour tous) et « pari » (18 ans et plus).

Il en va de même pour le logiciel SmartFilter, offert aux organisations, et qui comprend environ 70 types de contenu (ou catégories)[255]. Avec un nombre aussi impressionnant de catégories, ce logiciel, on le comprend, n'offre pas de classement selon l'âge. La taxonomie retenue incorpore certaines catégories spécifiques afin de se conformer à la loi du gouvernement fédéral américain s'appliquant aux écoles et aux bibliothèques, soit le *Children's Internet Protection Act* (CIPA). Ainsi deux de ces catégories conformes au CIPA sont :

- Pornography (sx)

  This category includes URLs that contain materials that are intended to be sexually arousing or erotic. This includes fetish pages, animation, cartoons, stories, and child pornography.

- Sexual Materials (sm)

---

[252] Consulter le document n° 71.1 du Cahier 4 *Logiciels - 2007 Internet Filter Report* (http://internet-filter-review.toptenreviews.com). Le document n° 35.2 du Cahier 4 *Tests des logiciels des contrôles parentaux* (www.filtra.info/web/resultats.aspx?nav=3) fournit le résultat de test de 24 logiciels sous l'angle du contrôle parental.

[253] Consulter le document n° 71.3 du Cahier 4 *Logiciels contre Pourriels - 2007 SPAM Filter Report* (http://spam-filter-review.toptenreviews.com)

[254] Consulter le document n° 44.10 du Cahier 4 *Service de filtrage Cleanfeed* (www.cleanfeed.co.uk/catlist.php) et le document n° 71.4 du Cahier 4 *Systèmes de codification de contenu sur Internet – Exemples* (www.cleanfeed.co.uk/catlist.php www.securecomputing.com/index.cfm?skey=86#al www.software602.com/products/contentfilter/overview.html)

[255] Consulter la page Web du site de SmartFilter : (www.securecomputing.com/index.cfm?skey=86#al)

> This category includes sites with sexual innuendo, humor, ecommerce, educational or medical descriptions or depictions of sexual acts, specifically those without the intent to arouse. Sites which contain material intended to arouse, fall under the Pornography category.

Il est à noter qu'il est quelque peu surprenant de constater qu'une même catégorie, soit « pornographie », inclut autant du contenu pour adulte que du contenu illégal (pornographie infantile).

De plus, si on examine d'autres catégories de ce logiciel, on en dénote qui correspondent à certains domaines génériques de premier niveau (gTLD) comme « Mobile Phone » (équivalent à « .mobi »), « Non-Profit Organizations » (équivalent à « .org ») et « Travel » (équivalent à « .travel »). Ceci illustre la crainte que le système de nommage du DNS ne veuille plus trop dire quelque chose, du moins à son premier niveau à cause de la liberté d'inscrire n'importe quel site dans les gTLD et donc pas nécessairement là où on s'y attendrait. Ainsi, le système de nommage est peu utile pour trouver les sites Web de voyage si un site Web de voyage spécifique ne s'inscrit pas sous ce premier niveau « .travel » mais plutôt avec « .com » ou « .ca ». Il devient alors nécessaire de refaire la classification des sites par le biais des systèmes de codification, ce qui apparaît comme une perte d'efforts. Mais, en plus, ne pas le faire sur la base d'un consensus international « babelise » énormément la codification des contenus.

La difficulté rencontrée avec une taxonomie propriétaire est souvent amenuisée avec la possibilité offerte aux clients de la modifier en permettant d'ajouter d'autres catégories. Cependant, cela apparaît comme remplacer une difficulté par une autre. En effet, au-delà de la taxonomie, il faut établir les règles d'accès permettant d'apparier le contenu à la bonne catégorie. Or, cet établissement de règles exige énormément d'efforts et de ressources afin d'atteindre un appariement exact. Seuls les grandes organisations ou un regroupement d'organisations peuvent atteindre une qualité d'appariement s'y rapprochant.

La pléthore de taxonomies, soit autant ou presque qu'il y a de logiciel de filtrage, laisse le parent ou l'école devant beaucoup de confusion. Et il devient difficile de partager de l'expertise sur une taxonomie si chaque outil de filtrage a recours à une taxonomie différente.

6.1.2 Systèmes du domaine public

La communauté internationale s'est dotée d'une organisation sans but lucratif qui offre une approche standardisée de codification du contenu des sites Web. Il s'agit de l'*Internet Content Rating Association* (ICRA)

(www.icra.org) qui propose aux propriétaires de sites Web, sur une base volontaire, de réaliser une codification de leur contenu (par page ou site Web), selon une taxonomie comprenant sept catégories ou types de contenu[256] et où chaque catégorie est divisée en sous-catégorie plus explicative et dont le nombre varie de sept à onze. La taxonomie est la suivante :

Catégories	**Sous-catégories**
Nudité	• Poitrine dénudée • Fesses dénudées • Organes génitaux visibles • Aucun des éléments ci-dessus
Contenu à caractère sexuel	• Baisers passionnés • Actes sexuels obscurcis ou implicites • Attouchements sexuels visibles • Langage de nature sexuelle et explicite • Érections/actes sexuels explicites • Érotisme • Aucun des éléments ci-dessus
Violence	• Agression/viol • Êtres humains blessés • Animaux blessés • Personnages imaginaires blessés (dont personnages d'animation) • Sang et démembrement, êtres humains • Sang et démembrement, animaux • Sang et démembrement, personnages imaginaires (dont personnages d'animation) • Torture ou mise à mort d'êtres humains • Torture ou mise à mort d'animaux • Torture ou mise à mort de personnages imaginaires (dont personnages d'animation)

[256] Consulter le document n° 23 du Cahier 4 *Vocabulaire descriptif de l'ICRA* (www.icra.org/vocabulary)

	• Aucun des éléments ci-dessus
Langage	• Injures ou grossièretés • Blasphèmes ou jurons • Exclamations de nature modérée • Aucun des éléments ci-dessus
Activités potentiellement dangereuses	• Scènes de consommation de tabac • Scènes de consommation d'alcool • Scènes de consommation de drogues • Scènes d'utilisation d'armes • Jeux d'argent • Contenu qui donne un mauvais exemple aux jeunes enfants : qui encourage ou apprend aux enfants à réaliser des actes dangereux ou à imiter un comportement dangereux • Contenu qui crée un sentiment de peur, d'intimidation, d'horreur ou de terreur psychologique • Incitation à ou scènes de discrimination ou mauvais traitement à l'encontre d'une personne ou d'un groupe en raison de son sexe, de son orientation sexuelle, de son appartenance ethnique ou religieuse, ou de son identité nationale • Aucun des éléments ci-dessus
Contenu généré par l'utilisateur (tel qu'un forum de discussions)	• Contenu généré par l'utilisateur, comme des forums de discussion ou des tableaux de messageries (modéré) • Contenu généré par l'utilisateur, comme des forums de discussion ou des tableaux de messageries (non modéré) • Aucun des éléments ci-dessus
Contexte (à vocation artistique, éducative ou médicale par exemple)	• Ce contenu apparaît dans un contexte à vocation artistique • Ce contenu apparaît dans un contexte à vocation éducative • Ce contenu apparaît dans un contexte à vocation médicale • Ce contenu apparaît dans un contexte lié au sport • Ce contenu apparaît dans un contexte lié à l'information

À chacune de ces sous-catégories correspond un code. Ainsi, le code « na 1 » est attribué à la sous-catégorie « Poitrine dénudée » de la catégorie « Nudité ». et le code « vi 1 » est attribué à la sous-catégorie « Torture ou mise à mort d'animaux » de la catégorie « Violence ». Ces codes sont transformés en langage reconnu dans le monde du Web, soit le langage RDF normalisé par le W3C, et intégrés dans le site Web concerné. Le site Web rend alors disponible cette codification à tout logiciel (tels que fureteur et engin de recherche) qui y accédera.

L'avantage marqué de l'étiquetage d'un site Web selon l'approche de l'ICRA repose sur le fait que la description du contenu du site Web qui en résulte est accessible à tout logiciel qui veut accéder à ce site (comme les fureteurs et les engins de recherche) alors que l'approche des systèmes de codification propriétaires emmagasine son système de codification dans une base de données propriétaires qui est accessible uniquement par les détenteurs des logiciels correspondants. Il va de soi que l'approche de l'ICRA est intéressante dans la mesure où les logiciels qui accèdent au contenu des sites Web sont en mesure de reconnaître ce langage de codification. Le fait que le plus populaire des fureteurs, soit Internet Explorer, ne reconnaisse pas la taxonomie de l'ICRA, n'est probablement pas étranger au manque de popularité de l'approche ouverte de l'ICRA. Il y a peu d'avantages économiques pour les fournisseurs de systèmes de codification propriétaire à soutenir l'approche ouverte et gratuite de l'ICRA, à moins, par exemple, il y ait des incitatifs de la part des gouvernements et de la société civile.

6.1.3 Systèmes relatifs à un type particulier de contenu numérique

Les jeux, avant l'ère d'Internet, ont fait l'objet de consensus international autour des deux standards, l'un européen et l'autre nord-américain. Ils se sont quelque peu adaptés avec l'accès des jeux par Internet. Cette « internétisation » des jeux peut avoir une influence sur le système de codification du contenu audiovisuel sur Internet.

Le système de classification européen, le PEGI - Pan European Game Information, comprend une classification par âge et une autre par type de contenu. Il comprend les cinq classes d'âge suivantes :

- 3 ans et +;
- 7 ans et +;
- 12 ans et +;
- 16 ans et +;

- 18 ans et +;

et les sept descripteurs de contenu suivants :

- Mauvais langage;
- Discrimination;
- Drogue;
- Peur;
- Pari;
- Sexe;
- Violence.

Le système de codification nord-américain, produit par le ESRB - Entertainment Software Rating Board (www.esrb.org/ratings), comprend une structure semblable mais avec des variantes concernant le nombre de classes d'âges et de descripteurs ou types de contenu. Il comprend les six classes d'âge suivantes :

et trente-deux (32) descripteurs de contenu, soit :

Catégorie	
Étiquette	**Description**
Alcohol Reference	Reference to and/or images of alcoholic beverages
Animated Blood	Discolored and/or unrealistic depictions of blood
Blood	Depictions of blood
Blood and Gore	Depictions of blood or the mutilation of body parts
Cartoon Violence	Violent actions involving cartoon-like situations and characters. May include violence where a character is unharmed after the action has been inflicted
Comic Mischief	Depictions or dialogue involving slapstick or suggestive humor
Crude Humor	Depictions or dialogue involving vulgar antics, including "bathroom" humor
Drug Reference	Reference to and/or images of illegal drugs
Edutainment	Content of product provides user with specific skills development or reinforcement learning within an

	entertainment setting. Skill development is an integral part of product
Fantasy Violence	Violent actions of a fantasy nature, involving human or non-human characters in situations easily distinguishable from real life
Informational	Overall content of product contains data, facts, resource information, reference materials or instructional text
Intense Violence	Graphic and realistic-looking depictions of physical conflict. May involve extreme and/or realistic blood, gore, weapons and depictions of human injury and death
Language	Mild to moderate use of profanity
Lyrics	Mild references to profanity, sexuality, violence, alcohol or drug use in music
Mature Humor	Depictions or dialogue involving "adult" humor, including sexual references
Mild Violence	Mild scenes depicting characters in unsafe and/or violent situations
Nudity	Graphic or prolonged depictions of nudity
Partial Nudity	Brief and/or mild depictions of nudity
Real Gambling	Player can gamble, including betting or wagering real cash or currency
Sexual Themes	Mild to moderate sexual references and/or depictions. May include partial nudity
Sexual Violence	Depictions of rape or other violent sexual acts
Simulated Gambling	Player can gamble without betting or wagering real cash or currency
Some Adult Assistance May Be Needed	Intended for very young ages
Strong Language	Explicit and/or frequent use of profanity
Strong Lyrics	Explicit and/or frequent references to profanity, sex, violence, alcohol or drug use in music
Strong Sexual Content	Graphic references to and/or depictions of sexual behavior, possibly including nudity
Suggestive Themes	Mild provocative references or materials
Tobacco Reference	Reference to and/or images of tobacco products
Use of Drugs	The consumption or use of illegal drugs
Use of Alcohol	The consumption of alcoholic beverages
Use of Tobacco	The consumption of tobacco products
Violence	Scenes involving aggressive conflict

On peut noter, malgré les différences entre les trois systèmes de codification (ICRA, PEGI et ESRB), plusieurs similitudes concernant les types de contenu et particulièrement entre la taxonomie proposée par l'ICRA et celle du ESRB. Avec l'internétisation de l'industrie des jeux, les deux standards de classification des jeux vont devenir davantage en compétition et l'industrie aura tout avantage à fusionner ces deux systèmes. Si cette fusion se produit, il sera très difficile à ce moment-là pour l'ICRA de percer réellement davantage qu'actuellement qui, incidemment, n'a que 200 000 sites Web référencés. Cela exigerait un soutien massif des

gouvernements et de la société civile pour que l'industrie (des logiciels et des producteurs de contenu) migre vers l'ICRA, à moins que le système de codification de l'ICRA évolue pour atteindre une cohérence avec le système de codification des jeux.

6.1.4 Systèmes relatifs à un type particulier de mode d'accès au contenu numérique

Maintenant que les mobiles (et particulièrement les téléphones mobiles) peuvent accéder à Internet et que les jeunes en sont particulièrement friands, il est devenu important d'établir une certaine codification du contenu sur Internet. Les systèmes de codification en cours de mise en oeuvre de par le monde se basent surtout sur un classement selon l'âge, en excluant le Canada qui, pour le moment, n'a pas décidé d'aller de l'avant sur une certaine régulation de l'accès Internet par mobile. En effet, la plupart des pays, à l'exception du Canada, ont convenu de catégoriser le contenu audiovisuel sur une base au moins binaire : soit moins de 18 ans ou non. Certains pays vont plus loin en détaillant la classe des moins de 18 ans. Chaque pays convient des critères qui leur sont propres pour déterminer ce classement. À titre d'illustration, nous examinerons la situation de deux pays, soit le Royaume-Uni et la France, qui ont fait tous deux des choix de classement selon l'âge mais l'un ayant recours à une codification binaire et l'autre une codification plus détaillée.

Au Royaume-Uni, les opérateurs de téléphonie mobile, en mode d'autorégulation (mais fortement incités par les autorités gouvernementales), ont convenu d'un cadre de référence de classification[257] qui détermine le contenu audiovisuel (incluant les jeux) pour les adultes (18 ans et plus) selon la présence ou non des caractéristiques suivantes :

- Thèmes - content must not actively promote or encourage activities that are legally restricted for those under 18 such as drinking alcohol or gambling;
- Langage - frequent and repetitive use of the strongest foul language;

[257] Consulter le document n° 44.6 du Cahier 4 *Système de classification du contenu pour téléphonie mobile* (www.imcb.org.uk/assets/documents/ClassificationFramework.pdf) pour le Royaume-Uni. Aux États-Unis, le choix de classement « binaire » sera vraisemblablement aussi adopté. Voir à cet effet le document n° 52.6 du Cahier 4 *CTIA Board Approved Guidelines* (http://files.ctia.org/pdf/CTIA_Board_Approved_Guidelines.pdf).

- Sexe - actual or realistic depictions of sexual activity, for example,
  - Real or simulated sexual intercourse;
  - Depiction of sexual activity involving devices such as sex toys;
  - Sexual activity with visible pubic areas and/or genitals or including threats of sexual violence such as rape.

  Note, however, that material which genuinely seeks to inform and educate such as in matters of sexuality, safe sex and health and where explicit images are the minimum necessary to illustrate and educate in a responsible manner may be permissible;
- Nudité - nudity where depicting pubic area and/or genitals (unless it is material which genuinely seeks to inform and educate such as in matters of sexuality, safe sex and health and where explicit images are kept to the minimum necessary to illustrate and educate in a responsible manner);
- Violence - graphic violence which in particular dwells on the infliction of pain, injuries or scenes of sexual violence. In respect of mobile games in particular:

  Gross violence towards realistic humans or animals such as scenes of dismemberment, torture, massive blood and gore, sadism and other types of excessive violence.

  Graphic, detailed and sustained violence towards realistic humans and animals or violence towards vulnerable or defenceless humans;
- Drogue - depictions which promote or encourage illegal drug taking or which provide instructive details as to illegal drug taking;
- Horreur - any depiction of sustained or detailed inflictions of pain or injury including anything which involves sadism, cruelty or induces an unacceptable sense of fear or anxiety;
- Technique imitables - dangerous combat techniques such as ear-claps, head-butts and blows to the neck or any emphasis on the use of easily accessible lethal weapons, for example knives.

  Detailed descriptions of techniques that could be used in a criminal offence.

En France, une recommandation, déposée en octobre 2006, sera vraisemblablement acceptée par le gouvernement français après y avoir apporté éventuellement ou non des modifications. Elle demeure intéressante à souligner par les choix qu'elle contient. Le système de classement est le suivant[258] :

- « tous publics »;
- « -12 » ou « déconseillé aux moins de 12 ans »;
- « -16 » ou « déconseillé aux moins de 16 ans »;

[258] Consulter le document n° 36 du Cahier 4 *Classification des contenus multimédias mobiles* (www.foruminternet.org/telechargement/documents/reco-CCMM-20061017)

- « -18 » ou « réservé aux adultes ».

Cette recommandation fournit, de façon similaire au Royaume-Uni, des critères d'attribution des classes, soit :

- « tous publics » - contenus qui ne relèvent d'aucun des types de contenus énoncés plus bas, et ne présentant aucun risque pour le développement psychique et moral des mineurs;
- « -12 » ou « déconseillé aux moins de 12 ans » - services dont les contenus comportent des représentations ou descriptions de scènes à caractère sexuel, de violence physique ou psychologique, ou susceptibles d'inciter les mineurs de 12 ans à commettre des actes dangereux ou réprouvés par la société. Les services dont les contenus font systématiquement l'emploi d'un langage grossier sont également classés « déconseillés aux moins de 12 ans »;
- « -16 » ou « déconseillé aux moins de 16 ans » - services dont les contenus comportent des représentations et descriptions de scènes visant à l'excitation sexuelle de l'usager, de grande violence, ou susceptibles d'inciter les mineurs de 16 ans à commettre des actes dangereux ou réprouvés par la société. Les services dont les contenus font systématiquement l'emploi d'un langage cru, ordurier ou obscène sont également classés « déconseillés aux moins de 16 ans »;
- « -18 » ou « réservé aux adultes » - contenus comportant des représentations ou des descriptions de scènes à caractère pornographique, de scènes de très grande violence, ou d'actions susceptibles d'inciter les mineurs à commettre des actes illégaux ou réprouvés par la société. Il s'agit notamment des contenus relevant de l'article 227-24 du Code pénal, qui interdit la diffusion de « messages pornographiques, violents ou portant gravement atteinte à la dignité humaine » lorsqu'ils sont susceptibles d'être vus ou perçus par des mineurs.

La recommandation fournit une explication encore plus détaillée des critères par classe d'âge selon le niveau des quatre types de contenus retenus, soit la nudité/sexe, la violence, le langage et le danger potentiel (tel que pari).

Ce choix de classement est justifié en France par l'objectif de maintenir une cohérence avec les classements des autres médias, soit télévision, cinéma et jeux vidéo (particulièrement le PEGI). Le choix de ne pas détailler davantage la classe des « moins de 12 ans » s'explique principalement par le fait que les opérateurs de téléphonie mobile ne recommandent pas un tel appareil à ces jeunes et par l'objectif de simplifier quelque peu la vie à ces opérateurs.

6.1.5 Systèmes relatifs aux « listes vertes » et aux « listes rouges »

Tout d'abord, il convient de préciser les termes « listes vertes » et « listes rouges ». Très souvent dans la littérature anglophone et dans les logiciels correspondants, on retrouve les termes « listes blanches » et « listes noires » comme outil pour protéger la jeunesse sur Internet. Ces derniers termes peuvent représenter une connotation raciste pour certains et on observe, en France particulièrement, que le terme « liste blanche » est remplacé par « liste verte ». Étant donné que la métaphore des feux de signalisation (rouge, on arrête et vert, on y va) est une façon de représenter les couleurs qui fait consensus au niveau international et que ces deux couleurs se retrouvent dans la plupart des systèmes de classification de films correspondant à « pour tous » et « pour adulte seulement », nous proposons d'y adhérer pour désigner ces listes. Les « listes vertes » représentent les listes des sites Web pour lesquels les jeunes peuvent y accéder (moins de 18 ans) et les « listes rouges », le contraire (18 ans et plus). La taxonomie binaire utilisée (verte ou rouge) correspond à celle retenue pour les mobiles au Royaume-Uni (moins de 18 ans et 18 ans et plus).

6.1.6 Conclusion sur la taxonomie et les systèmes de codification

On peut noter, dans les deux tableaux suivants, les similarités et les différences entre les taxonomies de la Régie du cinéma, des deux standards des jeux et des deux pays en matière de mobiles. Le système du ESRB, avec ses 32 types de contenu, est beaucoup trop détaillé pour y être comparé, sauf pour ce qui a trait à la codification selon l'âge. Il en va de même pour les systèmes propriétaires de codification.

Régie du cinéma	PEGI	ICRA	Mobile - RU	Mobile - France
Langage vulgaire	Mauvais langage	Langage	Langage	Langage
Érotisme	Sexe	Nudité	Nudité	Nudité/sexe
Sexualité explicite		Contenu à caractère sexuel	Sexe	
Violence	Violence	Violence	Violence	Violence
Horreur	Peur		Horreur	
	Discrimination			
		Activités potentiellement dangereuses (alcool, pari, armes, ...)	Thèmes (tels que alcool et pari)	Danger potentiel (tel que pari)
	Pari			
	Drogue		Drogue	
			Technique imitables (ex. : attaque à coups de couteau)	
		Contenu généré par l'utilisateur (tel qu'un forum de discussions)		
		Contexte (à vocation artistique, éducative ou médicale par exemple)		

Tableau 6.1 - Comparaison des taxonomies selon le type de contenu

Régie du cinéma	PEGI	ESRB	Mobile - RU	Mobile - France
Visa général – public de tout âge	3 +	3+	18-	Tous publics
	7+	6+		
13 ans et plus	12+	10+		- 12
16 ans et plus	16+	13+		- 16
		17+		
18 ans et plus	18+	18+	18+	- 18

Tableau 6.2 - Comparaison des taxonomies selon l'âge

Dans le prochain tableau, on retrouve quatre caractéristiques des systèmes de codification, soit :

- le niveau de granularité de codification (par pays ou site Web);
- le mode d'enregistrement du résultat de la codification (inséré au contenu sous forme d'étiquette ou enregistré dans une base de données propriétaire);
- l'adéquation de la taxonomie pour prendre en compte le contenu audiovisuel numérique;
- la prise en compte des classes d'âge et des types de contenu.

Critères	PEGI	ESRB	Mobile - RU	Mobile - France	ICRA	Syst. propr.
Codification par page Web	non	non	non	non	oui	non
Codification par site Web	oui	oui	oui	oui	oui	oui
Codification insérée au contenu [259]	oui	oui	non	non	oui	non
Codification insérée dans une BD propriétaire	non	non	oui	oui	non	oui
Adéquation au contenu audiovisuel sur Internet	partielle	partielle	limitée	oui	oui	oui
Prise en compte des classes d'âge	oui	oui	limitée	oui	non	non
Prise en compte des types de contenu	oui	oui	limitée	oui	oui	oui

Tableau 6.3 - Comparaison des systèmes de codification

Pour ce qui est des systèmes de codification selon l'âge, on peut constater la correspondance exacte des systèmes de codification de la Régie du cinéma des mobiles en France et une presque équivalence entre la Régie du cinéma et le PEGI.

Pour ce qui est des systèmes de codification selon le type de contenu, on peut constater que les cinq types de contenu de la Régie du cinéma se

[259] Il est pris pour hypothèse que l'internétisation des jeux s'effectue en étiquetant la version Internet des jeux, à défaut de boîtier. Mais il pourrait aussi y avoir tout simplement une simple notice, comme sur les boîtiers des jeux, lisible uniquement par une personne et non un logiciel.

retrouvent à peu près de façon identique dans les systèmes de codification du PEGI et des « Mobiles – RU ». De façon plus détaillée, on retrouve :

- une correspondance exacte entre tous les systèmes concernant deux des types, soit « violence » et « langage »;
- une équivalence concernant le type relatif à la sexualité qui se retrouve détaillé en 1 ou 2 types mais qui se résume à trois libellés, soit « sexe », « nudité » et « érotisme » où seule la Régie du cinéma présente le libellé « érotisme » et seuls le PEGI et Mobile – France ne comporte qu'un seul type pour décrire la sexualité, soit « sexe » ou « nudité/sexe »;
- les libellés « sexe » et « nudité » sont les plus fréquents;
- le type de contenu « horreur » ou « peur » se retrouve dans trois des cinq systèmes présentés, soit Régie du cinéma, PEGI et « Mobiles – RU »;
- seul le PEGI comporte un type de contenu relatif à la « Discrimination ». Cette particularité s'explique peut-être par le fait que c'est considéré comme illégal par les détenteurs des autres taxonomies et qu'il a été établi que l'on ne codifie pas le contenu illégal (comme la pornographie infantile);
- on observe beaucoup plus de variation pour codifier le contenu concernant les thèmes relatifs à l'intégrité physique des personnes (alcool, pari et armes);
- il y a deux types de contenu spécifiques à l'ICRA, soit « Contenu généré par l'utilisateur (tel qu'un forum de discussions) » et « Contexte (à vocation artistique, éducative ou médicale par exemple) ». Le premier type devient de plus en plus important dans le monde d'Internet avec la tendance concernant l'Internet participatif et l'interactivité avec les jeunes. Le second type est fort important afin de détecter, par exemple, si le contenu constitue de l'éducation sexuelle. La prise en compte correcte de ce type de contenu devient cruciale dans le contexte de la protection de la jeunesse car justement l'accès à ces contenus permet à ces jeunes de mieux se protéger.

À titre de conclusion sur l'ensemble des systèmes de codification du contenu, on peut faire le constat de leur « babelisation ». Par contre, on peut observer une certaine convergence pour ce qui est des systèmes de codification du domaine public et des jeux. Le choix de la France de la codification d'Internet pour les mobiles s'y rapproche.

De prime abord, il se dégage un début de consensus de codifier le contenu pour la protection de la jeunesse dans le contexte de l'accès par mobiles. Il est donc envisageable que ce consensus se généralise auprès de tous les pays et, éventuellement, tous les contenus audiovisuels sur Internet. Il est trop tôt pour prédire quelle taxonomie l'emportera. La taxonomie binaire, soit selon l'âge - « moins de 18 ans » et « 18 ans et plus », représente un

minimum à atteindre mais insuffisant pour vraiment protéger la jeunesse et particulièrement les plus jeunes. Par contre, l'approche de système de codification par pays apparaît peu pratique pour des utilisateurs de mobiles qui ... se déplacent d'un pays à l'autre, justement !

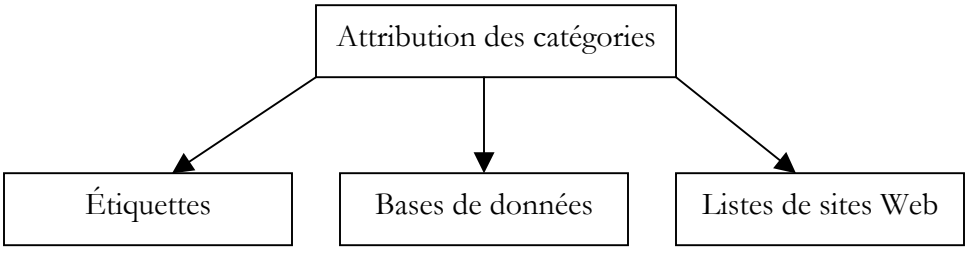
6.2 Établissement des règles d'accès

Les règles d'accès, de filtrage, ou de confiance devant servir à déterminer, lors du « filtrage », si un contenu peut être accessible à un internaute spécifique, correspondent à une caractérisation du contenu, de l'internaute ou du temps de l'internaute à consulter le contenu. Ces règles se regroupent sous les cinq volets suivants :

- Filtre;
- Homologation;
- Authentification;
- Temporalité;
- Profil.

6.2.1 Filtre

Nous avons vu, dans la section précédente, les diverses taxonomies des systèmes de codification en usage. Cette taxonomie sera utilisée dans une partie des stratégies de filtre et donc, du filtrage qui s'en suivra par la suite. Les filtres correspondent aux règles opérationnelles devant servir au filtrage. Les quatre éléments des règles peuvent être représentés ainsi :



- L'attribution des catégories;
- L'étiquetage des sites/ pages Web;
- La constitution des bases de données;
- L'établissement de listes de sites Web.

L'attribution des catégories

L'attribution des catégories consiste à déterminer de façon précise la façon dont sera codifié le contenu d'un site Web ou la façon dont sera apparié le contenu d'un site Web à une catégorie de la taxonomie choisie. Elle se fait de façon plus ou moins ouverte ou transparente selon le système de codification utilisé.

Ainsi, pour le contenu destiné à transporter une étiquette avec lui sur Internet, tel que dans le cas du système de codification proposé par l'ICRA, l'attribution des catégories est déjà explicite et complète en soi par la définition même de sa taxonomie. Il devrait y en être de même pour ce qui est des jeux qui devraient aussi transporter leur étiquette de codification avec eux. De plus, certains systèmes de codification propriétaires n'exigent pas de précision additionnelle pour l'attribution des catégories car celle-ci s'effectue par une personne, tout comme dans le cas des jeux.

Par contre, pour les systèmes propriétaires de codification qui automatisent cette attribution des catégories, il est nécessaire de détailler leurs règles afin d'apparier un contenu à un type spécifique de contenu. Pour ce faire, les producteurs de logiciel ont recours à des « filtres » ou critères détaillés d'attribution des catégories, filtres qu'un logiciel pourra traiter par la suite. Généralement, ces filtres ne sont pas publics ou non modifiables.

Ainsi, si on se réfère au système de codification du logiciel de filtrage CleanFeed[260] et que l'on considère la catégorie « explicite sexuellement » portant la description littérale « sites d'une nature sexuelle explicite », on constate que l'explication de la catégorie ne nous informe pas tellement plus que le libellé de la catégorie et qu'un logiciel de filtrage aura besoin de plus d'information pour pouvoir apparier automatiquement un site Web à une catégorie (ou type de contenu). À cette fin, le producteur du logiciel pourra recourir à un certain nombre de techniques plus ou moins élaborées et coûteuses, telles que les mots-clés, la reconnaissance d'images, un système expert de reconnaissance de contexte, etc. Ces techniques constitueront les règles d'attribution des catégories et qui seront utilisées par la suite pour le filtrage.

---

[260] Consulter le document n° 71.4 du Cahier 4 *Filtres – Systèmes de codification* (www.cleanfeed.co.uk/catlist.php
www.securecomputing.com/index.cfm?skey=86#al
www.software602.com/products/contentfilter/overview.html)

C'est justement dans cet « ajout d'intelligence » au système de codification, généralement non accessible au public, que peut s'installer le plus grand biais. Et, tel que rapporté en 2006 dans une méta-analyse de la performance des logiciels de filtrage réalisée par le Brennan Center for Justice de l'université de New York, on peut se retrouver avec des résultats imprévisibles tels que la Déclaration d'indépendance des États-Unis (le « We, the people »), l'oeuvre de Shakespeare et le roman d'Ernest Hemingway (*Moby Dick*) codifiés comme étant de la catégorie « pornographie » ! Ces techniques de codification automatique font en sorte que les logiciels de filtrage, basés sur des systèmes de codification propriétaires, bloquent trop de sites Web qui devraient être normalement accessibles aux moins de 18 ans et ne bloquent pas tous les sites Web qui ne devraient pas être accessibles aux moins de 18 ans. C'est ce qu'on désigne par le sur ou sous-filtrage. Ainsi, les résultats d'une étude conduite en 2002[261] concernant le blocage ou non du contenu relatif à l'éducation sexuelle, ont permis de démontrer que les logiciels de filtrage peuvent prendre pour de la pornographie le contenu relatif à l'éducation sexuelle dans une proportion de 1,4 % à 24 % selon les paramètres fournis aux logiciels de filtrage alors qu'ils prennent pour du contenu anodin certains contenus pornographiques dans une proportion d'environ 10 %.

L'étiquetage des sites / pages Web

Dans le contexte du système de codification de l'ICRA, l'étiquetage consiste à insérer sur chaque page Web ou pour l'ensemble du site Web, les étiquettes générées par le système de codification de l'ICRA (selon le langage normalisé RDF) sur la base des informations descriptives fournies par le détenteur du site Web et ce, sans autre artifice de transformation. Ces étiquettes insérées dans le site Web, une fois publié sur Internet, seront accessibles à tout logiciel accédant à ce site Web.

---

[261] Consulter le document n° 2 du Cahier 5 *See-No-Evil-How-Internet-Filters-Affect-the-Search-for-Online* (www.kff.org/entmedia/3295-index.cfm) ou le document n° 1 du Cahier 5 *Internet Filters : A Public Policy Report* (pp. 62 à 64) (www.fepproject.org/policyreports/filters2.pdf)

La constitution des bases de données

Les systèmes de codification propriétaires ont généralement recours à leur propre base de données pour enregistrer la codification des sites Web en conformité avec les règles d'attribution des catégories. Cette base de données sera intégrée au logiciel de filtrage concerné et nécessitera des mises à jour périodiques pour tenir compte de l'évolution des sites Web. Typiquement, ces bases de données comprennent les informations suivantes :

- Nom du site Web;
- Catégorie(s) attribuée(s).

Elles peuvent aussi contenir d'autres informations de gestion telles qu'une date permettant de déterminer si cette codification nécessite une mise à jour.

L'établissement de listes de sites Web

Dans le contexte où il est prévu offrir la possibilité de gérer l'accès aux sites Web au moyen de « listes vertes » ou « listes rouges », le producteur du logiciel constitue ces deux listes selon les règles d'attribution des catégories qu'il a retenues. Ces listes peuvent être établies par des personnes ou des logiciels. Bien qu'il est possible de constituer cette liste par page Web, généralement, ces listes sont établies par sites Web. Ces listes sont intégrées aux logiciels de filtrage ou autres logiciels de contrôle d'accès et nécessitent donc des mises à jour périodiques. Ainsi, en France, le gouvernement a confié à une université de Toulouse[262] la responsabilité d'établir la « liste rouge » qui a recours à la fois à des automates logiciels et des personnes pour mettre à jour cette « liste rouge ». L'initiative de la France d'établir une telle liste sur une base nationale est intéressante car elle réduit la variation d'un logiciel à l'autre dans le cas où ces logiciels ont intégré cette liste nationale. Les « listes vertes » peuvent être très utiles pour certains logiciels de gestion des accès comme un portail pour enfants. Cependant, encore là, un portail comprenant une liste de sites Web pour moins de 18 ans, correspondant aux « listes vertes », a peu de chance d'attirer les jeunes car cela exige une segmentation plus fine par tranche d'âge telle que moins de 7 ans, moins de 12 ans et moins de 16 ans.

[262] Consulter la page Web de la « liste noire » d'ÉducNet du ministère de l'Éducation de la France : www.educnet.education.fr/aiedu/listenoire.htm

Selon le logiciel utilisé ou l'approche de codification retenue, on peut donc retrouver le même site Web codifié de plusieurs façons de sorte qu'il peut arriver que l'accès soit autorisé avec un logiciel et bloqué avec un autre ou que le site Web soit classé dans des catégories différentes d'un logiciel à l'autre.

6.2.2 Homologation

Dans le contexte de la protection de la jeunesse, tel que couvert dans le chapitre précédent, il est possible d'homologuer les sites Web pour la jeunesse :

- de façon générale;
- de façon spécifique, sur un thème particulier.

Ainsi, il est possible de réaliser une **homologation** de façon **générale** pour tout un site avec la préoccupation des enfants. C'est habituellement réalisé par des organismes de protection de la jeunesse qui auront aussi la responsabilité d'offrir un environnement spécifique aux enfants, tel qu'un portail pour enfants. Cette homologation peut être plus ou moins formelle (avec un sceau ou pas) et être détaillée ou non par tranche d'âge. Ainsi, le projet de la France d'élaborer un sceau « Label citoyen » va dans le sens d'une homologation générale de sites Web pour enfants.

Il est aussi possible de réaliser une **homologation spécifique** concernant une partie particulière de la protection de la jeunesse. Ainsi, nous avons vu que les États-Unis offrent une homologation avec le sceau « Safe Harbor » destinée aux sites Web concernant la protection des renseignements personnels pour les jeunes de moins de 13 ans. De même, le Danemark s'apprête à mettre en place un sceau « Safe-chat smiley » pour les sites Web de clavardage destinés aux jeunes.

Actuellement, ces homologations décernées ne semblent pas codifiées dans le site Web mais apparaissent visuellement sur la première page du site Web. Ce qui signifie qu'actuellement, il n'y a pas de logiciel de gestion d'accès qui pourrait reconnaître automatiquement les sites détenant de tels sceaux d'homologation.

6.2.3 Authentification

L'authentification peut s'appliquer à un objet, tel qu'un courriel, ou à un internaute.

L'**authentification d'un objet** qui occupe le plus de visibilité présentement concerne les courriels selon l'approche proposée par Microsoft avec SenderID, Cette approche permet de réaliser une certaine authentification de l'émetteur de courriel en se basant sur la structure même du DNS.

L'**authentification de l'internaute** vise à s'assurer de la véracité de l'identité de l'internaute et de certaines de ses caractéristiques telles que l'âge. Dans le contexte de la protection de la jeunesse, certaines informations deviennent plus sensibles telles que l'âge pour s'assurer, par exemple, que des prédateurs sexuels ne leurrent pas les jeunes sur des sites de clavardage ou de blogues destinés aux jeunes. Cependant, il y a une tendance qui peut apparaître risquée à suivre, c'est de constituer des sites de clavardage où seuls les jeunes peuvent y accéder. Comme le souligne un document d'orientation du Danemark, il ne faut pas, sous le prétexte de la protection de la jeunesse, couper tout lien électronique entre les jeunes et les adultes et qu'il faut, au contraire, privilégier les occasions d'échange entre jeunes et adultes. Le concept de mentorat ou de tutorat peut y être appliqué avantageusement, à la condition de le gérer adéquatement afin, notamment, d'identifier explicitement le statut de chaque personne, tout en protégeant les renseignements personnels de chaque personne.

L'authentification peut s'effectuer de deux façons actuellement :

- par le biais des systèmes d'authentification nationale (SAN);
- par le biais des systèmes de vérification d'âge (AVS – Adult/Age Verification System).

Systèmes d'authentification nationale (SAN)

Actuellement, les gouvernements déploient, de façon variable chacun de leur côté, des efforts pour mettre en oeuvre des solutions d'authentification nationale des citoyens pour la prestation de services électroniques. Cette authentification est habituellement conçue pour le citoyen adulte et donc pas nécessairement adaptée pour les jeunes. Par contre, au Canada, on retrouve la Colombie britannique qui est à déployer un SAN, soit le « BCeID », pour tous ses citoyens, jeunes et adultes. Elle pourrait éventuellement s'en servir à des fins de protection de la jeunesse. Et, tel que nous l'avons vu au chapitre précédent, la Belgique a utilisé spécifiquement son SAN (« eID ») à des fins de vérification de l'âge afin de gérer l'accès d'un site de clavardage réservé aux jeunes.

Systèmes de vérification d'âge (AVS – Adult/Age Verification System)

Il existe, au niveau international, plusieurs offres de systèmes de vérification d'âge. Ces offres proviennent en très grande majorité du secteur privé[263]. Cependant, leur vérification d'âge adulte (18 ans et plus) s'effectue sur la base de la détention d'une cadre de crédit et d'avoir coché une case d'un formulaire électronique indiquant que l'on a effectivement 18 ans ou plus. Cela est plutôt mince comme procédure de vérification, d'autant plus que certains jeunes détiennent leur propre carte de crédit ou peuvent, disons, emprunter la carte de crédit de quelqu'un d'autre (comme leurs parents !). Ce système donne davantage bonne conscience aux détenteurs de sites Web pornographiques et les protège de poursuites judiciaires éventuelles. Mais ce système privé ne protège pas vraiment les jeunes.

Par contre, le gouvernement de l'Australie a mis en place son propre système de vérification d'âge[264], soit le « Restricted Access Systems Declaration », où la confirmation d'âge est exigée au moyen de pièce justificative légale. Bien que l'on ignore son degré de popularité, c'est un type de système de vérification d'âge qui donne réellement confiance à la vérification qui en résulte et au NIP (numéro d'identification personnel) qui est fourni.

6.2.4 Temporalité

La première préoccupation des parents, selon plusieurs sondages tant en Europe qu'en Amérique du Nord, est, non pas le contact potentiel de leurs enfants avec la pornographie, mais plutôt la quantité de temps qu'ils passent sur Internet. C'est pourquoi les parents peuvent décider d'accorder à leurs enfants des plages horaires et un nombre limite d'heures par jour ou semaine. La détermination de cette règle, pour qu'elle réussisse, a avantage à être établie en transparence avec le jeune et encore plus lorsqu'il vieillit. Car il est facile pour le jeune qui se considère brimé de visiter un copain de classe ou un voisin ayant des parents « plus conciliants » concernant l'accès à Internet.

---

[263] Consulter le document n° 67 du Cahier 4 *AVS - Liste de systèmes* (www.funfone.com/netsex/linkindex.shtml)

[264] Consulter le document n° 66 du Cahier 4 *AVS - Age verification system* (www.acma.gov.au/ACMAINTER.1507598:STANDARD::pc=PC_90159).

6.2.5 Profil

Le concept de profil, soit l'identification de l'internaute et la description des services ou informations auxquels il a droit d'accéder, est habituellement utilisé dans les entreprises ou le gouvernement. Cependant, il pourrait éventuellement être utilisé par les institutions ayant une clientèle de jeunes telles que les écoles et les bibliothèques. Le recours au profil permettrait, par exemple, d'établir un accès modulé par tranche d'âge (par exemple, moins de 7 ans, moins de 12 ans, moins de 16 ans et 18 ans et plus). Cela aurait avantage de gérer l'accès selon l'âge et de motiver davantage le jeune à utiliser Internet à l'école. En effet, selon une étude récente réalisée au Québec[265], alors qu'en 2000, les 2/3 des jeunes disaient utiliser Internet à l'école, en 2006, la très grande majorité affirmait ne pas l'utiliser. L'explication fournie par les jeunes : trop de contrainte d'accès les empêchant d'utiliser les sites Web qu'ils utilisent à la maison (comme pour le clavardage). Il peut aussi y avoir d'autres explications telles que les règles d'accès identiques sans égard à l'âge des jeunes : un jeune de 15 ans n'apprécie guère n'avoir pas plus d'accès qu'un jeune de 5 ans. Par contre, fournir à tout jeune l'accès à tous sites Web pour moins de 18 ans, ne protège pas nécessairement adéquatement les plus jeunes. Le profil pourrait donc être utile à cet effet, d'autant plus que les écoles et les bibliothèques disposent déjà de renseignements personnels vérifiés concernant l'âge, par exemple. Il ne s'agirait que d'en étendre l'utilisation et le consentement correspondant.

Le tableau suivant résume les différences concernant la facilité de mise en œuvre et la possibilité réelle de protection de la jeunesse entre les cinq volets de l'établissement des règles d'accès.

---

[265] Cette baisse d'utilisation d'Internet à l'école semble s'expliquer par les contraintes d'accès installées dans les écoles. Consulter le document n° 48.1 du Cahier 4 *The Appropriation of New Media by Youth* (www.mediappro.org/publications/finalreport.pdf)

Volets	Facilité de mise en oeuvre	Possibilité de protection
Filtre	Faible	Moyenne
Homologation :		
• générale	Élevée	Élevée
• spécifique	Moyenne	Élevée
Authentification :		
• système national (SAN)	Faible	Élevée
• système de vérification d'âge (AVS)	Élevée	Faible
Temporalité	Élevée	Élevée
Profil	Moyenne	Élevée

Tableau 6.4 – Comparaison des volets d'établissement des règles d'accès

6.3 Filtrage

Les deux étapes précédentes maintenant complétées, soit l'établissement de la taxonomie et des règles d'accès, il s'agit d'activer le filtrage pour permettre l'accès au contenu audiovisuel sur Internet aux jeunes, selon les paramètres retenus. Cette activation du filtrage peut s'effectuer selon les modes suivants, principalement par le biais de logiciels :

- portail pour les jeunes;
- moteur de recherche;
- logiciel de filtrage de sites Web;
- vérification de l'identité / âge;
- modération des forums / blogues / clavardage;
- logiciels de filtrage des contenus créés;
- logiciel de filtrage des pourriels;
- logiciel de contrôle parental;
- filtrage visuel.

6.3.1 Portail pour les jeunes

Une des façons de protéger la jeunesse sur Internet est de constituer un portail comprenant uniquement des sites Web considérés comme sûrs pour les jeunes.

Ces portails peuvent utiliser certains des résultats des diverses règles d'accès définies à la section précédente, tels que les « listes vertes », les sites homologués sûrs pour les jeunes et les sites Web des bases de données correspondant aux catégories appropriées pour les jeunes.

Il est important de souligner que la réussite de tels portails repose sur certains critères dont, notamment, une interface utilisateur adaptée à la clientèle de jeunes, une segmentation selon l'âge, une richesse de sites Web disponibles, des commodités de communication favorites des jeunes (telle que le clavardage) et une évolution dynamique du portail.

Deux exemples semblent satisfaire ces critères, soit le projet de *Maison danoise en ligne pour les enfants* ou Cyberhus conçu pour et par les jeunes et le site Web torontois TakingITGlobal, dirigé par les jeunes et ayant une portée internationale.

D'autres initiatives, avec une participation plus ou moins active des jeunes, existent provenant soit d'autorités gouvernementales soit d'organisations sans but lucratif.

6.3.2 Moteur de recherche

Les sources de sites Web pouvant servir aux portails pour les jeunes peuvent aussi servir comme base de référence aux moteurs de recherche. Les règles d'accès établies à la section précédente peuvent aussi être utilisées de façon dynamique pour décider uniquement lors d'une recherche spécifique quels sites seront accessibles ou pas. Si le moteur de recherche ne possède pas de facilité pour tenir compte de l'âge du jeune, il supposera qu'il cherchera dans tout site qui convient pour les moins de 18 ans. S'il dispose de l'âge et que les règles d'accès sont détaillées par tranche d'âge, il pourra aussi affiner la recherche selon la tranche d'âge de l'internaute.

Ainsi, on retrouve des moteurs de recherche adaptés pour les jeunes (désignés souvent comme l'option « Safe Search ») dans les moteurs comme Google, Yahoo[266], Dogpile et MSN.

---

[266] Consulter le document n° 69 du Cahier 4 *Moteur de recherche pour enfant* (http://kids.yahoo.com) et le document n° 70.1 du Cahier 4 *Portail pour enfants* (www.parentalfilter.fr/annuaire)

6.3.3 Logiciel de filtrage des sites Web

Les logiciels de filtrage sont les logiciels les plus populaires pour effectuer le filtrage du contenu sur Internet. Ils utilisent les règles établies ou les résultats de ces règles, selon qu'ils fonctionnent de façon statique (à partir de bases de données ou de listes établies) ou dynamique (en appliquant les règles d'accès à chaque fois qu'un accès est demandé).

Ces logiciels représentent probablement l'activité économique la plus importante de l'industrie du logiciel de protection de la jeunesse. Les stratégies de filtrage deviennent de plus en plus sophistiquées et étendues. Ainsi, il est maintenant fréquent que ces logiciels intègrent le filtrage selon les « listes vertes » et les « listes rouges » ainsi que le filtrage selon le type de contenu (ou catégories). De plus, ces logiciels tendent à intégrer la prise en compte du contexte du site Web afin de réduire le sur et le sous-filtrage par le biais de système de traitement de la langue. Il en va de même pour certains logiciels qui réalisent de la reconnaissance d'images (notamment pour détecter les catégories relatives au sexe). Cependant, il restera toujours difficile de réaliser parfaitement le filtrage à cause de la difficulté de distinguer adéquatement le contexte à prendre en compte et encore plus avec les sites Web dans des langues autres que l'anglais. Ainsi, la taxonomie de l'ICRA comporte une catégorie réservée au contexte éducationnel afin de tenter d'éviter le piège de bloquer du contenu destiné à l'éducation (sexuelle, civique, environnementale, respect des minorités, etc.).

De plus, certains logiciels utilisés par les représentants de la loi pour détecter la pornographie infantile dans le cadre de la lutte contre la cybercriminalité, tel que le logiciel CETS (Child Exploitation Tracking System), développé par le Centre national de coordination contre l'exploitation des enfants (CNCEE) du Canada, utilisent des techniques particulières uniques (comme la reconnaissance de la « signature de la caméra numérique » ayant produit les photos) afin de détecter, bloquer/effacer le contenu de certains sites jugés illégaux.

6.3.4 Vérification de l'identité / âge

Les sites pour adultes (habituellement les sites de pornographie) comprennent souvent une procédure d'autorisation en demandant le code d'accès (tel que le NIP) fourni par le système de vérification d'âge (AVS).

6.3.5 Modération des forums / blogues / clavardage

Une autre façon d'effectuer le filtrage du contenu numérique pour les sites interactifs où les jeunes peuvent y déposer des documents, est d'établir une surveillance dynamique (modération) par l'intervention humaine ou logicielle ou les deux. Habituellement, le logiciel de modération utilise dynamiquement les règles de filtrage établies précédemment et une personne intervient uniquement lorsqu'il y a des incertitudes dans le filtrage ou qu'il y a un contenu détecté pouvant être problématique. Cette façon de fonctionner est relativement nouvelle et il sera intéressant de vérifier l'évolution de cette modération et de son efficacité ainsi que l'impact sur la fréquentation des jeunes de tels forums, blogues ou sites de clavardage.

6.3.6 Logiciels de filtrage des contenus créés

La possibilité, pour les jeunes, de créer du contenu audiovisuel est disponible depuis quelque temps déjà. Cependant, le filtrage de ce contenu dynamique est habituellement, du moins pour le moment, exclu de toute codification et donc de filtrage. Ainsi, dans le domaine des mobiles, toutes les règles de filtrage excluent les contenus créés par les utilisateurs eux-mêmes. Le problème qui peut se produire, c'est que les jeunes peuvent diffuser du contenu illégal et donc commettre un acte illégal sans nécessairement en être conscient mais tout en laissant des pistes menant à eux de façon très claire.

6.3.7 Logiciel de filtrage des pourriels

Les logiciels de filtrage spécialisés pour les pourriels comprennent des règles particulières pour reconnaître les pourriels. Souvent, ces logiciels sont installés sur le serveur d'une organisation, comme le FAI.

Ainsi, un des FAI importants au Québec, Videotron, fournit automatiquement à tous ses abonnés le service de filtrage des pourriels, qui peut cependant être désactivé par l'abonné. L'expérience démontre que ce service permet de bloquer la très grande majorité des pourriels pour ses clients. Cependant, très souvent, ces logiciels ne diffusent pas leurs règles de filtrage et le client ne peut choisir celles qui lui conviennent uniquement.

Cette fonctionnalité peut se retrouver dans les logiciels de filtrage de sites Web. Cependant, parmi les logiciels populaires, il s'avère que les meilleurs logiciels de filtrage de sites Web ne sont pas les meilleurs logiciels de filtrage des pourriels, et vice-versa.

Il est intéressant de noter l'étude réalisée aux États-Unis par la firme Ferris Research qui estime que le coût de bloquer des courriels qui sont de faux pourriels, s'élève à 3,5 milliards $ pour les entreprises, tout en estimant que le coût des pourriels s'élève à environ 10 milliards $[267].

6.3.8 Logiciel de contrôle parental

Les logiciels de contrôle parental, en plus de comprendre les fonctionnalités d'un logiciel de filtrage des sites Web, offre des fonctionnalités permettant aux parents, par exemple, d'appliquer les règles de temporalité établies à la section précédente et d'obtenir un rapportage des accès aux sites Web et des tentatives d'accès. Certains de ces logiciels vont même jusqu'à offrir la possibilité de transmettre un courriel au parent si le jeune vient de faire l'objet de cyberintimidation, par exemple.

Il faut cependant noter que plus l'enfant vieillit, plus il devient délicat pour les parents d'avoir recours aux outils de rapportage sans miner la confiance des jeunes ainsi que de porter atteinte, dans une certaine mesure, à la vie privée du jeune.

Encore dans ce cas, les meilleurs logiciels de contrôle parental[268] n'offrent pas nécessairement une meilleure capacité de filtrage des sites Web, et vice-versa.

6.3.9 Filtrage visuel

Le filtrage visuel demeure encore un moyen pour permettre de décider, ultimement, de poursuivre la visite ou non du site Web.

En effet, il restera toujours, malgré la sophistication des autres moyens de filtrage utilisés, une portion d'Internet qui échappera au filtrage. Le filtrage visuel servira de dernier recours dans ce cas, tout comme il peut être de premier recours si aucun autre moyen de filtrage n'est mis en place. De plus, les sceaux d'homologation n'étant pas codifiés dans les sites Web homologués, ne peuvent être détectés par des logiciels et seule une vérification visuelle permet à l'internaute de vérifier la présence du sceau d'homologation et de décider de poursuivre ou non la visite du site Web selon ses règles personnelles d'accès.

---

[267] Consulter la page Web du journal « E-Week » : www.eweek.com/article2/0,1759,1571177,00.asp ou celle de la firme « Silicon.com » : www.silicon.com/research/specialreports/thespamreport/0,39025001,10005575,00.htm

[268] Consulter le document n° 71.2 du Cahier 4 *Logiciel de surveillance - Comparaisons 2006* (www.monitoringsoftwarereviews.org/consumer_guide.html)

Les deux tableaux suivants résument les différences de caractéristiques entre les neuf modes de filtrage couverts.

Mode de filtrage	Segmentation des classes d'âge	Possibilité d'adaptation selon valeurs familiales / école	Protection des enfants	Facilité d'utilisation
6.3.1 Portail	Possible	Non	Élevée	Élevée
6.3.2 Moteur de recherche	Possible	Non	Élevée	Élevée
6.3.3 Log. de filtrage des sites Web	Non	Oui	Moyenne	Moyenne à Élevée
6.3.4 Vérification d'âge	n.a.	n.a.	Faible à Élevée	Élevée
6.3.5 Modération des sites interactifs	Possible	Oui	Élevée	Moyenne
6.3.6 Log. de filtrage des contenus créés [269]	?	?	?	?
6.3.7 Log. de filtrage des courriels	n.a.	Oui	Élevée	Moyenne à Élevée
6.3.8 Log. de contrôle parental	Oui	Oui	Élevée	Moyenne à Élevée
6.3.9 Filtrage virtuel	Oui	Oui	Faible	Élevée

Tableau 6.5.1 – Comparaison des modes de filtrage

[269] Le peu d'exemples documentés de filtrage des contenus créés par les jeunes rend impossible l'évaluation de ce mode de filtrage. À ce stade actuel, on pourrait tout aussi bien répondre « oui » ou « faible » que « non » ou « élevée ».

Mode de filtrage	Respect de la liberté d'expression	Protection de la vie privée des jeunes	Intervention possible d'adaptation du mode de filtrage	Localisation du filtrage
6.3.1 Portail	Faible à élevée	Élevée	non	Fournisseur du portail
6.3.2 Moteur de recherche	Faible à élevée	Élevée	non	Fournisseur du moteur
6.3.3 Log. de filtrage des sites Web	Faible à élevée	Moyenne à Élevée	Parent-Institution	• Poste individuel (maison) • Serveur (FAI, école, biblio) • Fournisseur de logiciel
6.3.4 Vérification d'âge	Élevée	Faible à élevée	Enfant-Parent-Institution	n.a.
6.3.5 Modération des sites interactifs	Faible à Moyenne	Moyenne	non	n.a.
6.3.6 Log. de filtrage des contenus créés [270]	?	?	?	?
6.3.7 Log. de filtrage des courriels	Moyenne à Élevée	Moyenne à Élevée	Parent-Institution	• Poste individuel • Serveur (FAI, école, biblio) • Fournisseur de logiciel
6.3.8 Log. de contrôle parental	Faible à Moyenne	Faible à Moyenne	Parent-Institution	• Poste individuel • Serveur (FAI, école, biblio) • Fournisseur de logiciel
6.3.9 Filtrage virtuel	Élevée	Élevée	Enfant	Poste individuel (maison, école, biblio)

Tableau 6.5.2 – Comparaison des modes de filtrage

[270] Le peu d'exemples documentés de filtrage des contenus créés par les jeunes rend impossible l'évaluation de ce mode de filtrage. À ce stade actuel, on pourrait tout aussi bien répondre « oui » ou « faible » que « non » ou « élevée ».

Conclusion et axes d'action

La gouvernance du contenu audiovisuel sur Internet destinée à protéger la jeunesse, comme toute gouvernance d'Internet, s'insère dans une « gouvernance multicouche » où les modes de régulation sont choisis selon la culture du pays, où toutes les parties prenantes (gouvernements, société civile et secteur privé) sont mises à contribution, où la transparence des choix et du fonctionnement est privilégiée et où tous les niveaux d'intervention local, national, régional et mondial sont déclenchés selon les besoins spécifiques, sachant la primauté des États en cette matière. Ce paramètre de base de la gouvernance étant posé, il est justifié de se demander comment cette gouvernance peut s'articuler au Québec afin de mieux protéger la jeunesse. Nous proposons des axes d'action à cette fin, sans préjuger des choix que la Régie du cinéma ou le gouvernement du Québec dans son ensemble pourra décider. Ces axes sont regroupés autour de thèmes suivants :

- type de régulation;
- adaptation du cadre législatif et réglementaire;
- nécessité et rôle d'une organisation gouvernementale centrale;
- taxonomie du contenu audiovisuel sur Internet;
- programme québécois de protection de la jeunesse;
- gestion du DNS;
- veille sur projets de recherche.

Type de régulation : migration vers plus de mixité

Actuellement, au Québec, la gouvernance du contenu sur Internet s'effectue principalement en mode d'autorégulation, le gouvernement fédéral canadien ayant eu recours à la régulation classique en légiférant sur la cyberbercriminalité et à la corégulation en finançant des organismes canadiens dédiés à l'alphanétisation. La gouvernance actuelle retenue au Canada et au Québec repose sur les trois principes fondamentaux suivants qu'il convient de rappeler qui sont à la base de la « Stratégie canadienne pour l'utilisation sécuritaire, prudente et responsable d'Internet » :

- principe de non-intervention de l'État privilégié dans la régulation d'Internet afin de permettre, notamment, à l'industrie d'Internet de croître;
- principe de primauté de la liberté d'expression;

- principe de non-tolérance de contenu illégal sur Internet et particulièrement concernant la pornographie infantile.

La gouvernance en mode d'autorégulation, et donc la non-intervention du gouvernement du Québec, se doit d'être questionnée concernant la protection de la jeunesse par rapport au contenu audiovisuel sur Internet. Voici deux statistiques obtenues de sondages/entrevues réalisées auprès des jeunes :

- 80 % des jeunes déclarent que le contenu d'Internet devrait être régulé, particulièrement le contenu des sites reconnus dangereux en termes de pornographie, de haine ou de racisme (étude 2006 de MediAppro);
- Près de 50 % des jeunes de 18-19 qui ont vu de la pornographie sont d'avis qu'ils étaient trop jeunes lorsqu'ils en ont vu pour la première fois (étude au Royaume-Uni).

Cette autorégulation actuelle va en quelque sorte à l'encontre des choix déjà retenus pour protéger la jeunesse par le biais de la Régie du cinéma. Les films sur médias traditionnels et classés par la Régie sont maintenant accessibles de plus en plus par Internet, lieu de prédilection de communication et d'information auprès des jeunes. Le maintien de l'autorégulation actuelle dans ce domaine signifie, pour le gouvernement du Québec, à plus ou moins long terme, la remise en question de la mission même de la protection de la jeunesse par la Régie car une partie de plus en plus grande du contenu audiovisuel sera numérique et accessible par Internet, par des technologies filaires ou non, qu'elle ne couvre pas actuellement.

Afin de permettre à la Régie du cinéma et au gouvernement du Québec de poursuivre leur mission de protéger la jeunesse par rapport au contenu audiovisuel, il est difficile d'entrevoir une autre avenue que de migrer de l'autorégulation vers un mode davantage mixte comprenant à la fois de la corégulation et de la régulation, tout en conservant le plus possible le mode d'autorégulation. Le temps de la prohibition est révolu depuis longtemps au Québec et il faut éviter de tomber à l'extrême en privilégiant un mode de gouvernance trop contrôlant. Les expériences des autres gouvernements comme le Danemark, ont démontré qu'une telle mixité des modes de gouvernance est salutaire pour ses citoyens et que le mode de régulation classique est à utiliser comme dernier recours, quand il faut vraiment forcer la main à l'industrie à se réguler. L'exemple de la protection des renseignements personnels au Québec illustre assez bien l'importance d'intervention gouvernementale : le gouvernement du Québec avait décidé, dans un premier temps, de ne légiférer que le secteur public en cette matière, préférant une autorégulation « naturelle » du secteur privé. Après quelques années d'observation, il a décidé d'inclure dans sa législation ce secteur qui n'avait pas suffisamment pris au sérieux cette protection. La Régie du cinéma et le gouvernement du Québec se doivent donc de décider si elle opte ou non pour le maintien du mode de gouvernance actuelle ou non.

ISOC Québec recommande d'insérer une mixité de modes de régulation et, au minimum, sans avoir à changer son corpus légal et réglementaire, d'y insérer le mode de corégulation où le gouvernement du Québec financerait un ensemble d'actions, basées sur le volontariat et la sensibilisation, visant à mieux protéger la jeunesse sur Internet.

De ce choix de mode de gouvernance découle toute la pertinence ou non des autres axes d'actions énoncées ci-après.

Adaptation du cadre législatif et réglementaire et rôle de la Régie du cinéma

Il s'agit de réviser les lois et réglementations québécoises ainsi que les politiques, orientations et recommandations en découlant afin de couvrir explicitement la protection de la jeunesse par rapport aux contenus audiovisuels sur Internet.

Au besoin, il y aurait lieu de les harmoniser avec celles du gouvernement fédéral car, pour ce qui a trait à Internet accessible sans fil, cela touche aux télécommunications dont la gouvernance relève du gouvernement du Canada. Cela peut signifier de proposer au gouvernement fédéral et à ceux des autres provinces et territoires, par le biais du Conseil de la fédération ou d'autres mécanismes de concertation canadienne, d'effectuer cette révision de façon cohérente au Canada, tout en conservant la souplesse concernant les aspects de compétence provinciale ou territoriale.

Ainsi, la protection de la jeunesse est une mission déjà couverte par la *Loi sur le cinéma* au Québec pour ce qui a trait aux films et aux vidéos. Il y aurait lieu de se questionner sur la portée de cette loi afin d'y inclure la couverture explicite du contenu audiovisuel sur Internet et peut-être aussi sur tout contenu véhiculé, quel que soit le média utilisé, un peu comme certains pays l'ont fait (littérature, vidéo, jeux, etc.). L'appellation de « Loi sur les médias » serait, par exemple, alors plus appropriée. De prime abord, cette extension justifierait encore que cette loi soit du ressort d'un ministère de la Culture.

Il faut aussi noter que la révision légale ne porterait pas nécessairement uniquement sur la *Loi sur le cinéma*. D'autres lois ou politiques pourraient éventuellement être touchées. Ainsi, on retrouve en Ontario, une organisation qui vient en aide aux victimes d'Internet, soit la *Cyber Law Enforcement Organization* (CLEO). On peut se poser la question sur la pertinence d'intégrer cette préoccupation explicitement dans le cadre légal ou réglementaire par le biais d'une loi (autre que celle sur les médias), d'un programme, une organisation gouvernementale ou une délégation (en mode corégulation) dans la société civile. La portée de cette étude ne couvrait pas explicitement le volet légal et il serait hasardeux de s'y aventurer davantage.

Afin de réaliser cette révision, il serait intéressant de mettre sur pied un groupe de travail dirigé par un organisme tel que la Régie du cinéma et intégrant les autres intervenants (particulièrement la société civile et les réseaux parapublics) ayant pour mission de compléter l'inventaire des éléments actuels de ce cadre sous l'optique d'intégrer explicitement la protection de la jeunesse sur Internet (ou pour tous médias) et à en réaliser une mise à jour en conséquence. Lors de cette étude, au moins deux des politiques ont été déterminées comme ayant un besoin d'intégration, soit :

- politique québécoise de l'autoroute de l'information[271];
- orientations gouvernementales en matière d'agression sexuelle[272].

À titre d'exemple, en Europe, une recommandation (régulation classique en mode recommandation) a été adoptée en 2005 relative à la protection des mineurs et de la dignité humaine dans le domaine de l'audiovisuel et de la société de l'information afin de s'adapter à l'évolution de l'univers médiatique concernant les contenus illicites et préjudiciables sur Internet. Cette recommandation soulignait trois niveaux de responsabilité en matière de protection de la jeunesse par rapport à Internet, soit :

---

[271] Consulter le document n° 46.1 du Cahier 4 *La politique québécoise de l'autoroute de l'information* (www.services.gouv.qc.ca/fr/publications/enligne/societe/politique_autoroute.pdf)
[272] Consulter le document n° 46.5 du Cahier 4 *Orientations gouv. en matière d'agression sexuelle* (www.mfacf.gouv.qc.ca/publications/pdf/CF_orientations_agression_sexuelle.pdf)

- responsabilité politique;
- responsabilité des industriels;
- responsabilité éducative et parentale.

Et cette recommandation a été par la suite suivie dans chacun des pays européens d'un cadre réglementaire, de politiques ou de programmes en conformité à leurs spécificités nationales.

Il apparaît important que le gouvernement du Québec dispose d'une organisation centrale ayant comme mission la coordination de la protection de la jeunesse par rapport aux médias. La Régie du cinéma nous apparaît tout indiquée. Elle possède déjà une expertise et une sensibilisation sur les médias, leur classement et la protection de la jeunesse qu'elle seule a autant développées parmi tous les organismes gouvernementaux existants et il serait intéressant de lui confier ce rôle de coordination avec les autres ministères et organismes relevant des gouvernements du Québec[273] et du Canada (dont Industrie Canada et le CRTC) ainsi que le rôle de coordination avec la société civile et l'industrie. Une collaboration serait ajoutée expressément pour maintenir des échanges avec les organismes semblables de par le monde et particulièrement ceux de la Francophonie.

---

[273] Ainsi, les autres ministères et organismes du gouvernement du Québec pouvant être interpellés par la protection de la jeunesse sur Internet comprennent, notamment :

- ministère du Développement économique, de l'Innovation et de l'Exportation;
- ministère de l'Éducation, du Loisir et des Sports;
- ministère de la Famille, des Aînés et de la Condition féminine;
- ministère de l'Immigration et des Communautés culturelles;
- ministère de la Justice;
- ministère de la Santé et des Services sociaux;
- ministère de la Sécurité publique;
- ministère des Services gouvernementaux;
- Centre d'aide aux victimes d'actes criminels;
- Commission d'accès à l'information;
- Commission des droits de la personne et des droits de la jeunesse;
- Conseil de la famille et de l'enfance.

Il serait important de réexaminer le partage des responsabilités entre le fédéral et le Québec (et les autres provinces) concernant la protection de la jeunesse par rapport au contenu audiovisuel accédé par Internet sans fil (mobile) et de convenir d'une régulation appropriée, notamment en matière de codification du contenu et de son accès.

Il y aurait donc lieu, en fonction des choix gouvernementaux, d'adapter la mission et les activités de la Régie du cinéma en conséquence. Par exemple : lui conserver le rôle de classement traditionnel des films, vidéos et DVD et lui ajouter le rôle de coordination de la protection de la jeunesse sur Internet et de codification des contenus audiovisuels sur Internet selon une taxonomie et une façon de faire à déterminer. La Régie du cinéma pourrait s'inspirer notamment des organisations semblables à travers le monde telles que :

- le **Conseil des médias pour les enfants et les jeunes gens** du Danemark (Medierådet for Børn og Unge) qui couvre à la fois les films, les jeux et Internet, en attribuant les classements aux films et en réalisant des activités de sensibilisation aux dangers d'Internet;
- la **Délégation aux usages de l'Internet** (DUI) de la France – noeud français sur le réseau européen d'alphanétisation INSAFE, qui sert de coordination de la politique de protection de la jeunesse en France et de lieu de cybersignalement;
- l'**Autorité australienne des communications et des média**s (Australian Communications and Media Authority – ACMA) qui est responsable de la régulation de la télévision, des radiocommunications, des télécommunications et du contenu sur Internet. C'est cette organisation qui utilise le même système de codification du contenu audiovisuel sur Internet que celui utilisé par l'Office de classification des films et de la littérature.

Établir la taxonomie à privilégier pour codifier le contenu audiovisuel sur Internet

Actuellement, au-delà du statu quo, les choix suivants s'offrent à la Régie du cinéma en matière de taxonomie :

- Celle de la Régie, utilisée pour le classement des films et basée à la fois selon l'âge et selon le type de contenu;
- Celles des deux organismes des jeux vidéos des États-Unis et de l'Europe basées à la fois selon l'âge et selon le type de contenu;
- Celle de l'ICRA, basée selon le type de contenu;
- Les multiples taxonomies « propriétaires »;

- Toute autre variante imaginable (exemple : adaptation de la taxonomie de l'ICRA pour la faire migrer vers une taxonomie compatible avec celle de la Régie et d'un des deux organismes des jeux).

Il s'agit donc de proposer une structure de codification (ou taxonomie) du contenu sur Internet qui serait appliquée par les producteurs de contenu québécois ou canadiens. Cette taxonomie aurait au minimum deux classes d'âge (moins de 18 ans et 18 ans et plus) particulièrement pour le contenu sur Internet accessible par les mobiles.

Idéalement, il serait souhaitable que la Régie du cinéma œuvre au niveau international afin d'établir un consensus sur la question de la taxonomie. C'est un type de projet qui mériterait le soutien d'un organisme de concertation internationale comme l'UNESCO. De prime abord, *ISOC Québec privilégierait le système de codification de l'ICRA* (quitte à l'adapter pour y ajouter une codification selon l'âge) à cause de son concept d'étiquetage, basé sur une norme d'Internet (soit RDF), de la transparence de son approche de codification et de son indépendance par rapport aux systèmes propriétaires de codification. Cette approche ne les exclurait pas pour autant car tout logiciel de filtrage peut réutiliser la taxonomie de l'ICRA.

Voici un scénario global de fonctionnement du système de codification, uniquement pour fixer les idées et sans préjuger de la faisabilité. Le producteur du contenu pourrait attribuer des étiquettes au contenu selon le type de contenu et même en proposer selon l'âge. Par la suite, chaque organisme de classement pourrait réviser ou attribuer le classement selon ses propres critères et attribuer les étiquettes correspondantes selon l'âge, tout en s'identifiant comme producteur de ces étiquettes de classement. Lorsqu'une personne du Québec voudrait visionner un document audiovisuel sur Internet, cela activerait les étiquettes qui s'appliquent au Québec et l'information de codification lui serait fournie avant son accès au document comme tel. Les logiciels de filtrage pourraient alors, selon les paramètres que l'utilisateur a choisis, permettre ou non le visionnement du contenu audiovisuel.

Établir des collaborations permanentes au niveau international

La codification des contenus audiovisuels sur Internet représente un exercice qui peut difficilement se passer d'une coopération internationale. Il serait intéressant *que la Régie du cinéma (ou Régie des médias) établisse un mode de collaboration continue avec les autres organismes qui partagent ce rôle à travers le monde*, particulièrement avec les organisations gouvernementales et de la société civile de l'Australie, de la Belgique, du Danemark, des États-Unis, de l'Europe et de la France.

À cette fin, la Régie pourrait participer à la création, si ce n'est déjà fait, d'une association internationale des organismes de classement des contenus audiovisuels numériques ou bien établir tout autre mécanisme permanent facilitant la concertation internationale sur le système de codification de ces contenus. Cela pourrait être le lieu pour établir par consensus un système commun de codification de tels contenus et éventuellement de partager la tâche de codification de ces contenus. *Pour ce qui est de la tâche elle-même de codification, il y aurait lieu de s'interroger, dans le contexte d'Internet participatif, sur l'opportunité de déléguer cette codification au producteur du contenu.* Dans ce contexte, les organismes de classement n'auraient qu'à s'assurer de la qualité du processus de codification en, par exemple, élaborant un sceau de confiance émis à la suite d'une homologation à ces producteurs ou en réalisant des vérifications périodiques de la codification réalisée.

Établir un programme québécois de protection de la jeunesse sur Internet

Un peu comme l'Europe et certains autres pays l'ont réalisé ou sont en train de le faire, ISOC Québec propose à la Régie d'*établir un programme québécois de protection de la jeunesse sur Internet*, complémentaire à celui du gouvernement fédéral.

À cette fin, les actions suivantes sont proposées :

a. Élaborer un modèle de gestion des risques relatif à la protection de la jeunesse sur Internet

b. Mettre en oeuvre un programme massif d'alphanétisation

   b.1 Prévoir des sites Web pour l'éducation des jeunes aux périls sur Internet

   b.2. Réviser l'utilisation et l'enseignement d'Internet dans les institutions d'enseignement du primaire et du secondaire

   b.3 Conception ou recensement d'interface utilisateur Web pour les jeunes

   b.4 Portail pour jeunes de meilleure qualité et au contenu enrichi

   b.5 Mettre en place une CyberMaison des jeunes

   b.6 Mettre en place une CyberMaison des parents

   b.7 Mettre en place une CyberMaison des éducateurs

   b.8 Élaborer un Guide ou Code de pratiques parent-enfant

   b.9 Renforcer le maillage avec les organismes chargés de la lutte à la cybercriminalité

c. Codes de pratiques

d. Internet par mobiles

e. Observatoire permanent sur la protection de la jeunesse sur Internet

f. Filtrage : faciliter l'accès et l'utilisabilité

   f.1 Rendre disponible des outils de filtrage et de contrôle parental d'Internet

   f.2 Filtrage – évaluation des logiciels

   f.3 Vérifier la possibilité de réutiliser les outils de cybersurveillance policière

   f.4. Liste verte et liste rouge

g. Homologation

h. Authentification

i. Cybercriminalité

   i.1 Cybercriminalité et cybersignalement : augmenter leur visibilité

   i.2 Cybercriminalité : s'assurer de la couverture complète des crimes

   i.3 Cybercriminalité : réseau de cybersignalement

   i.4 Cybercriminalité : évolution de la cybercriminalité

j. Pollupostage

   j.1 Augmenter la lutte au pollupostage au Québec et au Canada

   j.2 Augmenter la lutte au pollupostage : WhoIs

   j.3 Augmenter la lutte au pollupostage : accords internationaux

   j.4 Augmenter la lutte au pollupostage : utilisation des serveurs racine ou autres éléments du DNS

Voici une brève explication de chacune de ces actions.

a. Élaborer un modèle de gestion des risques relatif à la protection de la jeunesse sur Internet

Plusieurs organisations nationales et internationales, tant du secteur gouvernemental que de la société civile, ont constitué une liste des dangers ou périls que les jeunes courent avec Internet. Souvent, cette liste est appuyée a posteriori d'une étude ou d'un sondage pour vérifier certaines hypothèses sur les dangers. Cette liste, ainsi confirmée, sert par la suite à établir les actions nécessaires pour réaliser la protection de la jeunesse sur Internet. C'est la façon de fonctionner de la plupart des pays étudiés et qui disposent d'un programme d'intervention. Ces listes nationales, bien que répondant à des besoins nationaux, ne sont pas nécessairement exhaustives et structurées adéquatement. On y retrouve des disparités d'un pays à un autre et après un examen attentif, on remarque que les dangers identifiés sont tantôt des risques, tantôt des conséquences possibles de ces risques. Ainsi, le risque de dépendance d'un jeune à Internet peut présenter des conséquences (ou impacts) sur le temps passé sur Internet et sur la diminution du temps passé à d'autres activités telles que le sport ou les activités sociales. Souvent, on va considérer sans distinction comme dangers : la dépendance, le grand nombre d'heures passées sur Internet et le retrait du jeune de certaines activités. Étant donné que la taxonomie des risques sert de base pour élaborer un programme d'intervention, il serait important d'établir une taxonomie des risques où les différents risques seraient définis et structurés en catégories cohérentes et non redondantes.

Une fois la taxonomie des risques établie, il s'agirait par la suite d'élaborer le modèle de gestion des risques où, notamment, les scénarios types de traitement des risques seraient définis. Il est possible de s'inspirer des modèles de traitement types des risques dans d'autres domaines de l'activité humaine tels que la gestion de la sécurité et la gestion des technologies de l'information (TI) afin d'élaborer les scénarios types de traitement. Il existe des normes en gestion des risques (dont celle de l'Australie) qui détaillent ces phases et étapes qui pourraient être réutilisées. Ce modèle de gestion des risques servira à choisir les actions à entreprendre en fonction de critères tels que le degré de gravité ou de fréquence des conséquences des risques.

La taxonomie des risques aurait avantage à être élaborée par consensus international. Cela permettrait de partager par la suite un vocabulaire international commun et éventuellement, de partager les efforts de définition d'actions visant à traiter certains des risques jugés les plus importants au niveau international.

Normalement, la taxonomie des risques et le modèle de gestion des risques devrait être identique à travers le monde. C'est ce qui se produit, actuellement, dans d'autres domaines d'activités humaines telles que le développement de logiciels. Les variations nationales qui reflètent la culture d'un pays/province/État sont prises en compte lors de l'évaluation des risques dans le contexte de cette culture. En fonction de cette évaluation, les actions choisies seront différentes d'un pays à l'autre. Si le modèle de gestion des risques est bien étoffé, un pays donné n'aurait qu'à activer les actions choisies à partir de l'ensemble d'actions (visant à traiter le risque) définies dans le modèle. Ce modèle se retrouverait à comprendre un compendium des actions possibles pour un risque spécifique. Déjà, en se basant sur les actions déjà entreprises dans certains pays, il serait possible d'élaborer un tel modèle en réutilisant et adaptant les connaissances et objets de gestion des risques déjà disponibles dans les différents pays.

b. Mettre en oeuvre un programme massif d'alphanétisation

Il a été observé qu'un programme massif d'alphanétisation porte ses fruits auprès des jeunes. Ainsi, lors d'une enquête (MediAppro), on a pu observer :

> « Autorégulation des enfants par rapport à la sécurité sur Internet, particulièrement en France, principalement grâce au programme massif de sensibilisation et d'éducation sur les périls et les moyens d'y faire face : les jeunes rapportent se retrouver dans des situations dangereuses ou même inconfortables extrêmement rarement. »

De même, une étude au Danemark concluait :

> « Plutôt que d'empêcher l'accès à Internet, il recommande que les parents permettent à leurs enfants d'acquérir les compétences nécessaires pour distinguer entre la fiction et la réalité (en matière de pornographie par exemple) »

Lorsque les jeunes sont bien formés à Internet, à ses risques et aux façons d'y faire face, ils adoptent une approche d'autorégulation qui fait montre de leur maturité et de leur autonomie devant des situations qui auraient pu être embarrassantes. Ils ont acquis un modèle de lecture d'Internet qui permet de faire la part des choses.

Au Québec, malgré les efforts du fédéral concernant ce sujet, il n'est pas assuré que les jeunes maîtrisent suffisamment Internet, ses risques et les stratégies de traitement de ces risques. C'est pourquoi ISOC Québec propose de *mettre sur pied un programme massif d'alphanétisation*, pouvant s'inspirer, notamment, du programme européen *Safer Internet* et du programme *i-SAFE* des États-Unis, tout en misant à réutiliser les ressources disponibles au Québec ou au Canada (comme celles de Réseau Média et CyberAverti). Certains éléments dignes de mention pour orienter ce programme comprennent :

- Former les jeunes sur l'utilisation d'Internet et des différentes commodités de **communication** (privilégiées par les jeunes);
- Former les jeunes sur la façon de gérer les relations électroniques; notamment en matière de risque, sûreté et de respect des droits des autres jeunes;
- Adopter des stratégies différentes selon le groupe d'âge;
- Faire participer toutes les parties prenantes de la gouvernance.

Voici quelques éléments de détails de ce programme :

b.1 Prévoir des sites Web pour l'éducation des jeunes aux périls sur Internet

Offrir de l'information aux jeunes sous une interface utilisateur qui correspond à la clientèle des jeunes (exemple : site de l'Australie www.cybersmartkids.com.au), idéalement, par classes d'âge et avec une préoccupation pour attirer autant les garçons que les filles, sachant que la forme ludique est plus appréciée chez les garçons.

b.2. Réviser l'utilisation et l'enseignement d'Internet dans les institutions d'enseignement du primaire et du secondaire

Actuellement, l'école est loin d'être le lieu de prédilection d'apprentissage et d'utilisation d'Internet. Elle semble même être le dernier lieu : les jeunes rapportent que l'école représente le lieu d'utilisation d'Internet que pour 26 % d'entre eux alors que la maison représente 67 % :

> « L'enseignement explicite d'Internet dans les écoles apparaît être sérieusement sous-développé : 82 % en Europe et 90 % au Québec : « Schools fail to teach the skills of information retrieval, search, site evaluation and creative production » (étude MediAppro)

De plus, il apparaît une disparité de plus en plus grande entre la réalité des jeunes (communication par Internet et très grande interactivité et très grande consommation audiovisuelle) et celle de l'environnement d'enseignement (interactivité nettement moindre avec des contenus éloignés de l'audiovisuel). Les nouveaux médias comme Internet exigent une révision de l'enseignement traditionnel.

ISOC Québec propose de *réviser l'utilisation et l'enseignement d'Internet dans les institutions d'enseignement du primaire et du secondaire*, et ce, sous la responsabilité du ministère de l'Éducation. Voici quelques éléments de réflexion ou d'orientation pour aiguiller cette révision :

- Former les formateurs (sur les nouvelles technologies elles-mêmes, sur les risques inhérents et les façons d'y faire face);
- Évaluer l'ensemble des outils et services (matériel, logiciel et liens de télécommunication) disponibles dans les institutions d'enseignement par rapport à ce qui est disponible sur le marché et réviser cet ensemble, le cas échéant, afin de doter adéquatement les écoles d'outils et de services Internet;
- Former les jeunes à utiliser Internet, y incluant la production de contenu : références de « sites de confiance », recherche d'information, évaluation de l'information recueillie, modes de communication et création de contenus afin d'augmenter la capacité des jeunes à profiter d'Internet et l'intégrer dans leur processus d'apprentissage qui leur servira par la suite toute leur vie durant;
- Former les jeunes en matière de gestion des risques : dangers potentiels (risques), et mode de traitement des risques afin d'augmenter la sûreté des jeunes sur Internet;
- Revoir les politiques d'accès à Internet par les jeunes à l'école : privilégier l'acquisition de compétences critiques par rapport au contenu audiovisuel par des activités pédagogiques appropriées plutôt que la prohibition pure et simple généralement observée (blocage d'accès aux logiciels ou sites que les jeunes fréquentent à la maison) (basé sur l'étude MediAppro au Royaume-Uni);
- S'assurer d'intégrer autant l'aspect éducationnel que l'aspect éthique d'Internet dans les programmes de formation visant à l'alphanétisation;
- Insérer, dans le curriculum des écoles, un guide permettant d'augmenter la sensibilisation des jeunes concernant les défis sociaux, culturels et économiques des nouveaux médias;
- Revoir comment intégrer le concept de jeux, dont les jeunes (garçons surtout) sont si friands dans les approches pédagogiques;

- Revoir comment intégrer les autres outils de communication ou d'interaction des jeunes (MP3, mobiles, etc.) dans le programme d'apprentissage scolaire;
- Réutiliser le matériel existant au Québec (notamment de Réseau Éducation Média) et ailleurs dans le monde.

b.3 Conception ou recensement d'interface utilisateur Web pour les jeunes

Actuellement, plusieurs des sites Web destinés à l'alphanétisation des jeunes affichent une interface utilisateur peu attirante pour les jeunes. ISOC Québec propose qu'*un guide de conception d'interface utilisateur orientée vers la clientèle de jeunes et un répertoire de bons exemples* soient réalisés.

À cette fin, il serait intéressant qu'un organisme de normalisation orienté contenu tel que le W3C Québec, appuyé de centres de recherche sur la psychologie du jeune selon ses différents âges et sur l'utilisabilité, se penche sur la définition de normes ou de lignes directrices facilement utilisables (il serait même intéressant de s'adjoindre des firmes de logiciels ou des représentants de logiciels libres) pour la conception de sites Web adaptés à un public jeune. Une première étape serait sûrement de recenser les sites Web pour jeunes et tenter de dégager des modèles, selon les âges.

b.4 Portail pour jeunes de meilleure qualité et au contenu enrichi

Les portails actuels pour jeunes, sauf quelques exceptions, ne présentent pas une interface utilisateur ou un contenu à la hauteur des attentes de ceux-ci. À la suite d'une enquête auprès d'enfants au Royaume-Uni, leurs recommandations étaient claires :

> « Meilleur contenu conçu pour eux;
>
> Sites interactifs qui interagissent à leurs contributions. »

ISOC Québec recommande que *des portails soient constitués qui tiennent compte des normes ou lignes directrices élaborées au point précédent et dont le contenu et l'interactivité soient à la hauteur des attentes des jeunes*. Leur participation à la conception même de ce ou ces portails apparaît essentielle.

b.5 Mettre en place une CyberMaison des jeunes

ISOC Québec propose de *développer et maintenir une CyberMaison des jeunes* par et pour les jeunes afin de doter les jeunes du Québec d'un lieu d'apprentissage et de création un peu comme le projet danois **Cyberhus** où sont disponibles, à la demande, des éducateurs, conseillers experts, mentors pour soutenir les jeunes et répondre à leurs questions. D'autres jeunes plus expérimentés peuvent servir de mentors.

Un autre exemple, canadien cette fois, est l'organisation torontoise **TakingITGlobal**[274] qui est dirigée par les jeunes et soutenue par la technologie et son site Web multilingue. Cette organisation permet d'interconnecter les jeunes à travers le monde et vise à développer la capacité des jeunes dans l'expression artistique et des médias, à rendre l'apprentissage plus engageant et à impliquer les jeunes dans certaines prises de décision globales. Elle est soutenue par l'ONU, des compagnies et des organisations de jeunes.

Il est important de développer des outils pour permettre aux jeunes de créer facilement du contenu selon son âge et ainsi commencer à apprendre l'exercice de ses droits et devoirs de citoyen par l'expression de ses opinions, tout en le faisant dans un contexte sûr. Il y serait intéressant de s'associer à des organisations comme Apple pour permettre de créer de la musique, du vidéo, du texte, des dessins, etc.

b.6 Mettre en place une CyberMaison des parents

Actuellement, la très grande majorité des jeunes au Québec indiquent que leurs parents s'impliquent très peu dans leur éducation relative à Internet :

> « 90 % des jeunes au Québec indiquent que leurs parents ne leur imposent aucune règle d'utilisation d'Internet. » (étude MediAppro)
>
> Très peu de parents discutent avec leur jeune sur leur utilisation d'Internet.

ISOC Québec propose de *développer et soutenir une CyberMaison des parents* par et pour les parents pour les aider à maîtriser Internet et leur rôle parental de conseils et de surveillance auprès des jeunes.

On pourrait y retrouver des formulations ou guides de stratégies d'intervention parentale pour la protection de la jeunesse qui pourraient comprendre, par exemple :

- Sensibilisation et formation des parents sur Internet et la façon de conseiller leurs jeunes en matière de protection;

[274] Pour plus de détails, consulter le document n° 47.1 du Cahier 4 *TakingIGGlobal* (www.takingitglobal.org)

- Établissement des façons d'intervention parentale (conseils, discussions, filtrage, contrôle, surveillance) en fonction de tranches d'âge et par sexe.

Un exemple de CyberMaison des parents est le programme i-PARENT de l'organisation i-SAFE aux États-Unis.

Cette CyberMaison des parents vise à réduire la fracture numérique entre les parents et leurs enfants.

b.7 Mettre en place une CyberMaison des éducateurs

ISOC Québec propose de *développer et soutenir une CyberMaison des éducateurs* par et pour les éducateurs pour les aider à maîtriser Internet et assumer leur rôle auprès des jeunes et de leurs parents. Un exemple de CyberMaison des jeunes est le programme de formation de l'organisation i-SAFE aux États-Unis.

b.8 Élaborer un Guide ou Code de pratiques parent-enfant

Le contrôle et la surveillance des jeunes peuvent sécuriser les parents mais les jeunes peuvent les considérer comme menaçants :

> « 63 % des enfants (12-19 ans) ont pris des actions pour cacher à leurs parents leurs activités en ligne. » (Étude auprès des jeunes au Royaume-Uni)

C'est pourquoi les jeunes demandent une meilleure considération de leurs besoins de protéger leur vie privée, incluant de la part de leurs parents.

ISOC Québec propose d'*élaborer un guide afin d'aider les parents et les enfants à établir les frontières entre le devoir de contrôle parental et le droit à la protection de la vie privée des jeunes*, et ce, selon les tranches d'âge. Ce guide pourrait même prendre la forme d'un code de pratiques à respecter, un peu comme le code de la route. Au fur et à mesure que l'enfant vieillit et est plus habile sur Internet, il pourrait aller explorer d'autres routes et son code de pratiques s'élargirait.

Il est important que ce Guide ou Code de pratiques véhicule le principe de transparence parent-enfant pour établir le contrôle parental (filtre, contrôle, surveillance).

b.9 Renforcer le maillage avec les organismes chargés de la lutte à la cybercriminalité

ISOC Québec *propose d'augmenter la concertation entre les organismes d'alphanétisation et ceux de la cybersurveillance* pour assurer une cohérence des pratiques de sensibilisation par rapport à l'évolution de la cybercriminalité et ainsi s'assurer que la sûreté des jeunes sur Internet est maintenue.

c. Codes de pratiques

ISOC Québec propose, dans un contexte de corégulation, d'examiner la possibilité de faire développer et respecter des codes de pratiques par l'industrie. Le meilleur exemple de codes de pratiques se retrouve en Australie.

Ces codes de pratiques peuvent porter, entre autres, sur l'accès à Internet par mobile, sur les hébergeurs, les fournisseurs d'accès à du contenu au Québec ou au Canada, les fournisseurs d'accès à du contenu extérieur au Québec ou Canada.

d. Internet par mobiles

Internet par mobiles exige une attention spéciale car le parent ou l'éducateur n'est plus à proximité pour exercer une surveillance ou fournir de l'aide au jeune aux prises avec des situations embarrassantes. Cependant, toute intervention dans ce domaine exige de remettre en question le principe d'autorégulation pour migrer, au moins, vers une corégulation de la gouvernance. Ainsi, on remarque que beaucoup de pays exigent une obligation d'abonnement (opt-in) pour accéder tout contenu destiné aux 18 ans et plus et la preuve d'âge y est contrôlée. Aux États-Unis, l'industrie prévoit une autorégulation très bientôt, à la suite de l'insistance du gouvernement des États-Unis. L'industrie prévoit mettre en place davantage de mesures pour décourager les enfants d'accéder au contenu pour adulte par le biais de leurs appareils mobiles. Il est intéressant de citer globalement le plan de la France en matière de gouvernance d'Internet par mobile, défini par une charte. Cette charte définit les cinq engagements suivants :

- renforcer et harmoniser la démarche déontologique encadrant le développement des contenus multimédias mobiles dans les kiosques et portails;
- informer et proposer de manière systématique aux parents un système gratuit de contrôle parental;

- renforcer la lutte contre les contenus illicites;
- informer le grand public sur les actions menées et participer à l'éducation pour tous aux bons usages de la téléphonie mobile;
- évaluer, informer et consulter régulièrement l'ensemble des parties concernées par cette démarche déontologique.

Cette charte s'appuie sur plusieurs dispositifs :

- l'outil de contrôle parental qui bloque l'accès à certains sites et est activable dès l'ouverture de la ligne;
- l'absence de contenus réservés aux adultes sur le portail des opérateurs;
- la modération des parties publiques des sites de clavardage et de blogues;
- un outil de cybersignalement des contenus susceptibles de porter atteinte à la dignité humaine.

e. Observatoire permanent sur la protection de la jeunesse sur Internet

Dans le cadre de tout programme, il est important de prendre périodiquement des mesures de la réalité concernée par le programme afin d'évaluer son évolution et les progrès accomplis grâce au programme mis en place. Cela permet, notamment, d'évaluer la pertinence d'un programme et de l'ajuster, le cas échéant.

ISOC Québec propose d'*élaborer et maintenir une enquête périodique sur les divers aspects de la protection de la jeunesse* en ayant recours aux organisations québécoises les plus susceptibles de réaliser une telle étude (telles que CEFRIO, Réseau Éducation Média, Université de Sherbrooke, etc.).

f. Filtrage : faciliter l'accès et l'utilisabilité

f.1 Rendre disponible des outils de filtrage et de contrôle parental d'Internet

Malgré les limites de tout filtrage et sachant que les filtres ne constituent qu'un complément à la sûreté sur Internet et ne remplacent en aucun cas la supervision parentale, il peut être utile d'y avoir recours. Voici quelques éléments militant en sa faveur :

- 90 % des jeunes au Québec indiquent que leurs parents ne leur imposent aucune règle d'utilisation d'Internet; (MediAppro);

- 2 % des parents installent des mesures prohibitives de contrôle de l'utilisation d'Internet; (MediAppro);
- Seulement 11 % des parents ont installé un logiciel de filtrage; (étude au Danemark);
- La principale préoccupation des parents est la somme de temps que le jeune passe sur Internet (pour 23 % des parents) et la seconde (pour 15 % des parents) concerne la pornographie; (étude au Danemark);
- 80 % des jeunes déclarent que le contenu d'Internet devrait être régulé, particulièrement le contenu des sites reconnus dangereux en termes de pornographie, de haine ou de racisme.

ISOC Québec propose *que soit rendu disponible gratuitement des commodités de filtrage et de contrôle parental d'Internet*, tant à la maison que dans les écoles et les bibliothèques, quel que soit le mode d'accès à Internet. À titre d'exemple, c'est une initiative en cours en Australie (au coût de 116 M $ AU).

Si la gratuité ne peut être offerte, ISOC Québec propose qu'il soit rendu obligatoire la disponibilité d'outils de filtrage et de contrôle parental auprès des FAI/FSI.

Dans tous les cas, ce logiciel doit pouvoir être activé ou désactivé par le parent.

f.2 Filtrage – évaluation des logiciels

ISOC Québec recommande d'évaluer les logiciels de filtrage (filtrage de sites Web, filtrage de pourriels, contrôle parental, etc.) selon les spécificités du Québec et de maintenir cette évaluation à jour. Les critères spécifiques pourraient être :

- soutien du français, de l'anglais au minimum, plus certaines autres langues;
- capacité d'adaptation de la taxonomie et des règles de filtrage selon les besoins québécois/canadiens.

f.3 Vérifier la possibilité de réutiliser les outils de cybersurveillance policière

Étant donné l'actuelle limitation de tout logiciel de filtrage, ISOC Québec recommande de *vérifier la possibilité de réutiliser en tout ou en partie les outils spécialisés de cybersurveillance policière* afin d'améliorer les logiciels de filtrage en matière de blocage des contenus illicites (pornographie infantile, apologie et incitation à la haine, racisme, discrimination, etc.).

f.4. Liste verte et liste rouge

ISOC Québec propose d'examiner la possibilité d'entreprendre les trois actions suivantes :

- Établir une liste verte et une liste rouge des sites, par classe d'âge (et peut-être par sexe), pouvant servir aux services de filtrage divers. Ces listes doivent majoritairement être en français, car il en existe déjà en anglais;
- Établir des collaborations avec les pays francophones dont la France (qui élabore une liste rouge sur la pornographie et une autre sur la haine et le racisme) et la Belgique afin d'échanger ces listes. S'il y a une taxonomie commune de type de contenu, cet échange pourrait se faire au niveau plus détaillé par type de contenu;
- Profiter de la cybersurveillance des équipes spécialisées afin de leur permettre de codifier du contenu examiné, qui, tout en étant légal, peut constituer un danger pour les jeunes (liste rouge).

g. Homologation

ISOC Québec propose d'*examiner la possibilité de mettre en œuvre certaines des homologations types possibles* de façon à augmenter la protection de la jeunesse.

À titre d'information, les principales étapes d'une homologation sont :

- Établir un code de pratiques à respecter;
- Déterminer le processus d'homologation;
- Déterminer l'organisme responsable de l'homologation : ouvert ou par appel d'offres;
- Déploiement de l'homologation.

Si des homologations sont retenues, il s'agira de décider à quel niveau ou selon quel modèle de partenariat devrait se faire l'homologation : Québec, Canada, Amérique du Nord, Francophonie, Europe, France, etc.

Les homologation types comprennent, de façon non exhaustive :

- homologation de sites Web par rapport à la protection des renseignements personnels (un peu selon le modèle du gouvernement des États-Unis – Safe Harbor);
- homologation de sites Web par rapport aux sites Web interactifs (blogue et clavardage, selon le modèle « SmartSmiley » du Danemark) ou indiquant la présence de modérateurs;
- homologation de sites Web de fournisseurs fiables (du genre « marque de confiance » en France ou IQUA en Espagne);

- homologation de fournisseurs (FAI/FSI) qui respecte les codes de pratiques (du genre « Ladybird Seal », mis en place en Australie);
- homologation de sites Web sûr pour les jeunes (du genre « label citoyen » en France) et idéalement par classe d'âge et par sexe;
- homologation de la codification du contenu selon, notamment la taxonomie de l'ICRA (certification décernée par l'ICRA ou ChildSafe International - ICCS™ Certification).

h. Authentification

ISOC Québec propose les actions suivantes en matière d'authentification :

- Examiner l'opportunité sociétale, technique et financière de déployer une authentification applicable aux jeunes un peu comme le fait la Colombie britannique et, surtout, la Belgique;
- Examiner la possibilité d'établir une authentification compatible avec d'autres provinces ou d'autres pays et s'inspirer de l'étude en cours en Europe sur cette question;
- Examiner la possibilité de favoriser d'autres authentifications existantes ou nouvelles, par exemple Sender ID permettant de lutter contre le pollupostage, ou pour les sites interactifs (clavardage, blogue, etc.) ou celle privée pour la clavardage (Net ID);
- Exercer une veille sur l'approche d'authentification Open ID pour les blogues dans le monde du logiciel libre.

Il est important de prendre note que l'authentification, malgré son attrait de protection des jeunes, peut enlever la possibilité des jeunes d'interagir de façon anonyme sur des sites de clavardage par exemple. Derrière l'anonymat, le jeune peut jouer des rôles, s'attribuer une personnalité différente et tester certains comportements. Le jeu de rôle est une activité importante d'apprentissage rendue possible grâce à l'anonymat. Il est crucial de ne pas noyer cette possibilité avec l'authentification. Il faut laisser de la place à ce jeu de rôle et peut-être même le favoriser en prévoyant des places, sites, forums dédiés à ça, tout en s'assurant que ce sont effectivement des jeunes qui sont en ligne et non pas des prédateurs.

i. Cybercriminalité

i.1 Cybercriminalité et cybersignalement : augmenter leur visibilité

Il existe actuellement un réseau canadien de cybersignalement. Cependant, ce réseau n'apparaît pas disposer d'une visibilité suffisante pour qu'il puisse être mis à contribution adéquate et il n'est pas sûr qu'il couvre bien tous les aspects de la cybercriminalité, au-delà de la pornographie infantile. Se référer à l'approche de la FTC qui possède une adresse de courriel qui peut être utilisée en tout temps et qui fournit une liste de tous les organismes où l'on peut porter une plainte ainsi que des organismes où l'on peut obtenir de l'aide si on a été victime de cybercriminalité[275].

ISOC Québec propose d'*examiner la possibilité de donner davantage de visibilité à la possibilité de cybersignalement et d'ajouter des points de cybersignalement* – par exemple auprès de chacun des FAI/FSI et des hébergeurs.

i.2 Cybercriminalité : s'assurer de la couverture complète des crimes

Actuellement, beaucoup d'emphase est mise sur la pornographie infantile, et cela est tout à fait compréhensible. Cependant, il existe d'autres crimes/comportements douteux pouvant se produire sur Internet qu'il est important de couvrir tels que l'intimidation (bullying), les menaces, la séduction (grooming), le leurre (luring), le racisme, la haine, le sexisme, l'apologie de l'anorexie et de la boulimie, les crimes contre l'humanité, etc. ISOC Québec recommande d'*étendre la couverture de la cybersurveillance à tous les types de crimes pouvant affecter la jeunesse*.

i.3 Cybercriminalité : réseau de cybersignalement

ISOC Québec propose d'*examiner la possibilité pour le Québec de faire partie du réseau européen de cybersignalement INHOPE ou de mettre en oeuvre un nouveau réseau à travers les pays de la francophonie*, un peu comme le réseau anglophone Virtual Task Force

[275] Consulter le site Web OnGuard Online - http://onguardonline.gov

i.4 Cybercriminalité : évolution de la cybercriminalité

ISOC Québec propose d'*examiner la possibilité pour le Québec d'établir des liens avec l'unité de recherche sur l'Internet de l'université Lancashire* (**Cyberspace Research Unit** du Department of Forensic and Investigative Science à University of Central Lancashire **UCLAN/CRU**) dont sa mission est d'explorer la façon dont les criminels utilisent Internet et l'impact sur les stratégies d'enquête.

ISOC Québec propose d'*exercer une vigie sur le projet de loi aux États-Unis, soit le Internet Safety and Child Protection Act,* qui vise à, notamment, exiger la vérification adéquate de l'âge et à percevoir une taxe de 25 % sur tout produit pornographique vendu par Internet. Cette taxe servira, si le projet de loi est adopté, à financer la protection des enfants contre les contenus pour adultes.

j. Pollupostage

j.1 Augmenter la lutte au pollupostage au Québec et au Canada

ISOC Québec propose les actions suivantes afin d'augmenter la lutte au pollupostage :

- *Prévoir une loi canadienne* permettant l'approche de désabonnement (opt-out) au minimum ou d'abonnement (opt-in) pour tout courriel non sollicité, y incluant les messages sur mobiles et le bannissement du « farming » (collecte de courriels). À cette fin, il serait intéressant d'établir une collaboration avec l'organisation CAUSE Canada - Coalition Against Unsolicited Commercial Email, association qui milite en faveur d'une réglementation antipourriel;
- *Offrir et publiciser une adresse électronique pour signaler tout pourriel.* Exemple du FTC des États-Unis : (spam@uce.gov) ou « abuse@nom_du_fournisseur_d'accès_Internet »
- *Rendre obligatoire la disponibilité gratuite d'un logiciel de filtrage des pourriels* offerts par les FAI/FSI, avec la possibilité pour l'abonné de le désactiver ou le paramétrer selon son choix. Rendre transparents et compréhensibles auprès des abonnés les critères de filtrage utilisés et en expliquer son fonctionnement. Déjà, le logiciel antipourriel de la firme québécoise RadialPoint est disponible auprès des clients des grands FAI au Québec (Bell, Telus et Videotron) inclus dans le prix d'abonnement. L'obligation ne serait donc qu'auprès des petits fournisseurs d'accès à Internet.

- *Étudier la possibilité d'établir un Code de pratiques contre les pourriels* – un peu comme au Danemark. Depuis janvier 2006, les FSI y ont mis en œuvre un code de conduite relatif au pollupostage qui les oblige à utiliser un filtre central contre les pourriels ou offrir une solution qui leur est propre. Les FSI doivent aussi indiquer à leurs clients le potentiel de filtrage et ses limites. Ce code de conduite inclut des dispositifs lorsque des pourriels sont effectivement envoyés.
- *Inciter les FAI/FSI à fournir une page Web informationnelle sur les pourriels* où on y retrouverait :
    - Informations permettant de se prémunir du pollupostage;
    - Lieu de signalement de pollupostage;
    - Lieu pour se désabonner (opt-out) des listes de diffusion connues ou s'abonner (opt-in) selon les choix légaux retenus.
- *Identifier et favoriser un organisme québécois de lutte au pourriel* et qui agirait comme coordonnateur québécois et liens avec les autres provinces et l'international, particulièrement dans le monde de la francophonie.

j.2 Augmenter la lutte au pollupostage : WhoIs

ISOC Québec recommande d'exercer une vigie et une influence auprès d'ICANN sur l'utilisation des informations personnelles du WhoIs, source de collecte de courriels (« farming ») par les polluposteurs.

j.3 Augmenter la lutte au pollupostage : accords internationaux

ISOC Québec propose d'*établir des accords* internationaux (ou interprovinciaux) bilatéraux ou multilatéraux avec d'autres pays (comme l'Europe, les États-Unis et l'Australie) pour coordonner la lutte au pollupostage et permettre le maintient de l'illégalité de pourriels venant d'autres pays signataires des accords à convenir.

j.4 Augmenter la lutte au pollupostage : utilisation des serveurs racine ou autres éléments du DNS

ISOC Québec propose d'*entreprendre une réflexion sur la non-utilisation des serveurs racine* pour réduire l'utilisation indue ou illicite des ressources critiques d'Internet (comme pollupostage ou pornographie infantile ou toute autre activité illicite au niveau national ou international). Au delà des serveurs racine, il pourrait y avoir une intervention au niveau des cinq registres régionaux d'Internet (RIR - Regional Internet Registry) ou bien

auprès de l'autorité nationale qui gère le code de pays (ACEI au Canada par exemple).

Suivi du DNS

a. Favoriser le déploiement de l'IDN au Québec

Actuellement, l'ACEI est à étudier la question du déploiement au Canada. ISOC Québec recommande de :

- Surveiller et participer à l'orientation de la solution proposée par l'ACEI;
- Soutenir la mise en place au Québec par des actions d'information concertées avec l'ACEI.

b. Favoriser le déploiement de l'IPv6 au Québec

ISOC Québec recommande d'effectuer une veille sur le déploiement de l'Ipv6 et d'en informer la communauté québécoise.

c. Surveiller l'évolution du DNS d'Internet

ISOC Québec propose les actions suivantes concernant l'évolution du DNS :

- Effectuer une veille sur l'évolution du DNS actuel, particulièrement par rapport au DNS lui-même géré par ICANN, mais aussi aux autres systèmes parallèles pouvant supplanter le DNS actuel (comme le ORSN- European Open Root Server Network), et ce, dans l'objectif d'assurer au Québec des solutions de rechange au DNS si des problèmes techniques ou politiques surviennent qui mettent en question la survie ou l'accessibilité du DNS actuel;
- Effectuer une veille sur l'évolution du système de nommage et d'adressage des objets (ONS) et en informer la communauté québécoise;
- Effectuer une veille sur l'évolution des noms de domaine générique;
- Proposer à l'ICANN un travail conjoint sur la taxonomie des noms de domaine générique et s'assurer de la cohérence de tout nouveau nom de domaine entre ce nom générique et les sites Web qui s'y inscriront. Actuellement, ces noms ne veulent plus trop dire quelque chose et cela va avoir un impact sur la taxonomie des contenus où on devra refaire le travail du DNS;

- Proposer à ICANN un groupe de travail pour contourner le problème de retrouver certains noms génériques « cachés » au 2e niveau d'un code de pays (comme « .com.fr » plutôt que « .com »). Il serait intéressant que cette information de taxonomie soit connue et disponible par les outils de recherche et de repérage;
- Proposer à ICANN un travail conjoint sur la signification des noms de domaine de code de pays afin d'éviter une dérive de l'utilisation des codes de pays pour autre chose (exemple : « .tv » et « .tk »);
- Soutenir l'initiative française et européenne d'ajouter un nom de domaine générique « .kid » et participer à l'élaboration du processus de gestion de ce domaine afin de s'assurer de la valeur des noms de domaine. Y insérer un processus d'homologation approprié.

d. Soutenir une décentralisation des serveurs racine

Actuellement, même s'il existe plusieurs serveurs miroirs, la très grande majorité d'entre eux sont contrôlés par les États-Unis. ISOC Québec propose que la *décentralisation des serveurs racine* soit effectuée afin de réduire quelque peu l'hégémonie américaine dans la gestion du DNS. Il serait intéressant, par exemple, que l'ACEI puisse gérer un tel serveur racine ou une autre autorité canadienne choisie par consensus ou appel d'offre.

Lutte à la fracture numérique

Actuellement, au Québec, ce ne sont pas tous les foyers qui ont accès à Internet à haute vitesse. Il y a un impact sur la protection de la jeunesse sur Internet :

- Nouveau danger : cyberexclusion chez les jeunes ou fracture numérique (due à la difficulté d'accès à Internet à large bande à prix abordable et au problème d'alphanétisation) (étude MediAppro);
- Abandon d'Internet par les parents si Internet à haute vitesse non disponible, ce qui a pour effet d'amoindrir le contrôle et l'éducation parentale.

Internet est considéré comme un bien commun de l'humanité et le service Internet devrait être un peu comme les services d'électricité au Québec – disponibles partout au Québec au même tarif. Il est important de ne pas tolérer des zones de seconde classe (basse vitesse ou tarifs désavantageux par rapport aux zones plus densément peuplées). ISOC Québec recommande que *tous les citoyens du Québec, incluant ceux des zones éloignées, aient accès à Internet à large bande (ou haute vitesse) à des prix acceptables*. À cette fin, les partenaires suivants pourraient être mis à contribution : le gouvernement du Québec (MDÉI et MSG, notamment) et du Canada (Industrie Canada ou Développement économique Canada), l'industrie et la société civile.

Veille sur projets de recherche

ISOC Québec propose d'exercer une vigie sur deux projets de recherche au R.U. ayant trait à la protection de la jeunesse :

- **projet Internet Safety Content Agent** (**ISCA**) dirigé par le Cyberspace Research Unit (CRU) de University of Central Lancashire (UCLAN) en partenariat avec le Home Office Internet Task Force. L'objectif du projet est d'augmenter les niveaux de sensibilisation et d'éducation à la sûreté sur Internet auprès de clientèles variées et particulièrement les enseignants, les parents et les jeunes gens. Ce projet a ceci de particulier : il vise à fournir, sans frais pour les fournisseurs de contenu ou de services, du matériel de sensibilisation par le biais d'un réseau de sites Web de tierce partie afin d'atteindre une couverture maximale, plutôt que par le biais d'un seul site Web. Ce projet apparaît très structurant et fédérateur pour toutes les activités de sensibilisation et de formation reliées à la protection des mineurs lors de leur navigation sur Internet;
- **projet COMPANIONS**, dirigé par l'Oxford Internet Institute. Ce projet vise à offrir un environnement d'accès au Web personnalisé selon l'utilisateur, en langue naturelle, et dont une version pourrait éventuellement être développée par la suite pour la jeunesse.

Annexe 1 : Liste des personnes et organismes

Consulter le document complémentaire.

Annexe 2 - Détail de la revue de littérature

Consulter le document complémentaire.