Bruno Hénocque **УДК 811.133.1**

RESPONSABILITÉ JURIDIQUE ET ÉDUCATION AUX MÉDIAS NUMÉRIQUES

ПЕРСОНАЛЬНАЯ ОТВЕТСТВЕННОСТЬ И ОБРАЗОВАНИЕ В ИНФОРМАЦИОННЫХ СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Аннотация. *В статье рассматривается вопрос защиты репутации подростков в Интернете, в частности, в социальных сетях (Фейсбук, Твиттер...). Цель данной работы заключается в изучении уважительного отношения к свободе выражения в Интернете. Часть решения этого вопроса заключается в формировании правильного отношения к средствам массовой информации, для того, чтобы быть натренированным в применении этих технологий, а также для получения навыков безопасного использования Интернета, зная законы и этические правила. Самый важный этический принцип - воспитание моральных норм и правил. В некоторых странах персональная ответственность введена с 13 лет. Такая ответственность касается как личной, так и общественной жизни. Защита свободы выражения, мысли, информации и сообщества в Интернете зависит от обучения в будущем цифровым средствам массовой информации в школе.*
Ключевые слова: *средства массовой информации, персональная ответственность, свобода высказывания, законы, правила.*

Summary. *The purpose of this article is to study the respect of freedom of expression on the Internet, especially in the social networks (Facebook, Twitter...). The main question is to protect the teenagers' dignity in these virtual spaces. A part of the solution is in the role of education for media use, not only to train on the use of technologies but also to use the Internet in a confident manner knowing the ethic rules and laws. The more important ethical principle is the moral and Law education. In some countries individual reponsability is engaged from 13 years old. This responsibility exists in private life as well as in public life. The protection of freedom of expression in the matter of opinion, information and association on the Internet depends partly on future education on the use of numeric media at schools.*
Key words: *media education, social media, freedom of expression, responsibility, laws, human's dignity*

Анотація. *В статті розглядається питання захисту репутації підлітків у Інтернеті, зокрема, в соціальних мережах (Фейсбук, Твіттер…). Мета даної роботи полягає у вивченні поважного ставлення до свободи висловлення в Інтернеті. Частина рішення цього питання полягає у формуванні правильного відношення до засобів масової інформації, для того, щоб бути натренованим у застосуванні цих технологій, а також для отримання навиків безпечного використання Інтернету, знаючи закони та етичні правила. Найважливіший етичний принцип – виховання моральних норм та правил. У деяких країнах персональна відповідальність введена з 13 років. Така відповідальність стосується як особистого, так і громадського життя. Захист свободи висловлювання, думки, інформації та співтовариства в Інтернеті залежить від навчання в майбутньому цифровим засобам масової інформації в школі.*
Ключові слова: *засоби масової інформації, персональна відповідальність, свобода висловлювання, закони, правила.*

Introduction

En attendant que les géants de l'Internet ne cherchent à mieux réguler le Web social,quel rôle peut jouer une éducation aux médias numériques respectueuse de la dignité humaine des enfants et des adolescents?Cette éducation aux médias est perçue comme nécessaire dans de nombreux pays (*Jeunes et Médias*, 2012). Elle vise à faciliter une appropriation plus sereine des médias sociaux (Facebook, Twitter...) par les jeunes internautes.Les enjeux sont suffisamment importants pour que les professionnels du numérique, regroupés dans un collectif, aient demandé au gouvernement français de faire du numérique une grande cause nationale dans les prochains mois.Cette culture du numérique devrait couvrir plusieurs domaines,dont le droit et l'éthique, en plus de la sociologie des usages et de l'économie. L'éducation aux médias doit permettre de recevoir plus sereinement les informations véhiculées par la presse à scandale dont les discours peuvent génèrer une grande anxiété.Certes, les atteintes au droit de la personne humaine sont rares rapportées au nombre des internautes utilisant les médias sociaux,mais les affaires relatives à des enfants ou à des adolescents sont suffisamment marquantes pour soulever à chaque fois l'indignation de l'opinion publique.Evoquer une éducation aux médias numériques conduit à centrer son propos à la fois sur la liberté d'expression (ONU, 2012) et sur la responsabilité juridique des auteurs pour les contenus numériques diffusés.Un internaute est responsable en effet du fait personnel en cas de dommages psychologiques causés à autrui.Il encourt des poursuites pénales à partir de 14 ans en Italie, Allemagne, Espagne et Autriche, de 13 ans en France et de 10 ans en Angleterre.Les parents et les enseignants sont responsables du fait d'autrui en cas de dommages causés par un enfant ou un adolescent qui n'a pas encore atteint l'âge de la responsabilité pénale.Cette démarche de responsabilisation est inscrite dans les recommandations faites par l'*Organisation des Nations unies pour l'éducation, la science et la culture* (UNESCO).il se trouve que l'offre de connexion au Web social est grandissante et que l'Internet des objets se développe partout. Les jeunes internautes sont parmi les plus connectés et disposent chacun d'au moins un support de connexion au Web: ordinateur ou tablette connecté, smartphone, parfois TV connecté, en attendant peut-être de se connecter aux réseaux sociaux et aux jeux en ligne sur les futurs automobiles connectées par Wifi. Si Internet est ainsi relié progressivement aux objets, l'homme connecté s'expose aussi davantage à des atteintes au droit de la personne humaine et à sa dignité.Le sujet est important quand on sait que le nombre de personnes inscrites sur un ou plusieurs réseaux sociaux est de 1,5 millard dont plus de 1 milliard 200 millions à Facebook et 200 millions sur le réseau social professionnel Linkedin. Enfin, 175 millions de tweets sont postés chaque jour.

Quelle éducation aux médias numériques?

Dans le contexte de ce développement exponentiel des médias numériques, l'UNESCO(2007) suggère plusieurs actions prioritaires, en premier lieu l'éducation aux médias et la mise en place de codes d'éthique.Yves Poullet (2007, p15)souhaite que les fournisseurs de services participent comme les établissements scolaires à cette éducation aux médias numériques. Il insiste pour que les utilisateurs de forum de discussion, de communautés virtuelles et de jeux en ligne soient attentifs à la "dimension d'autrui". Yves. Poullet propose ainsi l'apprentissage de règles procédurales.

Une traduction concrète de cette orientation est le dispositif du *Permis de bonne conduite sur Internet* pour les élèves français de CM2(enfants en moyenne de 10 ans). Ce dispositif se rapproche par analogie du *Permis piétons* déjà délivré aux élèves de CE2(enfants en moyenne de 8 ans)afin de les sensibiliser aux risques routiers. Des brigades de prévention de la délinquance juvénile participent dans les écoles à des actions de prévention, pour susciter les bons comportements parmi les enfants.Leur intervention fait débat actuellement par des enseignants qui souhaitent garder le contrôle de la formation.Il serait souhaitable que les programmes fassent une priorité de l'éducation aux médias, comme le demande par ailleurs la *Commission Nationale Informatique et Libertés* (CNIL) pour 2014.La demande de la CNIL a reçu le soutien de 50 organisations spécialisées dans le numérique et l'appui de personnalités de premier plan investies dans le numérique. Il s'agirait de donner aux professeurs de cycle élémentaire et aux intervenants toutes les possibilités d'éduquer pleinement les enfants aux règles qui régissent la liberté d'expression sur le Web. Le *Permis de bonne conduite sur Internet* vise déjà à inciter le développement de bons réflexes parmi les jeunes de 9-11 ans,en particulier de signaler à un parent,un professeur ou aux autorités (en France, www.pointdecontact.net ou encore www. Internet-signalement.gouv.fr) des contenus attentatoires à la dignité humaine (provocation au suicide, pornographie enfantine,incitation à la haine raciale et plus largement à la violence...).Cette éducation aux médias numériques ne doit en aucun cas porter atteinte à la vie privée et à l'intimité de la vie privée.La directive européenne 95/46/CE du 24 octobre 1995 le déclare explicitement dans l'article 1: «les Etats membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée à l'égard du traitement des données à caractère personnel».Cette éducation aux médias concerne étroitement les parents d'élèves autant que les professeurs car les contenus des médias sociaux relèvent selon les cas de la sphère publique ou de la sphère privée.Parmi les bonnes attitudes figure la compréhension du principe de finalité dans la collecte et le traitement des données. En effet,si le recueil de données à caractère ethnique est bien sûr interdit, il existe des cas où la collecte de cette catégorie d'information peut être tolérée, par exemple pour une entreprise de cosmétique qui veut proposer à chaque jeune fille une couleur de rouge à lèvres en parfaite adéquation avec sa couleur de peau. Ce qui prévaut, c'est donc dans ce cas le principe de finalité dans le traitement des données à caractère personnel. La directive européenne 95/64/CE du 24 octobre 1995 précise que les données «doivent être adéquates, pertinentes et non excessives au regard des finalités poursuivies» et qu'elles «doivent être explicites et légitimes».Le principe de finalité est déjà inscrit dans la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ce principe signifie que les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé. Tout détournement de finalité est passible de sanctions pénales.

La responsabilité juridique des jeunes internautes

Pour Michelle Blanc (2011), les médias sociaux sont véritablement ambivalents. Ils sont tout à la fois un lieu de socialisation et«un Far West sans foi ni loi que même les plus importants bénéficiaires (les plateformes elles-mêmes) n'arrivent pas à réguler onvenablement» (p. 174). Ils ont ainsi cette double face qu'André Vitalis (1991) assimilait à celle du Dieu romain Janus.

Il n'est pas exact cependant d'écrire qu'il n'existe pas de loi dans les affaires relatives aux atteintes au droit de l'homme sur les réseaux sociaux (atteinte à la vie privée, diffamation, harcèlement et intimidation). Tout un ensemble de textes,que les jeunes devraient connaître sommairement dès l'école primaire, existe dans les pays européens signataires de la *Convention européenne des droits de l'homme* (2010). L'Ukraine comme la France font partie du Conseil de l'Europe. Les jeunes internautes et les adultes responsables doivent en effet être conscients des limites qui existent à la liberté d'expression et de la chance sans précédent dans l'histoire que représentent ces médias sociaux.

Depuis 2008, des affaires de diffamation et d'injures publiques sur des médias sociaux ont mis en cause de nombreux internautes dans plusieurs pays. Ces affaires ont souvent trait à des internautes qui ont imprudemment ouvert leur profil, permettant aux abonnés du média social de lire les propos parfois incendiaires qu'ils tiennent contre un supérieur hiérarchique ou un professeur dans une école. Sur la foi, notamment, de leurs écrits(parfois signés) rendus publics, ces jeunes internautes ont été condamnés,Facebook ou Twitter fournissant ainsi des preuves à charge.Adresser un message par un réseau social à un «ami» sur son «mur» ne protège pas l'émetteur au même titre qu'une correspondance privée. Le fait de créer ainsi un «événement public» sur un réseau social engage la responsabilité de son auteur.Mais paramétrer son profil pour le fermer suffit-il à distinguer la sphère privée de la sphère publique?En effet, plus de 130 "amis" constituent la moyenne sur Facebook par utilisateur. A partir de combien "d'amis" un espace privé devient-il dès lors public? A cela s'ajoute pour Facebook le fait que certains messages privés sont apparus sur des espaces publics, à la suite de bugs. Certains des messages privés sont apparus ainsi sur le «Timeline» mélangés à des messages publics. Mais,il est des cas où les messages sont si scabreux qu'ils soulèvent l'indignation d'un nombre considérable d'internautes. Un jeune homme français a ainsi scandalisé l'opinion publique sur Facebook fin janvier 2014.Il a été filmé projetant à plusieurs reprises un petit chat roux contre un mur et sur un sol en béton. Cest pourquoi, 93.000 signataires en ligne et 43.000 fans d'un groupe Facebook ont réclamé une peine de prison contre ce jeune homme, avant sa comparution au tribunal correctionnel.Sur la foi de cette vidéo postée sur le Web, la Cour a condamné le 3 février 2014 à un an de prison

ferme l'auteur de ce méfait pour «actes de cruauté envers un animal domestique ou apprivoisé».

De la diffamation aux messages de haine

Le fait est que le Web est devenu aussi la tribune, le terreau de propos racistes ou négationnistes.Il est indéniable que des internautes trouvent sur le Web la possibilité de partager en un clic leur message avec des milliers d'internautes. Dans certains cas extrêmes, les directeurs de la publication coopérent pour rechercher les auteurs des propos discriminatoires.Mais la plupart du temps, les victimes sont désarmés devant la violence des mots.Michelle Blanc(2011, p.169) évoque les messages haineux dont elle a fait l'objet sur les médias sociaux ou sur son blog, qu'il s'agisse de menaces, de diffamation ou d'intimidation, y compris de la part de ses «amis» sur Twitter et Facebook, qualifiés par l'auteur de «méchants voyeurs»et de «chercheurs de trouble».A chaque fois, La loi protège la liberté d'opinion et condamne la discrimination fondée sur l'appartenance ou la non-appartenance à un ethnie, une nation ou une religion.S'agissant du racisme, on peut distinguer trois délits possibles. l'injure raciale (expression outrageante, termes de mépris ou invectives),la diffamation raciale (allégation ou imputation d'un fait qui porte atteinte à l'honneur d'une personne)et la provocation raciale (écrits ou annonces publiques). Plus de 2000 plaintes relatives à des propos tenus publiquement dans les médias, sur le Web (ou dans la rue) ont été enregistrés en France par exemple en 2012 (source: *Commission nationale consultative des droits de l'homme*). C'est ainsi que Twitter a fini par communiquer aux autorités les adresses et les noms des utilisateurs du mot clé #unbonjuif.

Comme Michelle Blanc, Caroline Criado-Perez en Grande-Bretagne a reçu sur son compte Twitter de nombreuses menaces et non des moindres puisqu'il s'agit de menaces de viol. La cause de ce cyberharcèlement?Elle a simplement demandé à ce que l'effigie de l'écrivain féministe Jane Austen figure sur les billets britanniques de 10 livres en 2017! Afin de se protéger mentalement du harcélement, Michelle Blanc propose une méthode en cinq étapes, inspirée de l'analyse transactionnelle. Le risque, écrit-elle, est d'entrer dans le triangle dramatique, dit triangle de Karpman (Brecar, Hawkes, 2008), qui repose sur un scénario relationnel typique entre victime, persécuteur et sauveur.L'auteur écrit: "C'est une schématisation qui tend à exprimer que, si une personne endosse un de ces rôles, elle entraîne l'autre à jouer un rôle complémentaire (le sauveur ou le persécuteur)" (2011,p. 170). Mais cette distance vis-à-vis de la cyberintimidation suppose une prise de recul que des adolescents émotifs n'ont pas.De plus, le fonctionnement de certains réseaux sociaux où l'anonymat est possible peut donner un sentiment d'impunité. Certes, la violence se retrouve dans les autres domaines de la vie en société mais la différence est que cette violence est potentiellement visible de tous ces «amis» ou de tous les abonnés au réseau social.

Ce qui est en cause est donc l'anonymat dont bénéficient les auteurs. Aucun réseau social n'est dangereux en soi. Cette cyberintimidation souligne l'importance d'une éducation aux médias, afin de développer parmi les enfants ou adolescents connectés des réflexes d'alerte auprès d'un parent, d'un professeur ou d'un site de signalement. Un juge français peut même ordonner un référé d'urgence en cas de danger grave et imminent.

Plusieurs affaires de suicides d'adolescents britanniques mettent en particulier en cause le réseau social Ask.fm depuis 2012 et 2013. Ces suicides ont provoqué une émotion considérable dans l'opinion publique.Ce réseau a été le foyer d'un grand nombre de messages de haine, leurs auteurs s'imaginant protégés par l'anonymat qui est toléré sur ce média. Ces affaires ont d'autant plus choqué en Grande-Bretagne que ces pratiques culturelles se forment en dehors du monde des adultes qui peuvent tout ignorer du drame vécu par l'enfant.Ces messages sont en outre visibles des 60 millions d'inscrits du site.

Parmi les victimes,Hannah Smith(14 ans) partageait ses tourments avec d'autres adolescents. La jeune Anglaise, inscrite sur le site Ask.fm, s'était livrée sur le souci que lui causait son eczéma. Victime d'un cyber harcèlement d'une rare violence,elle s'est donnée la mort. D'autres adolescents britanniques se sont suicidés aussi, après avoir eux aussi reçus de nombreux messages anonymes insultants, voire haineux sur le même site. Partout, l'affaire a soulevé l'indignation en raison de l'anonymat et de l'absence de contrôle parental. Le Premier ministre britannique a appelé au boycott de ce réseau. Cette question est suffisamment importante pour qu'une province du Canada, la Nouvelle-Ecosse, ait promulguée une loi qui punit la cyberintimidation(*Cyber safety act*, 2013).

Un autre exemple moins dramatique relevant cette fois du cyberchantage a surpris l'opinion publique française en 2013. Un adolescent a été victime d'une cyberchantage, son harceleur menaçant de diffuser sur le Web la vidéo où il se déshabillait imprudemment face à une webcam!

Afin de réduire toutes ces dérives regrettables,des associations se sont investis depuis plusieurs années dans une sensibilisation aux dangers du Net auprès des jeunes et des parents qui le souhaitent. Les associations françaises de protection *e-Enfance* et *Calysto* en font partie.Il serait vivement souhaitable que ces initiatives se développent et soient soutenues.

Une autre forme de harcèlement (le *stalking* en anglais) s'est développée récemment. Elle met en cause des photos prises à l'insu de célébrités (Jodie Forster aux Etats-Unis ou Mylène Farmer au Canada) ou d'adolescentes et, à degré moindre, d'adolescents.Avec le Web, le harceleur développe un sentiment d'impunité, sature la boite mail de la personne, envoie des virus et agit dans la sphère privée ou la sphère publique de sa victime. Les femmes sont les victimes les plus fréquentes de ce harcélement et dans 80% des cas, les harceleurs sont des hommes. Dans plusieurs pays de l'union européenne, (Italie, Belgique ou Luxembourg), existent déjà des lois contre ce harcèlement.

Le droit à l'image et à la vie privée

Dans La loi française, chaque personne dispose d'un droit exclusif sur son image et peut de manière discrétionnaire en autoriser la reproduction (Code civil, article 9). Le fait de capter, reproduire et diffuser l'image d'une personne prise dans un lieu privé sur le web sans son autorisation est une atteinte à la vie privée ou à l'intimité de la vie privée"

La question de la vie privée et du droit à l'image est problématique pour les touristes par exemple car il existe des disparités d'un pays à l'autre. Un ressortissant français ou étranger filmé ou photographié à son insu en France et dont les images sont ensuite diffusées sur le Web peut saisir un tribunal français pour atteinte au droit à l'image, si

le diffuseur est domicilié en France. Ainsi, l'une de mes étudiantes,manifestante dans le cadre de la loi française relative au mariage pour tous du 17 mai 2013, a vu sa photographie, ses prénom et nom et sa ville de résidence apparaître sur le Web, ce qui la rendait tout à fait identifiable. Il a suffi d'une lettre au directeur de la parution pour enlever cette atteinte à sa vie privée. Il est interdit en France en effet de capter, reproduire et diffuser sur le Web l'image d'une personne sans son autorisation. Sont tolérées des scènes de groupe dans la rue. Une personne ne peut faire l'objet d'un gros plan, sauf si elle est l'objet même de la manifestation, si elle porte une banderole ou un porte-voix ou encore si elle est l'organisatrice ou la responsable associative de l'événement.

Nous abordons maintenant le cas de photographies d'enfants qui sont«instrumentalisés» par un parent sur un média social afin de servir une conviction politique. Un père français a dû ainsi comparaître en septembre 2012 devant le tribunal correctionnel de Lyon pour «incitation à la haine raciale», avant finalement d'être relaxé pour avoir posté sur un réseau social des photographies montrant son enfant enveloppé du drapeau de l'Allemagne impériale de Guillaume1°,confondu par les enquêteurs avec le drapeau nazi. Il s'agit d'une confusion qui montre à quel point la diffusion sur le Web d'un message, quel qu'il soit, peut avoir des conséquences regrettables.

Mais il y a beaucoup plus grave. L'image créée de toutes pièces en 3D puis diffusé sur le Web d'un enfant philippin de10 ans appelée Sweetie a permis de débusquer un nombre important de pédophiles interagissant avec cet enfant par des messages à caractère sexuel.L'approche de la branche néérlandaise de l'association *Terre des Hommes* qui l'a créé est constructive car elle n'a pas eu d'impact sur un enfant réel Elle permet en outre de surveiller les cyberpédophiles.Selon *Terre des hommes*, qui cite des chiffres de l'ONU, 750 000 cyberpédophiles en moyenne à travers le monde seraient en ligne simultanément(Silicon.fr, Septembre 2009). En France, le service cybercriminalité de la gendarmerie permet à des agents de se faire passer pour des enfants. A la division de lutte contre la cybercriminalité (DLCC), les enquêteurs du département de répression des atteintes aux mineurs sur Internet (Rami) réalisent ainsi des investigations sous pseudonyme.Ils peuvent se rendre sur le Web avec une identité fictive d'adulte ou de mineur, ou prendre le relais d'une identité réelle(celle d'un enfant contacté par un pédophile par exemple). La loi française sur la prévention de la délinquance (mars 2007) le permet tout en interdisant toute provocation à de telles infractions à la loi.

Les chartes du bon usage des ressources informatiques

La e réputation est devenue un enjeu majeur. Dans ce cadre, à l'occasion d'une candidature à un stage ou à un emploi,le premier réflexe des entreprises est de rechercher les informations que le candidat a posté sur les médias sociaux (photographies, vidéos, forums de discussion).

Au sein des établissements scolaires, les chartes informatiques en particulier sont, de plus en plus répandues. Elles engagent bien entendu la responsabilité de tous les usagers. Les chartes des entreprises sont moins connues.Les élèves et les étudiants stagiaires sont tenus de respecter la charte informatique comme l'ensemble des salariés.Les connexions à l'extérieur de l'entreprise soulèvent en effet de tels problèmes de sécurité qu'il conviendrait d'assurer des connexions personnelles urgentes sur un ordinateur isolé et déconnecté des intranets et des réseaux informatiques "sensibles" de l'entreprise afin de ne pas rapatrier de virus ou de risquer des intrusions extérieures.

Ainsi, la connaissance des chartes des ressources informatiques devrait faire partie d'une éducation aux médias numériques. A cet égard, la charte pionnière (2001) du groupe Renault est très éclairante. Cette charte s'adresse tout aussi bien aux salariés qu'aux stagiaires issus du système éducatif. Sont évoqués dans cette charte les points sur lesquels la responsabilité de l'utilisateur est engagée. Ainsi, le risque de voir l'adresse IP d'un stagiaire ou d'un salarié reprise dans un courrier de masse comportant des contenus d'information illicites n'est pas à écarter, si la connexion a lieu de son poste de travail. A cela s'ajoutent les risques d'interception d'enregistrement et d'utilisation de messages émis du poste du travail à d'autres fins par un tiers, afin de capter des préoccupations de l'entreprise ou d'accéder à des techniques de fabrication. Les révélations liées à l'affaire Snowden n'ont fait qu'accroître la prise de conscience des risques encourus. Les questions de la e-regulation et des atteintes à l'image de marque de l'entreprise se posent toutes les fois où des traces numériques sont laissées sur un site de connexion. La participation anonyme à des forums de discussion engage également la responsabilité des utilisateurs,sachant aussi que les règles juridiques qui régissent les sites Web ne sont pas les mêmes dans tous les pays.

Cependant, la question des usages privés au travail n'est pas si simple à réguler. Des usages privés au travail ne peuvent être différés comme par exemple l'organisation de la réception d'un colis à domicile, aux heures ouvrables de l'entreprise de livraison. La Commission nationale informatique et liberté (CNIL) évoque dans ses recommandations un usage "raisonnable"(rapport du 5 février 2002) des outils de connexion dans la sphère professionnelle, mais il s'agit là d'une tolérance propre à la France. En tout état de cause, la question des frontières de la vie privée et de la vie publique à l'ère du numérique en situation de travail hiérarchique est peu traitée dans la littérature, comme le rappelle justement Béatrice Rey (2013, p 105). Il est utile en France de s'appuyer sur l'arrêt de la chambre sociale de la cour de cassation du 2 octobre 2001, relatif à la célèbre affaire entre M. Onof et la société Nikon en France pour comprendre ce que sont les enjeux depuis de nombreuses années. Cet arrêt qui a cassé et annnulé la décision de la Cour d'appel, reconnaît en effet le droit au respect de l'intimité de la vie privée et au secret des correspondances. Cette tolérance propre à la France fait qu'un salarié est protégé par la loi s'il a créé un fichier intitulé «personnel» ou «privé» ou un en-tête de courriel «personnel » ou «privé». Cependant, s'il ne s'agit pas d'une atteinte à la vie privée,un employeur peut accéder à une messagerie (et dans certains cas saisir le disque dur de l'ordinateur) en dehors de la présence du salarié.S'agissant du contrôle exercé sur les messages produits par les stagiaires ou les salariés, il serait en en effet simplificateur de dénoncer toutes formes de contrôle ou d'assimiler les dispositifs de surveillance à la seule structure panoptique imaginée par le grand philosophe anglais du droit Jérémy Bentham (1791). Non pas que le sentiment d'omniscience invisible créé par le dispositif ne soit pas un modèle possible pour représenter le contrôle permanent exercé dans l'entreprise par des systèmes informatiques en

étoile.Mais les tentatives d'intrusion dans les systèmes d'information des entreprises et d'interception des messages numériques émis et reçus par les entreprises atteignent un tel niveau qu'il convient de renforcer les dispositifs de protection des données qui transitent par réseaux filaires ou hertziens.

Vers de nouveaux réseaux sociaux?

Il se crée sans cesse de nouveaux réseaux sociaux dans le monde.En quelques années, ces médias sont devenus omniprésents dans nos vies. En France, ils ont conquis près de 32 millions d'adeptes et près des deux tiers d'entre eux se connectent au moins une fois par jour. Les réseaux sociaux ont des limites, notamment en termes de protection de la communication et de respect de la vie privée Dans la mesure où beaucoup d'utilisateurs évoquent des craintes concernant l'utilisation de leurs données personnelles, la nouvelle plateforme Whaller permet à chaque internaute de construire ses propres réseaux sociaux. Whaller permet surtout de cloisonner ses communications selon qu'elles concernent les amis, la famille ou encore les collègues. Représentés sous formes de "sphères", les différents réseaux(amical, familial et professionnel) sont privés et cloisonnés. Une caractéristique qui supprime le côté "voyeur potentiel"(Michelle Blanc, 2011) de ses «amis». Le site accorde énormément d'importance à la protection des données personnelles. C'est pourquoi, les responsables s'engagent à ne pas les exploiter à des fins commerciales. De plus, ces données ne sont pas conservées. Enfin, Whaller est garanti sans publicité. Cette plateforme cherche aussi à « éduquer les nouvelles générations à une bonne utilisation du numérique ».

Conclusion

Le droit de l'Internet doit prendre toute sa place dans une éducation aux médias numériques dont on espère qu'elle va faire son entrée ou se renforcer dans les systèmes scolaires européens. Des initiatives comme **le Permis de bonne conduite sur Internet** proposé en France à l'école primaire sont intéressantes mais il conviendrait d'évoquer sérieusement la question de la liberté d'expression sur le Web et de slim:ites de cette liberté à tous les niveaux de la scolarité. Actuellement, les technologies de l'information et de la communication (TIC) sont seulement abordées en France dans les sections de technologie au collège ou dans l'option Informatique et sciences du numérique ouverte depuis septembre 2012 en terminale scientifique.

Plusieurs libertés fondamentales sont finalement à protéger : la liberté de réunion et la liberté d'expression, d'information et d'opinion.Que d'aucuns prennent prétexte des abus pour limiter ces libertés, surveiller les réunions par le Web, voire interdire des sites Web est un risque évident, y compris dans des pays qui ont ratifié la Convention européenne des droits de l'homme.

Bibliographie

1. Jérémy Bentham. *Panoptique* (1791) traduction en français de Christian Laval. Ed. Mille et une nuits. 2002.
2. France Brecar, Laurie Hawkes. *Le Grand livre de l'analyse transactionnelle*. Ed. Eyrolles. Paris. 2008
3. Centre d'études sur les jeunes et les médias. *Jeunes et Medias. Les cahiers francophones de l'éducation aux médias*. «L'éducation aux médias dans le monde. Etat des lieux et perspectives». Ed. Publibook. Paris. 2012. N°4
4. Conseil des droits de l'homme des Nations Unis (ONU). Résolution sur les droits des internautes à la liberté d'expression. 6juillet 2012. New York. EU
5. Michelle Blanc. *Les médias sociaux*. Les Editions logiques. 2011 Québec (Canada).
6. Groupe Renault. *Charte du bon usage des ressources informatiques électroniques et numériques du groupe Renault du 1er juillet 2001*. Liaisons Sociales.Paris Conventions et accords. 2 août 2001.
7. Béatrice Rey. *La vie privée au travail.Retour sur la place du privé en contexte hiérarchique à l'ère du numérique* Les Cahiers du numérique. Paris. N°2/2013. P. 105-136
8. Yves Poullet. Rapport final. *Ethique et droits de l'homme dans la société de l'information.* Actes, synthèse et recommandations. Conférence de la région Europe organisée par la l'UNESCO et le Conseil de l'Europe. Strasbourg. 13-14 septembre 2007, P. 7-18.
9. Mary Rundle.«Identités et réseaux sociaux» in *Ethique et droits de l'homme dans la société de l'information*. Strasbourg. 13-14 septembre 2007, pp. 40-44.
10. André Vitalis. *La fausse transparence du réseau*. Réseaux n°48.Vol.9.CNET.1991.pp51-58

Webographie

1. «Convention européenne des droits de l'homme».Conseil de l' Europe et Cour européenne des d roits de l'homme.Strasbourg.1° juin 2010 in www.echr.coe.int
2. «L'éducation au numérique, grande cause nationale 2014?». 1° octobre 2013 in www.cnil.fr/les-themes/scolarite-mineurs/actualites-education/.
3. *Loi sur la liberté de la Presse* du 29 juillet 1881.. Articles 23, 24, 42. www.legifrance.gouv.fr
4. *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* in. www.legifrance. gouv.fr
5. *Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* in www.legifrance.gouv.fr
6. Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 *relative à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. in www.publications.europa.eu/official/index.fr.htm. www.silicon.fr/pedophilie-sur-internet-lonu-tire-lasonnette-dalarme Septembre 2009
7. Association des Fournisseurs d'Accès et des Services Internet (AFA). www. passe-permis-web-quizz-afa
8. Loi sur la cyber-sécurité de la Nouvelle-Ecosse (Canada) in www.nsbs.org/parts-cyber-safety-act-now-effect-nova-scotia *6* août 2013
9. Guide d'usage pour la lutte contre la pédopornographie. 22/01/2014 in www.afa-france.com.