DOCTRINE

La régulation du web 2.0[1]

Pierre Trudel[2]

Le rôle central de l'usager est souvent présenté comme une caractéristique majeure du web 2.0. L'expression «web 2.0» vise des situations dont le trait commun est une intensité accrue de l'implication des usagers dans les environnements en ligne. Tant au plan juridique que dans ses configurations pratiques, l'environnement que constitue le web 2.0 se caractérise comme un réseau. Alors que plusieurs fonctions emblématiques d'internet des premières époques se présentent sous une forme analogue aux médias diffusés, le web 2.0 prend résolument l'allure d'un réseau. Au sein du réseau, les usagers, professionnels ou amateurs, assument des rôles déterminants aussi bien au plan des contenus que des processus de fonctionnement. Mais en plus, ils sont en situation d'engendrer des risques pour les autres, ce qui les investit d'une capacité de régulation.

À l'instar des autres dimensions d'Internet, le web 2.0 est un réseau constitué de nœuds et de relais de normativité. Chaque nœud dispose d'une certaine capacité d'imposer des normes aux autres interconnectés. La faculté d'imposer des normes est principalement tributaire de la capacité effective d'engendrer des risques pour les autres. La question de la régulation du web 2.0 doit donc être abordée en tenant compte des enjeux et risques que posent les principales activités qu'on y associe.

Sur Internet, la régulation s'applique en réseau et selon un mode réseautique, elle est pensée et produite dans les nœuds de normativité d'Internet que sont les instances étatiques, les lieux de conception des normes techniques de même que les différents acteurs. Ces derniers relaient à leurs partenaires les exigences et les risques qu'ils ont à gérer. Ainsi envisagée, la régulation des environnements du web 2.0 est essentiellement une démarche continue de prise en compte et de gestion des risques perçus. La notion de risque permet de rendre compte du phénomène de modulation dans l'application effective des droits nationaux sur Internet.

Dans un réseau, les régulateurs et les acteurs sont en position d'accroître ou de réduire les risques pour eux-mêmes ou pour les autres. La technique produit des situations qui augmentent ou diminuent les risques. Il en est de même pour les lois étatiques et les autres normativités. Dans le cyberespace, les acteurs envisagent les contraintes et possibilités techniques de même que les lois qui sont susceptibles de s'appliquer à leurs activités comme autant de risques à gérer. La régulation agissante à l'égard du web 2.0 est essentiellement la résultante des stratégies de gestion des risques des acteurs et des régulateurs. Ces stratégies s'élaborent dans les différents nœuds de normativité. Les normes ainsi énoncées engendrent des risques pour les acteurs visés. Ces derniers auront à leur tour à gérer ces risques en relayant ces normes vers les autres participants aux activités du web 2.0.

• • •

[1] Étude réalisée dans le cadre du programme de recherche de la chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique et dans le cadre d'un projet de recherche appuyé par la fondation Quebecor. L'auteur a bénéficié de l'aide de France Abran, agente de recherche au Centre de recherche en droit public et de Cynthia Gaudette, étudiante au diplôme de droit notarial à la Faculté de droit de l'Université de Montréal.

[2] Professeur titulaire de la chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique, Centre de recherche en droit public, Faculté de droit, Université de Montréal, pierre.trudel@umontreal.ca.

ANGLAIS A VENIR

I. INTRODUCTION

Nous pouvons convenir que le vocable « web 2.0 » relève en partie du slogan ou du *buzzword*. L'expression demeure mal définie[3], mais elle renvoie à un ensemble de réalités et de situations qui échappent à une définition qui serait exhaustive[4]. Caractérisé par certains éléments emblématiques, le web 2.0 renvoie à une constellation de fonctions possédant des caractéristiques communes. Parmi ces caractéristiques, il y a un niveau élevé d'implication des usagers dans la fourniture de contenus. On associe également au web 2.0 ces environnements structurés dans lesquels les contenus

[3] Philippe Chantepie, « Éléments du Web 2.0 : interfaces, bases de données, plates-formes », Propriétés intellectuelles, 2007, n° 24, p. 285.

[4] Dion Hinchcliffe, « Review of the Year's Best Web 2.0 Explanations' », Web 2.0 Journal, http://web2journal.com/read/165914_p.htm.

sont créés en bonne partie par les utilisateurs comme les sites d'édition collective tel celui de l'encyclopédie Wikipedia. Ces sites permettent aux internautes d'éditer et de modifier des contenus à leur guise. Dans d'autres cas de figure, on évoque la possibilité de combiner des applications et des contenus et synchroniser un site web avec d'autres[5]. Les sites de partage de contenus comme YouTube ou Dailymotion permettent aux internautes de diffuser des contenus en ligne. Les sites de réseaux sociaux comme Facebook ou Myspace permettent aux individus de diffuser leur profil personnel de même que d'autres informations portant sur d'autres personnes[6]. Nicolas Vermeys observe que la notion de web 2.0 « désigne la tendance, observée chez certaines entreprises présentes sur le Web, à publier un contenu généré (*sic*) par les utilisateurs plutôt que de recourir au modèle d'affaires traditionnel de mise en ligne de contenus médiatiques propriétaires »[7].

Sur Internet, les usagers ont depuis longtemps la possibilité d'introduire des contenus en ligne. Ce qui paraît caractéristique du web 2.0 au plan du droit est le rôle plus actif que jamais tenu par l'usager. La notion de web 2.0 renvoie à une kyrielle de situations juridiques dans lesquelles les rôles paraissent moins stables ou délimités. Les réalités associées au web 2.0 sont en mutation constante et peuvent se trouver hors de la portée des lois de certains États. Devant un tel éclatement des catégories, on ne peut s'en tenir à considérer que la simple exégèse des textes promulgués du droit étatique suffit à rendre compte de la réglementation qui prétendrait assurer la régulation des environnements associés au web 2.0.

Il existe des phénomènes contribuant à moduler les normativités énoncées par les États ou les divers acteurs d'Internet et qui empêchent leur application de bout en bout du réseau. Malgré le caractère global du réseau, les appréciations et les valeurs présentent encore d'importantes différences dans les multiples milieux culturels dans lesquels s'appliquent les règles[8]. De tels phénomènes préviennent l'application de règles qui pourraient être décontextuées par rapport aux situations ou au substrat culturel dans lequel la norme s'applique. L'un de ces phénomènes paraît bien être le risque juridique[9] : l'évaluation que font les acteurs des possibilités concrètes d'application effective de lois nationales ou d'autres règles à leurs activités permet d'expliquer que même si Internet est un réseau global, personne ne se sent tenu de se conformer à la totalité des lois nationales qui peuvent théoriquement trouver application.

Afin de rendre compte du droit relatif au web 2.0, il faut s'intéresser à la normativité effectivement agissante : celle qui engendre suffisamment de risques auprès des acteurs pour que ceux-ci jugent opportun de s'y conformer. Le droit étatique n'est pas seul à encadrer les activités sur Internet : la normativité qui encadre les ressources associées au web 2.0 procède de ce que la technique permet ou prohibe, elle résulte en grande partie des pratiques obser-

5 Mary Madden et Susannah Fox, « Riding the Waves of « Web 2.0 » more than a Buzzword, but still not easily defined, Pew Internet, Backgrounder, http://www.pewinternet.org/pdfs\PIP_Web_2.0.pdf ; Lis Veasman, « « Piggy Backing » on the Web 2.0 Internet : Copyright Liability and Web 2.0 Mashups », 30 *COMM/ENT*, 2008, 311-337.

6 Steven James, « Social Networking Sites : Regulating the Online « Wild West » of Web 2.0 », 2 *Ent. L.R.*, 2008, 47-50.

7 Nicolas W. Vermeys, « Chronique – responsabilité civile et Web 2.0 », *Repères*, juillet 2007, http://rejb.edition-syvonblais.com/ (page visitée le 27 juin 2008).

8 Jack Goldsmith et Tim Wu, *Who Controls the Internet ? Illusions of a Borderless World*, New York, Oxford University Press, 2006, chapitre 9, « Consequences of Borders ».

9 Voy., pour une méthodologie d'analyse des risques juridiques : Franck Verdun, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, pp. 39 et s.

vées par les différents acteurs. Ces configurations et ces pratiques engendrent des risques ou visent à transférer des risques à d'autres. Mais les régulateurs étatiques peuvent estimer que les risques engendrés par des activités se déroulant sur Internet sont suffisamment préoccupants pour imposer aux acteurs des obligations et ainsi baliser ce qu'ils peuvent faire en ligne. Par leur réglementation, ils créent des risques pour les acteurs concernés.

Envisagée dans la logique du réseau[10], la régulation du web 2.0 s'exprime par une normativité agissante résultant des décisions de gestion des risques prises par les régulateurs et les acteurs actifs sur le net. Sur Internet, les États, les usagers, les entreprises et les autres acteurs gèrent des risques. Par leurs décisions et leurs comportements, l'ensemble des producteurs de normativités créent et relaient les risques issus de la normativité qui leur est applicable à leurs cocontractants et partenaires. Les producteurs de normes ne peuvent prétendre à la souveraineté dans le cyberespace, mais ils conservent une pleine capacité de formuler des règles qui engendrent des risques pour les acteurs.

I. LES RISQUES ET ENJEUX DÉCOULANT DES FONCTIONS ASSOCIÉES AU WEB 2.0

Plus encore que le web de première génération, le web 2.0 se caractérise par l'omniprésence du réseau. Résultante des interactions constantes des différents acteurs, le web 2.0 se présente comme un réseau constitué de nœuds incarnés tantôt par les sites, tantôt par les usagers, parfois par les régulateurs publics et privés. Chacun de ces nœuds se trouve doté d'une capacité d'énoncer ou d'imposer des règles aux autres interconnectés. Une telle capacité d'imposer des règles aux autres entités dans le réseau est tributaire de la capacité à générer un niveau plus ou moins élevé de risques auprès de ceux qui sont en interrelation.

Le web 2.0 soulève des questionnements quant aux cadres juridiques qui lui sont applicables car il est porteur de risques et enjeux qui paraissent inédits. Par la dissolution des repères et l'effacement des catégories, il soulève des enjeux qui sont fréquemment perçus comme un changement dans l'échelle des risques pourtant inhérents à la communication en ligne.

A. Le changement de l'échelle des risques

La normativité crée, accentue, réduit ou transfère les risques. Les risques découlant des normativités sont à ce titre des risques juridiques. Le web 2.0 n'est peut-être pas complètement nouveau, mais il paraît poser de façon plus dramatique les enjeux et risques inhérents aux environnements en ligne. Si les risques qu'il implique ne sont pas nécessairement nouveaux, ils paraissent démultipliés. Franklin Brousse explique que le web 2.0 :

« […] repositionne l'internaute au cœur du web. Il modifie donc les risques et responsabilités juridiques liées le plus souvent à l'exploitation des sites web. En contribuant grâce aux outils et aux technologies offertes par les nouveaux services web 2.0, à la création, l'organisation et le partage libre au sein d'une communauté de tous types de contenus (écrits, sonores, ou visuels), chaque internaute prend le statut d'auteur et/ou d'éditeur de contenus et doit assumer une nouvelle responsabilité liée à la

[10] Thomas Schultz, *Réguler le commerce électronique par la résolution des litiges en ligne*, Bruxelles, Bruylant, 2005, p. 151. Cet auteur envisage le réseau comme un « métamodèle de régulation ». Voy. également dans le même sens, Philippe Amblard, *Régulation de l'internet – L'élaboration des règles de conduite par le dialogue internormatif*, Bruxelles, Bruylant, 2004.

fois à ses propres créations et à l'usage qu'il fait de celles des autres »[11].

Le rôle accru de l'usager contribue à déplacer et à démultiplier les lieux où se manifestent des risques et enjeux dont plusieurs peuvent présenter des dimensions juridiques. En raison du rôle actif qu'il tient, l'usager lui-même devient un nœud de normativité dont doivent forcément tenir compte les autres acteurs. Les décisions que prend l'usager sont, plus que dans l'internet de première génération, susceptibles d'emporter des conséquences pour les tiers. Mais comme l'environnement du web 2.0 s'inscrit en dehors d'un modèle dans lequel une entité centrale assume les responsabilités, le cadre juridique se trouve caractérisé par un ensemble de risques répartis entre un nombre indéterminé d'acteurs de dimensions et de statuts différents.

Les risques ont aussi une échelle modifiée en raison des mutations quantitatives et qualitatives de la diffusion de l'information. Internet banalise la circulation de l'information : celle-ci peut aisément se trouver à être diffusée en dehors des cercles de circulation légitime ; d'où l'accroissement des risques[12]. Les environnements du web 2.0 contribuent à modifier les repères spatiaux et temporels qui permettent de délimiter les lieux de circulation légitime ou licite de l'information. Les multiples fonctions du web 2.0 donnent accès à des informations qui étaient, il y a peu de temps, tenues pour n'avoir vocation à circuler que dans des espaces restreints. Les balises conçues dans un monde dans lequel les réseaux prenaient moins de place sont prises en défaut[13].

Tous ces changements dans les dimensions des enjeux indiquent des modifications dans les niveaux de risques causés par la circulation de l'information dans le réseau. Ces dimensionnements nouveaux des risques induisent des mutations au niveau de la raison d'être des règles de droit. Ils peuvent également nécessiter des outils de régulation reflétant le caractère réseautique des processus de relais et de transferts des risques au sein du réseau.

Internet modifie l'échelle spatiale à partir de laquelle s'apprécient les risques. En dehors du monde en réseaux, l'accessibilité à une information exige des ressources qui peuvent être importantes. Sur Internet, on a l'impression que beaucoup d'informations sont à portée d'une requête de moteur de recherche[14]. Une telle facilité d'accès tend à banaliser l'information et accentue les risques de décontextualisation.

La persistance de l'information emporte que celle-ci traverse les espaces temporels dans lesquels elle était tenue pour légitime, il en résulte un décentrage temporel. Par exemple, une information peut être légitimement disponible à un ensemble « d'amis » dans un site de réseautage social. L'archivage et la disponibilité virtuellement permanente sur Internet peuvent conférer à ce type d'informations *a priori* anodines, une persistance et une diffusion allant au-delà de la communication au sein d'un cercle d'amis.

En plus, l'effacement des efforts à consacrer pour trouver l'information emporte la disparition de protections par défaut pour la plusieurs droits fondamentaux comme la réputation et

11 « Web 2.0 : un point complet sur les aspects juridiques », *Indexel*, http://www.indexel.net/1_6_4523__3_/9/33/1/ Web_2.0___un_point_complet_sur_les_aspects_juridiques.htm.

12 Karl D. Belgum, « Who leads at Half-time ? – Three Conflicting Visions of Internet Privacy Policy », *Rich. J.L. & Tech.*, 1999, 6, 1.

13 Frederick Schauer, « Internet Privacy and the Public-Private Distinction », *Jurimetrics*, 1998, 38, 555.

14 Daniel J. Solove, « Access and Aggregation : Public Records, Privacy and the Constitution », *Minn. L. Rev.*, 2002, 86, 1137-1218, p. 1139.

la vie privée. Les capacités d'agglomération d'information permettent la constitution de gisements d'informations sur les personnes qui peuvent du coup devenir disponibles pour des forces de police de même que devenir des enjeux pour des malfaiteurs.

B. Les principales catégories de risques et enjeux

La régulation du web 2.0 s'inscrit dans le tissu des impératifs de modulation et de gestion des risques. Ceux qui prennent part à des activités dans les environnements web 2.0 le font avec plus ou moins d'intensité selon qu'ils ont ou non conscience qu'ils auront à supporter plus ou moins de risques. Les configurations techniques, les modes de fonctionnement, les normes applicables et les sujets concernés par un environnement web 2.0 sont autant de facteurs qui sont susceptibles d'engendrer, accroître ou limiter les risques des acteurs impliqués.

Bien qu'il paraisse impossible d'énumérer dans l'abstrait l'ensemble des enjeux et risques que peut poser l'exploitation d'un site web possédant les caractéristiques associées au web 2.0, il est possible d'identifier les principales catégories d'enjeux et de risques que la plupart des acteurs voudront considérer afin de calibrer leurs décisions. De façon générique, il est possible de reconnaître que les environnements de web 2.0 impliquent des risques de comportement ; ils peuvent présenter des risques du fait de leur configuration technique ou ergonomique et il y a des risques de régulation. Chacun de ces risques peut être géré en créant ou en accentuant les risques associés à l'une ou l'autre de ces catégories.

1. Les risques de comportement

Il s'agit des risques découlant des comportements que peuvent adopter les internautes qui interagissent sur un site. Les pratiques qui sont susceptibles de mettre à mal les droits des personnes sont celles qui viennent le plus souvent à l'esprit.

Risques pour la réputation des personnes – Avec le web 2.0, il est facile de parler de soi et des autres et de conférer à de tels propos une diffusion pratiquement universelle. Or, les mécanismes qui assurent la protection du droit à la réputation des personnes tiennent en compte le contexte de la diffusion du propos et apprécient son caractère diffamatoire par rapport au sens qui est donné au propos, compte tenu de l'ensemble des circonstances de sa diffusion. C'est ainsi que l'on peut trouver licite un commentaire formulé en cercle restreint sur les faits et gestes d'une personne dans le cadre de l'exercice de ses fonctions. Mais le même commentaire porté à l'attention d'un tiers non concerné pourra avoir un caractère diffamatoire. Plusieurs environnements associés au web 2.0 comme les sites de réseautage sociaux procurent des facilités sans précédent de faire passer un propos de l'univers de l'intime à celui du public.

Risques pour la vie privée – Plusieurs applications du web 2.0 ont le potentiel de briser les lignes séparatrices entre ce qui est tenu pour être privé ou partagé uniquement dans un cercle limité et les informations disponibles à un plus large public. Par exemple, dans un site de réseautage social, il est possible de publier des renseignements nous concernant mais aussi des renseignements concernant nos contacts. De telles informations peuvent être dévoilées lors de la rédaction d'un commentaire. Nos contacts peuvent également mettre des renseignements nous concernant dans leurs propres sites personnels.

Les informations personnelles dévoilées sur un site de réseautage social peuvent être utilisées de plusieurs façons. Par exemple, des entreprises peuvent se servir des informations

pour sonder le marché, des prédateurs sexuels peuvent trouver des victimes potentielles en recherchant des profils vulnérables ou des employeurs éventuels peuvent surfer sur les espaces personnels pour en apprendre plus sur des candidats avant de les engager[15].

L'accumulation et l'agglomération de données sur les personnes par les sites à contenu généré par les usagers et d'autres fonctions disponibles sur Internet emportent la constitution de répertoires importants d'information potentiellement disponibles aux activités de surveillance de toutes sortes. C'est un risque qui paraît inhérent aux modes de fonctionnement actuel d'Internet.

Risques pour le droit à l'image. – Les enjeux relatifs à la diffusion des images concernent évidemment les droits de propriété intellectuelle mais ils mettent aussi en jeu le droit des personnes de s'opposer à la diffusion de leur image sans leur consentement ou en dehors de circonstances où la diffusion serait justifiée par l'intérêt public ou par l'intérêt que pourraient avoir certains proches.

Risques pour la propriété intellectuelle. – La banalisation des applications permettant aux usagers de publier des contenus sur des sites web présente des risques au regard de la propriété intellectuelle : des usagers peuvent reproduire une œuvre sans autorisation puis la publier sans autorisation sur un site. Les principes juridiques de la propriété intellectuelle qui sont interpellés par ce type d'activités ne sont pas nouveaux. Mais l'ampleur du phénomène, la facilité avec laquelle il est désormais possible de diffuser des contenus pose des défis majeurs. Les risques de non-conformité aux droits de propriété intellectuelle paraissent accrus[16].

Risques de diffusion de contenus contraires aux lois. – Plus on multiplie les lieux de décision en matière de publication sur le réseau, plus les risques de publication de contenus contraires aux lois s'accroissent.

Dans un contexte de site à contenu généré par les usagers, l'ensemble de ces risques découlent principalement des comportements adoptés par les internautes. On se retrouve donc avec une multitude de centres de décision tous en mesure de diffuser des informations à partir de leurs perspectives. Ce rôle accru de l'amateur dans des situations autrefois dominées par des professionnels tend à brouiller les frontières entre producteur et consommateur, ce qui dramatise la question des statuts et responsabilités respectives des uns et des autres[17].

Le nombre infini de situations possibles et la difficulté de distinguer celles qui constituent des violations des lois incite à envisager ce genre de situations juridiques dans lesquelles les usagers tiennent une place si importante selon une approche de risques juridiques. Dans un univers où le réseau paraît omniprésent dans toutes les dimensions de l'activité humaine, il est de moins en moins réaliste de conférer un statut spécifique à chaque usager. Les comportements de ces derniers peuvent être tributaires d'une multitude de facteurs parfois très volatils qui peuvent affecter la qualification juridique de leurs gestes. C'est donc en évaluant les risques qu'il devient possible de rétablir une certaine prévisibilité juridique ou normative.

15 Susan B. Barnes, « A Privacy Paradox : Social Networking in the United States », *First Monday*, http://www.firstmonday.org/issues/issue11_9/barnes/index.html, page consultée le 27 juin 2008.

16 Lisa Veasman, « " Piggy Backing " on the Web 2.0 Internet Copyright Liability and Web 2.0 Mashups », *COMM/ENT*, 2008, 30, 311-337.

17 Pierre-Yves Gautier, « Le contenu généré par l'utilisateur », *Legicom*, n° 41, 2008/1, pp. 1-7.

2. Les risques de configuration

Les environnements du web 2.0 emportent certains risques qui ne découlent pas exclusivement de la volonté ou du comportement du maître de site ou de l'usager. La façon dont sont configurés les environnements peut faciliter l'accomplissement de gestes qui peuvent se révéler illicites. Par exemple, la facilité technique avec laquelle il est possible d'introduire un contenu sur un blogue ou sur un site de partage de documents audio ou vidéo est en elle-même génératrice de risques. Cette normativité par défaut facilite des gestes qui peuvent aisément contrevenir à d'autres règles, telles que celles relatives à la propriété intellectuelle.

Ces lieux diversifiés sur Internet de même que la puissance de certaines fonctions de traitement des informations mènent au constat que l'environnement cyberspatial induit des risques accrus qu'il importe de gérer au sein du réseau. Par exemple, on a fréquemment signalé l'importance des effets d'agrégation et des capacités des moteurs de recherche[18]. L'information – même de caractère public – peut plus facilement être trouvée puis agglomérée de manière à déduire des informations qui elles relèvent de la vie privée. De ce fait, les risques pour la vie privée changent d'échelle sur Internet. Un tel phénomène suppose une gestion des risques qui s'opère forcément en réseau.

La configuration même d'Internet, qui ignore les frontières territoriales, engendre des risques. Par exemple, plusieurs fonctions du web 2.0 permettent l'utilisation hors contexte de l'information. La conception des sites de réseautage personnel procède d'une reconnaissance qu'il y a, pour chaque personne, des lieux différenciés au sein desquels le statut des informations ne sera pas forcément le même. Par exemple, il pourra être fautif de reprendre un commentaire formulé dans l'intimité et le diffuser à un cercle plus vaste.

Internet n'est pas un environnement univoque : on y trouve des lieux de toutes sortes. Certains comportent plus de risques pour la vie privée de personnes qui les fréquentent. Par exemple, les sites de réseautage social sont configurés de façon à faciliter la rencontre et la mise en relation de personnes via leurs réseaux sociaux. Des sites tels *MySpace* et *LinkedIn* proposent un service en ligne qui permet de mettre en relation tous ces gens. De tels sites peuvent servir à agrandir son cercle d'amis, à créer des relations professionnelles, à faire connaître des groupes musicaux, mettre en relation avec des gens qui partagent les mêmes intérêts, à retrouver des anciens camarades de classe, etc. Il suffit de choisir le site qui répond à nos besoins et de s'y inscrire pour être potentiellement relié à des millions de gens.

Le formulaire d'inscription permet en général de créer un profil de base, qui peut contenir le nom de l'usager, sa ville de résidence ainsi que son occupation. Par la suite, l'usager peut compléter les informations qui le concernent de façon plus détaillée, en ajoutant sa photographie, son curriculum vitae ou encore ses centres d'intérêts. Tous ces renseignements seront regroupés dans un espace personnel.

Pour pouvoir profiter de la mise en relation avec d'autres personnes, les usagers peuvent ajouter des contacts à leur carnet d'adresses. Pour ce faire, ils peuvent rechercher des individus qui sont déjà membres du site et leur proposer d'entrer en relation. L'usager peut prendre contact avec quelqu'un qui n'est pas membre en l'invitant à s'inscrire et à prendre contact. Certains sites vont offrir d'importer la liste des contacts d'une adresse de courriel déjà existante dans le but d'envoyer à toutes ces personnes des courriels d'invitation. Si les

[18] Daniel J. Solove, « Access and Aggregation : Public Records, Privacy and the Constitution », *Minn. L. Rev.*, 2002, 86, 1137-1218.

personnes concernées se joignent au site, elles apporteront à leur tour leurs contacts et le réseau grandit de cette façon.

On peut enfin signaler la volatilité des contenus circulant dans plusieurs environnements du web 2.0. Les contenus peuvent être modifiés par un usager et recombinés à l'infini. Les usagers ont la possibilité d'intervenir sur les contenus et d'y apporter des modifications. Le contenu ne peut pas être tenu pour définitif au sens où on avait l'habitude de le postuler pour les publications éditées. Le processus d'édition se présente désormais comme en un mouvement continu dans lequel une pluralité d'intervenants de statuts différents ont vocation à intervenir.

3. Les risques et enjeux de régulation

La régulation elle-même – qu'elle résulte des configurations techniques, de l'activité des acteurs eux-mêmes ou des règles mises en place par les autorités étatiques – est génératrice de risques. Les règles ont évidemment vocation à être observées. Mais en pratique, les acteurs ne vont pas se conformer à des règles qui vont à l'encontre de leurs intérêts s'ils perçoivent que le risque de devoir subir des conséquences adverses pour leur non-conformité est faible.

La superposition des rôles et des catégories tels que définis dans la réglementation applicable dans les différents territoires accroît le risque. Jan Trzaskowski observe que :

« In the absence of globally accepted standards for geographical delimitation of content on the Internet, the infringement of foreign law is a risk which businesses inevitable will run when carrying out electronic commerce »[19].

Dans les environnements web 2.0, les différents acteurs occupent des positions et tiennent des rôles qui changent. Cette volatilité des rôles tenus par les acteurs peut rendre problématique la détermination des responsabilités. Il en découle une difficulté à identifier qui « répond » des contenus et activités. Ce phénomène de déficit d'*accountability* tend à accroître la relative incertitude quant à l'identité de ceux qui auront à répondre d'un fait dommageable ou illicite.

Les usages et les pratiques en réseau engendrent également des régulations qui peuvent être génératrices de risques pour certains usagers. Mettre en ligne un site dans lequel il est loisible à n'importe quel usager d'introduire des propos ou images portant sur une autre personne constitue assurément une régulation par défaut qui engendre des risques pour les tiers éventuellement concernés par les documents mis en ligne.

Les usagers agissent en réseau. Ils interagissent et du coup développent des solutions aux problèmes rencontrés et des façons de faire afin de minimiser leurs risques. Dans plusieurs situations, ils vont mettre en place un ensemble de règles qui encadrent le déroulement des activités. En somme, les normes elles-mêmes sont en partie produite dans le cadre des interactions en réseau[20]. Mais une fois établies, ces normes engendrent forcément des risques pour les autres acteurs.

II. UNE RÉGULATION EN RÉSEAU DE GESTION DE RISQUES

Une fois reconnu, le risque emporte des obligations de précautions ; il doit être géré. Le risque juridique découle en effet des situations où la

[19] Jan Trzaskowski, « Legal Risk Management in a Global Electronic Marketplace », *Scandinavian Studies in Law,* 2006, 49, 319-337, p. 320.

[20] David D. Johnson, Susan P. Crawford et John G. Palfrey jr, « The Accountable Internet : Peer Production of Internet Governance », *Virginia Journal of Law & Technology*, 2004, 9, 1-32.

violation des droits d'autrui est susceptible de se produire. Même s'ils sont différents, il y a une étroite proximité entre le risque technologique et le risque juridique : lorsque le risque technologique est avéré, il naît presque toujours une obligation d'en tenir compte et de se comporter de façon conséquente. Le risque juridique peut aussi découler de la possible non-conformité à une loi ou à une autre sorte d'obligation également applicable comme un contrat. Le risque juridique, en toute hypothèse, résulte des situations dans lesquelles la responsabilité d'une personne peut être mise en cause.

Dans la conception traditionnelle, le risque juridique est une notion inusitée. Les juristes voient le risque dans tous les phénomènes qu'ils ont à examiner mais le fait qu'une sanction puisse découler de la transgression d'une règle n'est pas envisagé comme un risque en tant que tel par le juriste[21]. Par contre, dans une approche de gestion, le risque juridique apparaît plus clairement. Le gestionnaire envisage les règles de droit comme étant porteuses de risques. Trzaskowski remarque que « Legal risk management is not a well-established or well-defined concept, which like risk management in general is of a proactive nature »[22]. Par contre, il paraît clair que les juristes appelés à conseiller les décideurs sur Internet procèdent à une analyse de risques juridiques[23].

Dans un environnement en réseau, le risque juridique se présente comme comportant deux composantes : une ou des normes et un événement. C'est de la conjonction de la norme et de l'événement que découle le risque juridique. La norme peut être énoncée dans une loi ou un règlement mais elle peut aussi découler d'un contrat ou d'une configuration technique. Le propre de la norme, c'est qu'elle est susceptible d'être sanctionnée, c'est-à-dire qu'une conséquence adverse est susceptible de découler de la transgression. La transgression survient lors d'un événement. Il peut s'agir d'un acte affirmatif ou d'une omission qui a lieu dans un contexte concret. L'événement doit nécessairement être anticipé ou à tout le moins, sa survenance possible détectée. Le dommage qui peut découler de cet événement doit être évalué.

Pour donner lieu à un comportement conforme à celui qui est recherché, une norme ou un processus de régulation doit être perçu comme générant plus de risques que les bénéfices qui peuvent résulter de sa transgression. Sur Internet, les acteurs font nécessairement une évaluation des risques juridiques. Comment expliquer autrement le fait qu'en dépit du caractère universel du réseau, et donc de la certitude qu'un site web non restreint aux utilisateurs possédant le droit d'y accéder sera accessible dans tous les pays, aucun maître de site ne fait le choix de se conformer à la totalité des législations nationales possiblement applicables ? En fait, sur Internet, la régulation qui est effective est celle qui engendre chez les acteurs, un seuil minimal de perception de risques pouvant résulter de comportements qui y dérogent.

Un État ou un autre régulateur peut agir afin d'augmenter les risques de certains comportements ou activités ou réduire les risques associés à une conduite saine. Par exemple, lorsque l'État adopte une loi sévère contre certaines

21 Franck Verdun, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, p. 20.

22 Jan Trzaskowski, « Legal Risk Management in a Global Electronic Marketplace », *Scandinavian Studies in Law,* 2006, 49, 319-337, p. 321.

23 Rachel Burnt, « Legal risk mangement for the IT industry », *Computer Law & Security Report*, 2005, 21, 61-67 ; David N. Weiskopf, « The Risks of Copyright Infringement on the Internet : A Practitioner's Guide », *University of San Francisco L.Rev*., 1998, 33, 1-58 ; Keith J. Epstein et Bill Tancer, « Enforcement of Use Limitations by Internet Services Providers : "How to Stop that Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber" », *COMM/ENT*, 1997, 19, 661-693 ; Karl Belgum and Hilary Rowen, « Insurance for Internet-Related Risks », *Journal of Internet Law*, January 2000, pp. 11-16.

pratiques, cela accroît les risques associés à celles-ci. À l'égard des usagers qui se livrent à des activités légitimes, l'État peut baliser, voire limiter les risques. Mais alors, les risques inhérents aux activités concernées sont forcément supportés par d'autres.

La régulation du web 2.0 s'envisage comme un ensemble de mesures conçues de manière à se renforcer les unes et les autres afin de limiter les risques des internautes qui s'adonnent à des activités licites. La normativité se déploie en réseau : imposant des règles aux acteurs et incitant ces derniers à en relayer les exigences à tous ceux à l'égard desquels ils exercent une influence.

Dans une logique de risques, les mesures étatiques seront plus efficaces si elles sont assorties de politiques dynamiques de surveillance et de poursuites puisque ce sont des conditions nécessaires pour que les acteurs perçoivent un risque à y contrevenir. Il s'agit alors de faire en sorte que les risques découlant de ces lois soient relayés vers tous ceux qui mènent des activités illicites.

Dans un réseau, chacun de ceux qui sont en mesure d'imposer leur volonté disposent d'une capacité d'accroître les risques des autres. Ainsi, un État peut imposer des devoirs aux citoyens qui se trouvent sur son territoire. Ces derniers auront alors à gérer leurs risques découlant de ces obligations. Ils chercheront à s'assurer que leurs partenaires agissent en conformité avec les obligations auxquelles ils sont eux-mêmes tenus et à l'égard desquelles leur responsabilité peut se trouver engagée. Ils vont donc relayer, par contrat ou autrement, les obligations et les risques afférents à ces exigences.

La régulation d'Internet résulte des équilibres toujours provisoires entre les risques et les précautions. L'ensemble des acteurs cherche à minimiser leurs risques qui relèvent de situations sur lesquelles ils sont effectivement en mesure d'avoir une prise. La régulation des activités associées au web 2.0 doit viser à accroître les risques associés aux comportements qui mettent les autres à risque et diminuer les risques de ceux qui ont des comportements prudents. La normativité interviendra habituellement lorsqu'il est jugé opportun de rééquilibrer les risques respectifs des participants à une activité.

A. Les nœuds de normativité

Dans un réseau, les normativités sont pensées et exprimées dans divers lieux qui sont autant de nœuds de normativité. Sur un territoire spécifique, le droit étatique constitue un nœud majeur de normativité : l'ensemble de ceux qui sont situés sur le territoire n'ont pratiquement pas le loisir d'ignorer la loi. Les risques de ne pas s'y conformer sont habituellement élevés. Ils pourront toutefois être tentés de courir le risque de se trouver en situation de non-conformité avec une ou plusieurs lois s'ils ont le sentiment que ces lois sont peu appliquées ou que la volonté de les appliquer n'est pas apparente. On voit bien ici à quel point le cyberespace est un environnement dans lequel l'usager exerce une grande maîtrise. S'il a l'impression qu'il court peu de risques de se voir inquiété pour avoir ignoré les lois, la possibilité s'accroît qu'il soit tenté de prendre le risque de se livrer à une activité prohibée ou dommageable.

Mais dans un univers réseautique comme le web 2.0, les nœuds de normativité sont multiples et la capacité de ceux-ci à engendrer assez de risques pour générer des normes effectives paraît être en fluctuation continue.

1. Les lois étatiques

Les lois étatiques pénales et civiles procurent une partie importante des balises aux pratiques des internautes. Pour la plupart des acteurs du cyberespace, la responsabilité au

regard du droit d'un État ou de plusieurs se présente comme un ensemble de risques à gérer. Les personnes et les entreprises doivent s'assurer que leurs pratiques sont conformes aux exigences des dispositions des lois susceptibles de trouver application et d'engager leur responsabilité. Ils chercheront à maîtriser les risques découlant de leurs activités en prenant les précautions susceptibles de les prémunir contre les effets adverses de l'application des lois nationales. Lorsqu'il existe des règles énoncées dans des textes de loi, les acteurs ont tendance à ajuster leurs pratiques de façon à limiter leurs risques de se retrouver en contravention avec celle-ci.

Même si elle peut se révéler insuffisante en elle-même, la loi est porteuse d'un effet symbolique : sa seule existence est comprise comme un message par la plupart des acteurs. Une loi qui est effectivement appliquée indique aux acteurs qu'il est préférable d'adopter un comportement exempt de pratiques nuisibles.

Pour engendrer des résultats optimaux, la législation doit viser l'ensemble des situations pouvant être associées à des pratiques liées au web 2.0. En plus, dans une logique de réseau, la normativité effective est fréquemment celle qui est énoncée dans les législations nationales et supra-nationales influentes. La prise en compte des législations nationales et supranationales influentes est nécessaire à la fois dans la conception des législations nationales et dans l'arrimage qui peut être envisagée avec les lois de juridictions des États exerçant plus d'influence sur le réseau.

Des lois relevant des divers champs d'activités sont susceptibles d'être concernées. La législation sur la concurrence, notamment les dispositions ayant trait à la publicité trompeuse et aux fausses représentations de même que la législation sur la protection des consommateurs peuvent s'appliquer à plusieurs comportements caractéristiques du web 2.0. Mais plusieurs activités se déroulant dans les environnements associés au web 2.0 sont susceptibles de constituer des fautes civiles. La perspective de devoir éventuellement répondre de ses actes à l'occasion d'un recours en responsabilité civile peut constituer un risque significatif pour plusieurs acteurs du web 2.0. C'est d'ailleurs en grande partie au moyen de règles qui balisent les recours en responsabilité pour certaines catégories d'acteurs que les législateurs de plusieurs juridictions ont modulé les risques associés à la diffusion d'information sur Internet.

Par exemple en droit américain, l'article 230 du Communications Decency Act[24] (CDA), prévoit une immunité au profit du « bon samaritain »[25] à l'égard des gestes ou omissions posées à l'égard d'un contenu. Le Communications Decency Act protège les services informatiques interactifs de l'imputation d'une responsabilité, et ce, même après que ces services aient été informés de l'existence d'une publication prétendument diffamatoire ou menaçante[26]. Seul un fournisseur ou un utilisateur d'un service informatique interactif peut profiter de la décharge de responsabilité accordée par le CDA[27]. L'article 230(f)(2) du CDA précise la signification de l'expression « service informatique interactif » : il s'agit de tout service d'information, système ou fournisseur d'un logiciel d'accès qui procure ou permet l'accès à un serveur informatique aux multiples utilisateurs, incluant spécifiquement un service ou un système qui fournit l'accès à Internet et de tels systèmes gérés par les bibliothèques ou

[24] Communications Decency Act, 47 U.S.C. § 230 (1996)

[25] Communications Decency Act, 47 U.S.C. § 230(c) (1996). « Protection for « Good Samaritan » blocking and screening of offensive material ».

[26] *Zeran* v. *America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).

[27] Communications Decency Act, 47 U.S.C. § 230(c)(1) (1996).

les institutions d'enseignement ou des services qu'elles offrent.

Les principaux modèles de sites à contenu générés par l'utilisateur ont pu se développer aux États-Unis grâce à l'immunité conférée au fournisseur de service interactif au regard des contenus fournis par les tiers fournisseurs de contenus. Il revient aux États de déterminer le niveau de risque qui paraît optimal afin d'encourager le développement de services en ligne vis-à-vis la protection des autres intérêts comme la réputation, la vie privée ou la propriété intellectuelle.

2. Les configurations technologiques

Ce qui paraît caractéristique de l'environnement cyberspatial, c'est que la normativité effectivement agissante est soit celle qui est d'application immédiate, comme celle qui résulte des configurations techniques, soit celle qui engendre des perceptions de risques auprès des acteurs. Internet est un environnement construit par la technique. Les risques qu'il comporte sont nécessairement le résultat de décisions normatives comme celles qui donnent lieu à des configurations techniques[28]. Ce phénomène est particulièrement visible dans les environnements du web 2.0.

Grimmelman observe que les configurations logicielles sont automatiques ; elles sont d'application immédiate et possèdent des caractéristiques de flexibilité dans la mesure où les concepteurs de logiciels peuvent implanter tout système « they can imagine and describe precisely »[29]. Mais la régulation juridique possède une plus grande flexibilité. En outre, les configurations logicielles régulent sans transparence. Grimmelman écrit que :

« Frequently, those regulated by software may have no reasonable way to determine the overall shape of the line between prohibited and permitted behavior. The plasticity of software and its automated operation also bedevil attemps to have software explain itself. Even experts may not understand why a program acts as it does ».[30]

Dans le web 2.0, l'architecture technique détermine les conditions d'accès et les conditions d'utilisation des ressources mises à la disposition des internautes. Par exemple, les conditions d'utilisation de MySpace prévoient que le site « MySpace assure les fonctions techniques nécessaires pour offrir les Services MySpace, y compris, mais sans toutefois s'y limiter, la conversion de code et/ou le reformatage du Contenu pour permettre son utilisation sur l'ensemble des Services MySpace »[31].

En fin de compte, le caractère fondamentalement construit par la technique des environnements du web 2.0 porte à nuancer la conception que l'on tend à s'en faire d'un lieu dans lequel les usagers seraient maîtres d'y insérer les contenus selon leur seul bon vouloir. Cette grande latitude laissée à l'usager est le résultat de choix techniques et de configuration. On peut même se demander si ce type de choix technique aurait été envisageable dans un environnement juridique moins favorable aux exploitants de services en ligne que celui qui prévaut en droit américain.

28 Joel R. Reidenberg, « *Lex Informatica* », *Texas Law Review*, 1998, 76, 553-593 ; Lawrence Lessig, *Code and Other Laws of Cyberespace*, Basic Books. 1999.

29 James Grimmelman, « Regulation by Software », *Yale L.J.*, 2005, 114, 1719, p. 1723.

30 James Grimmelman, « Regulation by Software », *Yale L.J.*, 2005, 114, 1719, p. 1723.

31 Conditions d'utilisation de MySpace.com, clause 6.6, http://www.myspace.com/index.cfm ?fuseaction =misc.terms.

3. Les pratiques des internautes

Les pratiques des internautes font partie des cadres normatifs d'Internet. Dans l'univers du web 2.0, l'implication des usagers prend plus de place, l'importance des pratiques tend à s'accroître.

Edward Lee observe que l'émergence du contenu produit par les utilisateurs remet en question les conceptions traditionnelles de l'application des lois[32]. Prenant exemple sur les pratiques des internautes au sujet des œuvres protégées par le droit d'auteur, il soutient que l'application formaliste de la loi passe à côté de la réalité. Les lois sur la propriété intellectuelle comportent des zones grises et des silences qui ne sont que très occasionnellement comblés par les décisions des tribunaux. Les pratiques des acteurs contribuent à combler les silences et ambiguïtés des lois. Devant ce qui paraît ressembler à des pratiques contraires aux lois, tout se passe comme si les titulaires de droits évaluent les avantages et inconvénients de saisir les tribunaux. Pour leur part, les usagers adoptent des pratiques qui reflètent ce qu'ils perçoivent comme des risques raisonnables, notamment d'être poursuivis.

On convient généralement de la nécessité de s'assurer de l'existence et de la diffusion appropriée de ce que les acteurs identifient comme étant de « bonnes pratiques » ou pratiques exemplaires afin de réduire les risques du web 2.0[33].

Même si les usages et pratiques dans un champ d'activité donné sont souvent pris en compte et ainsi intégrés au droit étatique, l'intérêt de ce type de norme réside dans sa capacité à organiser de façon autonome les comportements et les transactions des membres d'une communauté. Le respect des usages et pratiques est, dans de telles circonstances, la condition essentielle de l'adhésion d'un participant à une communauté donnée. C'est à ces titres que les « bonnes pratiques » constituent une source de réglementation qui viendra souvent compléter les exigences plus formelles du droit étatique. En particulier, les « bonnes pratiques » sont souvent orientées vers les solutions afin de limiter les risques pouvant résulter de certains comportements.

4. Les normes énoncées dans les forums internationaux

Les forums internationaux paraissent constituer le lieu le plus efficace de l'élaboration de métanormes, celles qui sont exprimées sous forme de principes destinés à être relayés dans les législations nationales et dans les autres lieux d'élaboration de normativité. Tant les instances internationales conventionnelles que les associations non gouvernementales se présentent comme des lieux d'élaboration de méta-normes. Ce sont des lieux où l'on travaille à l'identification des dénominateurs communs.

C'est souvent dans les forums internationaux que sont établies les balises à caractère universel qui délimitent le licite et l'illicite. Afin de demeurer pertinentes face au rythme accéléré de l'évolution des pratiques, ces instances doivent de plus en plus fonctionner en réseaux.

De plus, étant donné la nécessité de tenir compte d'un spectre très large de contextes dans lesquels la normativité aura à trouver application, les délibérations internationales donnent lieu à l'élaboration de principes se présentant comme ayant vocation à être

[32] Eward Lee « Warming Up to User-Generated Content », *University of Illinois L. Rev.*, 2008, n° 5, http:// papers.ssrn.com/sol3/papers.cfm ?abstract_id=1116671.

[33] Adam Thierer, *The MySpace-AG Agreement : A Model Code of Conduct for Social Networking ?*, Washington D.C., The Progress & Freedom Foundation, janvier 2008.

relayés dans les ordres normatifs des États et des autres entités exerçant de l'influence. Les lois nationales tendent à trouver application selon une logique de subsidiarité. Elles relaient dans les contextes culturels spécifiques, les principes abstraits reconnus dans les forums globaux. C'est pourquoi il devient possible de considérer que l'efficacité du droit étatique tient à sa capacité d'assurer effectivement le relais des valeurs et principes fondamentaux tenus pour légitimes.

B. Le relais des normativités

Les processus par lesquels on obtient l'application effective[34] des règles dans un univers comme Internet sont une composante majeure de la normativité en réseaux. Les relais sont les différents moyens par lesquels les acteurs reçoivent et appliquent effectivement les normes perçues par eux comme relevantes ou obligatoires.

Sur Internet, les règles que les usagers et autres acteurs considèrent relevantes ou obligatoires sont celles qui représentent des risques. Par exemple, une entreprise qui décide d'être active sur Internet en mettant en place un site de transaction va nécessairement évaluer les lois et autres normes qu'elle doit suivre afin de minimiser ses risques. Elle considérera relevantes, les règles qui sont effectivement susceptibles de trouver application à l'égard des activités qu'elle mène. Ainsi, un restaurant proposant la livraison à domicile de repas dans un quartier de Bruxelles pourra s'estimer justifié d'attacher peu d'importance aux lois en vigueur au Népal !

C'est ce phénomène qui explique que l'on ne se sent pas tenu d'être conforme aux exigences de toutes les lois de tous les pays de la planète lorsqu'on mène une activité sur Internet. En fait, on va considérer nécessaire d'être conforme uniquement aux lois qui sont susceptibles de trouver effectivement application à notre activité. Autrement dit, on s'assure de respecter les lois et autres normes qui peuvent effectivement nous être appliquées de façon significative. C'est généralement en faisant une évaluation des risques associés à la non-conformité avec les lois de pays avec lesquels on entretient ou prévoit entretenir des liens étroits que l'on identifie à quelles lois nationales il importe de se conformer lors de la réalisation d'une activité sur Internet. Par exemple, une entreprise située au Québec et envisageant de commercer aux États-Unis et en Europe ne se sentira pas obligée de se conformer aux lois du Népal même si son site est tout à fait susceptible d'être reçu sur le territoire népalais. À l'inverse, elle pourra trouver nécessaire de s'assurer d'être conforme aux lois québécoises, américaines et européennes.

Au niveau de l'activité de chacun des acteurs ou usagers d'Internet, la gestion adéquate des risques suppose souvent d'anticiper les conflits et d'identifier de façon contextuée, comment seront relayées les exigences issues du droit ou des normativités qui, compte tenu des activités effectivement accomplies, risquent de trouver pratiquement application.

Par exemple, un exploitant de site devra se donner une politique afin de déterminer les conduites à tenir à l'égard des différents aspects du fonctionnement de l'environnement en ligne. Pour ce faire, il devra tenir compte de ce qui est tenu pour illicite dans le territoire dans lequel se trouvent ses infrastructures ou les lieux virtuels sur lesquels il est en mesure d'exercer une activité significative. Pour évaluer les mesures à prendre, il aura forcément à

[34] On entend par effectivité, un degré suffisant de réalisation, dans les pratiques sociales, des règles énoncées. Voy. sur cette notion : André-Jean Arnaud (dir.) *Dictionnaire encyclopédique de théorie et de sociologie du droit*, 2e éd., Paris, L.G.D.J., 1993, p. 217.

analyser les situations qui sont susceptibles d'engager sa responsabilité. Avec le web 2.0, ce type de démarche doit être poussé encore plus loin puisque les usagers disposent d'une certaine capacité de générer des risques pour les autres usagers ou pour l'entité qui organise un site.

Les relais rendent compte des processus de dialogue qui existent entre les divers pôles de normativité et entre les acteurs. Ces derniers ont forcément à prendre acte et à s'assurer qu'ils sont en conformité avec les règles engendrant des risques pour eux. Pour cela, ils devront les relayer à leurs partenaires et en combler les interstices afin d'en assurer une application concrète et effective.

1. La régulation pratiquée dans les sites

À l'instar de plusieurs environnements en ligne, les sites associés au web 2.0 pratiquent une régulation des contenus et des comportements des usagers. Ces processus internes à chacun des sites permettent, avec la participation des usagers ou seulement au moyen d'interventions sous l'autorité du maître du site, d'identifier et de résoudre les possibles enjeux et risques découlant de la non-conformité aux exigences des règles de droit ou qui contreviennent à d'autres normes. Par ces mécanismes, se relaient une bonne part des règles qui sont considérées comme impératives par les acteurs aux divers niveaux des environnements du web 2.0.

a. La surveillance par le site lui-même

Les sites web 2.0 sont souvent surveillés par des modérateurs, qui se chargeront de vérifier le contenu proposé par les usagers avant ou après sa mise en ligne. Un site Internet peut employer ces modérateurs ou alors il peut lancer un appel au public pour recruter des modérateurs bénévoles, comme le fait par exemple le site d'évaluation de personnes HOTorNOT[35].

La modération peut se faire avant ou après la mise en ligne du matériel. Lorsqu'elle est faite *a priori*, cela implique généralement que tout le contenu est vérifié avant d'être publié sur le site[36]. Les personnes naviguant sur les sites modérés *a priori* ont donc moins de risque d'être exposées involontairement à du matériel inapproprié, étant donné que toutes les contributions des usagers ont été jugées appropriées par les modérateurs pour qu'elles puissent se retrouver en ligne. La modération *a posteriori* consiste à permettre aux usagers de contribuer au site sans restriction[37]. Les modérateurs vont généralement se fonder sur les plaintes émanant des usagers pour cibler le contenu à surveiller. Ils peuvent également vérifier le site de façon aléatoire.

b. La surveillance par les usagers du site

Certains sites web 2.0 ont développé des méthodes de surveillance dans lesquelles l'usager joue un rôle majeur. Cette façon de faire reflète la difficulté pour un site contenant des millions de pages de contrôler l'ensemble de son contenu. La surveillance par les usagers permet de profiter des efforts d'un nombre indéterminé d'usagers qui portent un regard sur les contributions qui pourraient être inappropriées.

L'évaluation du contenu, ou *rating* par les usagers permet de gérer les risques pouvant

35 Voy. http://mod.hotornot.com/.

36 Le site Amazon.fr (http://www.amazon.fr/) est un exemple de site Internet où le contenu est soumis à une modération *a priori*. Tous les commentaires soumis par les usagers du site ne sont pas mis en ligne immédiatement. Le site se réserve un délai de cinq à sept jours avant la publication, pour se permettre de vérifier les commentaires avant leur publication.

37 Par exemple, le site RateMyProfessors (http://www.ratemyprofessors.com/) utilise la modération *a posteriori*.

découler de l'exploitation d'un site web 2.0. Cette surveillance s'effectue par les visiteurs du site, qui notent le contenu écouté ou lu selon une échelle qui est généralement de 0 à 5[38]. En principe, le contenu de mauvais goût ou de mauvaise qualité sera sanctionné par une mauvaise note. Mais les usagers du site n'ont pas tous les mêmes goûts. Certaines personnes peuvent alors bien noter un contenu que d'autres trouvent répugnant. Elles peuvent également attribuer une mauvaise note à ce que d'autres personnes considèrent comme étant un chef d'œuvre. Une telle approche repose sur l'hypothèse que les visiteurs ne seront pas portés à visionner des vidéos ou lire des articles qui ne sont pas bien notés.

Le signalement du contenu inapproprié, ou *flagging*, est l'une des méthodes les plus utilisées par les sites web 2.0 pour inciter les usagers à dénoncer le matériel qui pourrait être offensant, insultant, menaçant, ou autrement considéré comme illicite. Cette méthode consiste à insérer, avec chaque contribution des usagers, un lien permettant de dénoncer le contenu s'il est inapproprié[39]. Lorsqu'une personne visite un site web 2.0 et qu'elle se heurte à de la pornographie juvénile, par exemple, il suffit de cliquer sur ce lien, qui enverra automatiquement un avertissement aux administrateurs du site disant que du contenu inapproprié a été trouvé à tel endroit. Certains sites Internet vont inviter tous leurs visiteurs, membres ou non, à signaler le contenu inapproprié, d'autres sites vont permettre seulement à leurs membres de le faire[40].

Pour éviter la possible aggravation des dommages découlant d'un contenu offensant, certains sites vont masquer automatiquement la contribution qui a été dénoncée jusqu'à ce que la décision de la retirer ou non soit prise[41].

La méthode du signalement permet de compter sur un nombre considérable de surveillants du site. En effet, il est difficile de penser qu'un nombre restreint de modérateurs puissent surveiller à eux seuls tout un site web 2.0 contenant des millions de contributions des usagers. En comptant sur les visiteurs pour contrôler le site, il y a donc un plus grand bassin de personnes qui surveillent. Evidemment, les usagers doivent prendre le temps de dénoncer le contenu inapproprié sinon la surveillance sera inefficace.

c. Les mécanismes de règlement des différends

Plusieurs sites web 2.0 offrent aux utilisateurs des mécanismes dédiés de règlement des conflits. Ces modes de règlement des conflits peuvent aller de la simple dénonciation d'un contenu inapproprié, qui sera examiné par un modérateur bénévole ou rémunéré par le site, jusqu'à des mécanismes élaborés d'arbitrage des différends. Les sites eBay[42] (pour la partie du site qui propose d'évaluer les commerçants)

38 Le site YouTube (http://www.youtube.com/), par exemple, permet aux visiteurs d'attribuer jusqu'à cinq étoiles sur cinq à un contenu publié.

39 Le site YouTube (http://www.youtube.com/) est un exemple de site qui met à la disposition des visiteurs un moyen de dénoncer facilement le contenu inapproprié. Chaque vidéo ajoutée au site est accompagné d'un lien nommé « Flag as Inappropriate », qui permet de signaler une vidéo offensante.

40 Voy., par exemple, le site YouTube (http://www.youtube.com/), où il faut être membre pour pouvoir dénoncer une vidéo.

41 Par exemple, lorsque l'on fait une plainte concernant une évaluation sur le site Ratemyprofessors (http://www.ratemyprofessors.com/), l'évaluation litigieuse sera automatiquement masquée et remplacée par la mention « (Rating under review) » jusqu'à ce que le commentaire soit approuvé ou non.

42 « Resolving Feedback Dispute », *in* eBay, http://pages.ebay.com/help/feedback/feedback-disputes.html (page consultée le 27 juin 2008).

et Wikipedia[43] (pour ce qui est de la version anglophone) présentent des mécanismes complets de règlement des différends.

Le contrôle du contenu dénoncé. – Les visiteurs des pages web 2.0 sont souvent invités à dénoncer le contenu qu'ils jugent inapproprié par des mécanismes que le site met à leur disposition, comme le *flagging*. Une fois ce contenu ciblé, il faut analyser le bien-fondé de la plainte avant de retirer la contribution du site. Cette tâche reviendra habituellement aux modérateurs. Ces derniers visionneront le contenu dénoncé et ils vont ensuite voir si effectivement, il y a lieu de retirer la contribution du site.

Le délai entre le dépôt de la plainte et le retrait du matériel illicite variera d'un site à l'autre[44]. Plusieurs personnes peuvent donc être exposées au contenu pendant le processus décisionnel et en subir un préjudice. C'est pourquoi certains sites jugeront prudent de retirer temporairement du site Internet les contributions qui reçoivent des plaintes et ce, jusqu'à ce qu'un modérateur se soit penché sur la question[45].

Ce processus est unilatéral. Il est difficile de savoir sur quoi les modérateurs se fondent lorsqu'ils décident de retirer un contenu puisque tout se passe généralement à l'interne. Il y a par contre certains sites qui fondent leurs décisions sur les conditions d'utilisation du site[46].

La négociation. – Certains sites web 2.0 peuvent demander aux parties qui sont impliquées dans un litige de négocier entre elles pour tenter de résoudre le problème qui les oppose. La négociation peut se définir comme étant une démarche entreprise par les parties pour discuter du problème qui les oppose, afin d'arriver à une solution équitable et ce, sans avoir recours à une tierce partie[47]. La solution trouvée incorporera idéalement des propositions de tous les acteurs impliqués. La négociation est un processus consensuel, les parties peuvent se retirer de la négociation ou la continuer à leur guise.

Les façons de négocier varient d'un site à l'autre, tout dépendant des moyens mis à la disposition des usagers pour communiquer entre eux. Par exemple, sur Wikipedia, les gens qui soumettent des textes vont généralement échanger entre eux par le truchement de la page de discussion. Lorsqu'un conflit survient sur une page de Wikipedia, la procédure à suivre est simple[48]. Elle vise à éviter d'envenimer le différend en éditant à plusieurs reprises le contenu de l'article ou en écrivant sur celui-ci des commentaires personnels. Les personnes impliquées doivent plutôt aller sur la page de discussion et tenter d'y trouver un consensus, pour ensuite modifier l'article. La négociation est essentielle puisque les parties ne peuvent soumettre leur litige à la médiation

43 « Wikipedia : Dispute resolution », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Resolving_disputes (page consultée le 27 juin 2008)

44 Nous avons testé le système de retrait d'évaluation du site RateMyProfessors (http://www.ratemy professors.com) pour évaluer le délai qui peut courir entre le dépôt d'une plainte et le retrait de l'évaluation. Pour une infraction évidente à la politique d'utilisation du site, dans ce cas-ci il s'agissait de dire que le professeur préférait un certain groupe ethnique, le délai a été plutôt court, soit de cinq jours. Par contre, un délai d'environ deux semaines a été observé avant qu'un modérateur approuve un commentaire dont le caractère illicite était plutôt ambigu.

45 C'est d'ailleurs la méthode utilisée par le site Rate MyProfessors (http://www.ratemyprofessors.com/).

46 Voy., par exemple, la page http://www.ratemyprofessors.com/rater_guidelines.jsp, qui contient les directives du site RateMyProfessors pour écrire une évaluation.

47 Karim Benyekhlef et Fabien Gélinas, *Le règlement en ligne des conflits : enjeux de la cyberjustice*, Paris, Romillat, 2003, p. 66.

48 « Wikipedia : Dispute resolution », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Resolving_disputes (page consultée le 27 juin 2008).

ou à l'arbitrage s'il n'est pas démontré qu'elles ont préalablement tenté de s'entendre et ce, sans succès[49].

Les litiges sur eBay concernant les évaluations laissées par les cocontractants sont aussi visés par une procédure de négociation. En effet, eBay s'implique très peu dans ces litiges dont la résolution dépend finalement de la bonne volonté des parties impliquées. Des outils pour résoudre les conflits sont tout de même mis à la disposition des usagers, comme le retrait mutuel d'évaluation. Lorsque les deux personnes sont d'accord, il est possible de faire retirer les évaluations litigieuses dans le but de ne plus faire compter celles-ci dans le calcul des notes totales[50]. Par contre, les commentaires soumis resteront dans le dossier des parties.

La médiation, contrairement à la négociation, implique la présence active d'une tierce partie. En effet, il y a médiation lorsque les personnes impliquées dans un litige ont décidé, d'un commun accord, de soumettre leur différend à un médiateur qui les aidera à trouver une solution satisfaisante[51]. Le médiateur, contrairement à l'arbitre, ne pourra imposer une décision aux parties, il ne peut qu'en suggérer une. Ces dernières ne sont pas tenues d'accepter la solution et elles peuvent à tout moment mettre fin au processus de médiation.

Le site Wikipedia propose à ses usagers de recourir aux services d'un médiateur si les personnes impliquées dans un conflit n'ont pas été capables, par d'autres moyens, d'arriver à un consensus. La partie qui désire profiter de l'aide d'un médiateur doit remplir un formulaire, le faire parvenir au comité de médiation, et signifier aux autres parties en litige le désir de prendre part à ce processus[52]. La médiation est un processus volontaire, les gens qui ont reçu la signification disposent de sept jours pour accepter d'y participer, sinon elle n'a pas lieu[53]. Après quelques semaines, si l'affaire est acceptée, un médiateur interviendra et les parties pourront alors faire valoir leur point de vue[54].

Le site eBay propose plutôt à ses utilisateurs d'avoir recours à SquareTrade[55]. Ce site met à la disposition des usagers du site eBay un moyen pour résoudre les litiges qui y sont nés. En effet, lorsqu'un problème survient entre deux cocontractants, il est loisible à l'un ou l'autre de remplir un formulaire de plainte sur SquareTrade expliquant les raisons du mécontentement. À la suite de la soumission de la plainte, la partie adverse recevra un courriel lui expliquant que son cocontractant a fait une plainte, que SquareTrade est un service pour aider à résoudre les conflits sur eBay et qu'il est possible d'aller remplir à son tour un formulaire expliquant sa version des faits[56].

L'étape suivante est de tenter de négocier et si cela ne fonctionne pas, SquareTrade met à la disposition de ses membres des médiateurs qui peuvent aider à régler l'affaire moyennant

49 «Wikipedia : Dispute resolution », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Resolving_disputes (page consultée le 27 juin 2008).

50 «What is Mutual Feedback Withdrawal ? », *in* eBay, http://pages.ebay.com/help/feedback/questions/mutual-withdrawal.html (page consultée le 27 juin 2008).

51 Karim Benyekhlef et Fabien Gélinas, *Le règlement en ligne des conflits : enjeux de la cyberjustice*, Paris, Romillat, 2003, p. 67.

52 «Wikipedia : Mediation », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia :Mediation, (page consultée le 27 juin 2008).

53 «Wikipedia : Mediation », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia :Mediation (page consultée le 27 juin 2008).

54 «Wikipedia : Mediation », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia :Mediation (page consultée le 27 juin 2008).

55 http://www.squaretrade.com/.

56 Ethan Katsh et Janet Rifkin, « Online Dispute Resolution : Resolving Conflicts in Cyberspace », San Francisco, Jossey-Bass, 2001, p. 181.

paiement d'honoraires[57]. Lorsqu'un médiateur est assigné, il propose une solution aux parties après avoir pris connaissance du dossier. Pour que la solution soit acceptée, les deux parties doivent être d'accord. Bien que SquareTrade ne vise pas seulement les conflits concernant les évaluations, il est possible de requérir ce service pour arriver, entre autres, à une entente de retrait mutuel des évaluations.

L'arbitrage est un processus selon lequel les personnes impliquées dans un litige décident de confier le règlement de celui-ci à un tribunal indépendant qui prendra une décision, suite aux représentations des parties, qui aura force de loi et qui écartera tout recours possible devant un tribunal judiciaire[58].

Par exemple, le site Wikipedia offre une procédure d'arbitrage à ses utilisateurs. Il met à la disposition des usagers un comité d'arbitrage qui décidera d'entendre certaines affaires, à sa discrétion[59]. Les affaires qui seront entendues sont notamment celles qui ont été référées par le comité de médiation, ou celles qui ont passé par toutes les étapes de la résolution de conflit et ce, sans succès[60].

L'arbitrage est enclenché lorsqu'une des parties complète une demande pour aller en arbitrage[61]. Elle doit préciser les procédures qui ont été prises préalablement pour régler le conflit, elle doit expliquer le conflit et elle doit envoyer des notifications aux autres parties qu'une demande d'arbitrage a été faite[62]. Par la suite, si l'affaire est acceptée par le comité d'arbitrage, une page permettant de publier la preuve sera créée et les parties pourront tenter de convaincre les arbitres[63]. Une fois la preuve établie, le comité passera au vote et la décision finale sera celle qui aura obtenu la majorité des voix[64]. Des mesures peuvent également être prises pour éviter que le conflit perdure. De telles mesures vont de l'interdiction d'éditer une catégorie d'articles jusqu'à l'interdiction totale de participer au site Wikipedia[65].

Les mécanismes internes de régulation mis en place par divers sites ouverts à la participation des usagers visent manifestement à gérer les risques inhérents à l'exploitation d'un site dont le contenu est essentiellement fourni par l'usager. C'est assurément un lieu important d'élaboration et de relais de la normativité effectivement appliquée dans les environnements du web 2.0

2. Les mécanismes de responsabilité

Pour la plupart des acteurs, la responsabilité au regard du droit d'un ou de plusieurs États se présente comme un ensemble de risques à gérer. Les personnes et les entreprises doivent s'assurer que leurs pratiques sont conformes aux exigences des dispositions des lois suscep-

57 Ethan Katsch et Janet Rifkin, « Online Dispute Resolution : Resolving Conflicts in Cyberspace », San Francisco, Jossey-Bass, 2001, p. 183.

58 Karim Benyekhlef et Fabien Gélinas, *Le règlement en ligne des conflits : enjeux de la cyberjustice*, Paris, Romillat, 2003, p. 72.

59 « Wikipedia : Arbitration policy », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Arbitration_policy (page consultée le 27 juin 2008).

60 « Wikipedia : Arbitration policy », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Arbitration_policy (page consultée le 27 juin 2008).

61 « Wikipedia : Requests for arbitration/Request template », *in* Wikipedia, http://en.wikipedia.org/wiki/ Wikipedia :Requests_for_arbitration/Request_template (page consultée le 27 juin 2008).

62 « Wikipedia : Requests for arbitration/Request template », *in* Wikipedia, http://en.wikipedia.org/wiki/ Wikipedia :Requests_for_arbitration/Request_template (page consultée le 27 juin 2008).

63 « Wikipedia : Requests for arbitration/Request template », *in* Wikipedia, http://en.wikipedia.org/wiki/ Wikipedia :Requests_for_arbitration/Request_template (page consultée le 27 juin 2008).

64 « Wikipedia : Arbitration policy », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Arbitration_policy (page consultée le 27 juin 2008).

65 « Wikipedia : Arbitration policy », *in* Wikipedia, http://en.wikipedia.org/wiki/Wikipedia : Arbitration_policy (page consultée le 27 juin 2008).

tibles de trouver application et d'engager leur responsabilité. S'agissant des sites à contenu produit par l'utilisateur, les acteurs effectivement à l'origine de l'information délictueuse ne sont pas toujours identifiables ou peuvent se trouver hors d'atteinte : une victime peut se trouver dans une situation où seul un intermédiaire paraît être en mesure de répondre de la diffusion de matériel fautif qui lui cause préjudice. Ceux qui proposent des environnements à la disposition des utilisateurs sont souvent plus faciles à identifier et peuvent se révéler plus solvables que la personne qui serait à l'origine de la diffusion du document délictueux. D'où l'intérêt de déterminer où commence et où s'arrête la responsabilité des intervenants intermédiaires dans la chaîne de transmission de l'information sur Internet[66].

Lorsqu'un préjudice est causé, l'on recherchera une sanction et une réparation. Alors la normativité étatique sera souvent appelée en renfort. La responsabilité apparaît comme l'un des principaux lieux où se construit l'articulation entre les valeurs contradictoires que recèlent les droits et libertés. En départageant ce qui constitue un comportement fautif, les régimes de responsabilité contribuent à procurer les différentes hiérarchies et préséances entre les droits fondamentaux. Par exemple, un régime strict de responsabilité peut induire les acteurs à opter pour la mise en place de mesures et précautions. À l'inverse, un régime procurant une grande immunité à certains acteurs permettra le développement de types d'activités qui auraient pu autrement paraître plus risquées. Ainsi, il est peu probable que des sites à contenu généré par les usagers comme Facebook, You Tube ou les sites d'évaluation des personnes (comme ratemyprofessor.com) auraient été mis en ligne dans une environnement juridique qui ne prévoit pas l'immunité de l'article 230(a)(1)2 du Computer Decency Act[67].

3. Les contrats

Les contrats sont à la fois un nœud et un relais de normativité. C'est au moyen de contrats que les acteurs d'Internet vont chercher à transférer certains risques à leurs cocontractants. De cette façon, sont relayées plusieurs exigences des lois nationales des territoires où sont situés les sites. Avec le Web 2.0, les contrats qui sont conclus en ligne s'inscrivent de plus en plus dans un environnement de transactions ouvert au sein duquel la crédibilité et la confiance tendent à jouer un rôle régulateur central[68].

La pratique contractuelle contribue largement à l'identification et au développement des usages élaborés par les multiples opérateurs d'Internet. Dans un environnement où la pratique contractuelle prend tant d'importance, le développement de guides et de contrats-types devient également un relais par lequel se traduisent concrètement les principes énoncés dans les lois et autres textes provenant d'autorités en mesure d'exercer une influence. Une politique de concertation avec les acteurs privés exerçant une influence est de nature à accentuer l'efficacité des mesures mises en

66 Fabrice De Patoul, « La responsabilité des intermédiaires sur internet : les plates-formes de mise en relation, les forums et les blogs », [2007] 27 *R.D.T.I.* 85-106 ; Pierre Trudel, *La responsabilité sur Internet selon le droit civil du Québec* », rapport préparé pour le colloque de droit civil 2008 de l'Institut national de la magistrature, Ottawa, 13 juin 2008.

67 Computer Decency Act, 47 U.S.C. s 230(a)(1) ; Melissa A. Troiano, « The New Journalism ? Why Traditional Defamation Laws Should Apply to Internet blogs », *Am. U.L.Rev.*, 2006, 55, 1448 ; Robert G. Magee et Tae Hee Lee, « Information Conduits or Content Developpers ? Determining Whether News Portals Should Enjoy Blanket Immunity from Defamation Suits », *Comm L. & Pol'y*, 2007, 12, 369-404.

68 Shmuel I. Becher et Tal Z. Zarsky, « E-Contract Doctrine 2.0 : Standard Form Contracting in the Age of Online User Participation », *Michigan Telecommunications and Technology L. Rev.*, 2008, 14, 303-366.

place par un État. Pour optimiser les initiatives du secteur privé et des autres secteurs, il faut, dans toute la mesure du possible, promouvoir et valoriser les initiatives et bonnes pratiques mises en place ou expérimentées dans le secteur privé. Les initiatives du secteur privé se retrouvent non seulement au niveau de la répression mais aussi en amont. Les pratiques contractuelles jouent un rôle significatif[69].

Une politique active de concertation autour de contrats types peut constituer un relais efficace afin de porter les risques à la connaissance de ceux qui sont le plus en mesure de les gérer. Le contrat est l'outil de prédilection pour assurer le relais des obligations qui découlent des lois vers les parties qui sont en position d'y donner suite[70]. C'est aussi un moyen par lequel il est possible de transférer les risques découlant d'une activité. Par exemple, le contrat d'assurance procure un mécanisme de transfert de certains risques, c'est l'un des modes de régulation fondés sur le contrat qui peut être utilisé afin de gérer les risques[71].

En fin de compte, le développement de pratiques contractuelles contribue à relayer les principes normatifs exprimés dans les lois étatiques qui sont relevantes à une activité. Un tel relayage s'inscrit souvent dans le cadre de processus de corégulation.

4. Les processus de corégulation

L'ensemble des risques associés au web 2.0 peuvent être discutés et les solutions validées dans un cercle plus ou moins large d'acteurs du secteur public, privé et communautaire : d'où l'intérêt des processus de corégulation. Les processus d'autorégulation et de corégulation[72] se révèlent d'importants relais des normativités encadrant les activités relatives à Internet. Par ces processus, on opère l'actualisation, l'adaptation et la particularisation des règles de droit considérées comme relevantes aux diverses activités prenant place sur Internet.

De tels processus peuvent s'envisager comme un cycle continu dans lequel les exigences découlant des autres normativités, dont les lois étatiques, sont systématiquement discutées, évaluées et ajustées de manière évolutive. Par exemple, en octobre 2007, un ensemble de grandes entreprises activées sur Internet et importantes détentrices de droits d'auteurs ont mis de l'avant des principes sur la diffusion de contenus générés par les usagers. Les Principles for User Generated Content Services énoncent un ensemble d'objectifs partagés par les protagonistes dans les termes suivants :

« In coming together around these Principles, Copyright Owners and UGC Services recognize that they share several important objectives : (1) the elimination of infringing content on UGC Services, (2) the encouragement of uploads of wholly original and authorized user-generated audio and video content, (3) the accommodation of fair use of copyrighted content on UGC Services, and (4) the protection of legitimate interests of user privacy. We believe that adhering to these Principles will help UGC Services and Copyright Owners achieve those objectives »[73].

69 *1267623 Ontario* c. *Nexx Online* O.J., 1999, n° 2246, voy. : Marie-Hélène Deschamps-Marquis, « Courriels indésirables, s'abstenir ! », Juriscom.net, octobre 1999, http://www.juriscom.net/int/dpt/ dpt20.htm#note1.

70 Vincent Gautrais, *L'encadrement juridique du contrat électronique international*, Bruxelles, Éditions Bruylant, 1998.

71 Richard V. Ericson, Aaron Doyle et Dean Barry, *Insurance as Governance*, Toronto, University of Toronto Press, 2003, p. 8.

72 Jacques Berleur et Yves Poullet, « Quelles régulations pour l'Internet ? », *in* Jacques Berleur, Christophe Lazaro et Robert Queck, *Gouvernance de la société de l'information*, Bruxelles-Namur, Bruylant, Presses universitaires de Namur, 2002, pp. 133-151.

73 Principles for User generated Content Services, http://www.ugcprinciples.com/ ; Internet and Media Industry

La déclaration énonce ensuite quinze principes relatifs à la protection des droits d'auteurs mais également des engagements relatifs au recours aux technologies d'identification des œuvres, celui d'accommoder l'utilisation équitable et de coopérer avec les autres entités intéressés. Bien qu'elle ne constitue pas en tant que tel un contrat emportant un effet obligatoire pour les signataires, une telle déclaration paraît emblématique des modes d'application des règles de droit dans un univers comme celui du web 2.0. Prenant appui sur la législation d'un État telle qu'elle est, les principes indiquent comment la loi sera suivie et appliquée et précisent en quelles circonstances des poursuites civiles pourront être engagées[74]. On voit clairement ici la fonction de relais d'une normativité tenue par ce type de démarche de corégulation.

5. La sensibilisation des usagers

Dans une approche fondée sur la gestion des risques, le volet sensibilisation et éducation prend une importance considérable. Il faut en effet s'assurer que chaque usager est en mesure de reconnaître et de gérer à son niveau les risques. Plus l'implication de l'usager est importante, plus il faut s'assurer que ce dernier est adéquatement en mesure d'identifier et de gérer les risques qui doivent l'être à son niveau. Dans un environnement ouvert tel qu'Internet, il est impossible de postuler qu'une entité quelconque est en mesure de se substituer à un usager pour reconnaître et gérer les risques à sa place. C'est dans cet esprit que s'inscrivent les mesures visant à rendre les usagers conscients des risques. Par exemple, la section « sécurité » des conditions d'utilisation du site MySpace.fr comporte les mises en garde suivantes aux usagers[75] :

« MySpace vous permet de vous exprimer, de vous connecter avec des amis et de faire connaissance avec de nouvelles personnes, mais n'oubliez pas que ce que vous publiez peut vous mettre dans une situation embarrassante ou vous exposer à un danger. Voici quelques directives qu'il est préférable de respecter lorsque vous utilisez MySpace :

N'oublie pas que ton profil et les forums MySpace sont publics. Ne publie rien dont tu ne souhaites pas qu'il soit rendu public (numéro de téléphone, adresse, nom de scène ou allées et venues). Évite de publier toute information qui permettrait à un étranger de te localiser, par exemple les lieux que tu fréquentes chaque jour après l'école.

Les gens ne sont pas toujours qui ils disent être. Sois prudent lorsque tu ajoutes des étrangers à ta liste d'amis. Se connecter avec des amis MySpace du monde entier est amusant, mais évite de rencontrer en personne des gens que tu ne connais pas parfaitement. Si tu as l'intention de rencontrer quelqu'un, fais-le en public et amène un ami ou un adulte de confiance avec toi.

Le harcèlement, les propos d'incitation à la haine et les contenus inappropriés doivent être signalés. Si tu as l'impression que le comportement de quelqu'un est déplacé, signale-le. Parles-en à un adulte en qui tu as confiance ou signale-le à MySpace ou aux autorités.

Ne publie pas quelque chose qui pourrait te mettre dans une situation gênante plus tard. Penses-y à deux fois avant de publier une photo ou des informations que tu ne veux pas que tes parents ou ton patron voie !

Leaders Unveil Principles to Foster Online Innovation While Protecting Copyrights, http://www.ugcprinciples.com/press_release.html.

74 « The Principles for User Generated Content Services : A Middle-Ground Approach to Cyber-governance », *Harvard L. Rev.*, 2008, 121, 1387 p. 1388.

75 Http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safetytips.

Ne trompe pas les gens en leur faisant croire que tu es plus âgé ou plus jeune. Si tu mens à propos de ton âge, MySpace supprimera ton profil.

Il faut également assurer l'information en continu sur les risques et enjeux auxquels les usagers peuvent avoir à faire face. Le caractère essentiellement évolutif de l'environnement interdit de postuler que les dangers sont connus et maîtrisés une fois pour toutes. Les nouvelles tendances, les « nouveaux trucs » doivent être identifiés et les risques évalués. Les stratégies les plus adéquates doivent être discutées et diffusées auprès des diverses catégories d'usagers.

CONCLUSION

La régulation du web 2.0 peut être envisagée selon un modèle de gestion des risques. Sur Internet, l'usager – plus actif que jamais – gère ses risques : il les accepte ou les transfère, il peut choisir de les augmenter ou de les minimiser. La portée et la teneur effective des réglementations balisant les activités associées au web 2.0 sont la résultante des décisions de gestion des risques de l'ensemble des acteurs. Les principaux risques du web 2.0 découlent de la configuration des espaces virtuels dans lesquels il est possible d'interagir. Ces environnements sont construits par la technique et ce qu'il est possible d'y faire ou non sont largement tributaires des configurations. Les comportements des usagers et des entreprises actives sur le réseau sont aussi générateurs de risques. La régulation elle-même, qu'elle résulte de la loi ou d'autres sources de normativités est, en pratique, perçue comme un risque à gérer.

Pour leur part, les États peuvent mettre en place des mesures afin d'accroître ou de limiter les risques que peuvent avoir à prendre les internautes à l'égard desquels s'appliquent leurs lois. Mais encore là, pour les acteurs du web 2.0, les lois des États se présentent à leur tour comme des risques à gérer. Le droit des États et les autres normativités – comme les normes issues de la technique – créent plus ou moins de risques pour la vie privée ou pour les autres intérêts des acteurs du net.

Comprise comme un ensemble de risques à gérer, la régulation du web 2.0 s'envisage comme un réseau de normes pensées et mises en place dans des nœuds multiples d'un environnement qui est lui-même configuré en réseau. De telles normes sont forcément relayées via une pluralité de processus. L'incitation à relayer les exigences d'une règle de manière à obliger l'autre est fonction de la capacité de cette règle à générer un risque qui sera perçu comme significatif par les acteurs concernés. Envisager ainsi la régulation permet de tenir compte des dynamiques régulatrices qui sont nécessairement mises en place par les acteurs dès lors qu'ils ont conscience de courir des risques.

La normativité issue de la technique peut engendrer des risques ou procurer des solutions en limitant l'incidence. Une portion de l'activité régulatrice des États pourra être dévolue à la mise au jour des risques associés à certains types de pratiques et activités dans les environnements du web 2.0. L'État et les autres régulateurs peuvent accroître ou limiter les risques comme par exemple ceux qui découlent des activités d'une entité vouée à la mise en place de sites de réseautage sociaux. Les décisions de gestion des risques qui se prennent dans les divers lieux en mesure d'imposer leur volonté engendrent des normes qui à leur tour sont relayées par les autres acteurs. Les États peuvent imposer des obligations qui limitent les risques pour les individus et autres sujets de droit. Sur Internet, ces mesures seront à leur tour généralement perçues par les acteurs comme autant des risques à gérer et à transférer aux cocontractants. L'efficacité de la

régulation est fonction de la capacité effective d'accroître les risques de ceux qui mènent des activités problématiques et à gérer les risques des utilisateurs légitimes.