Quelles limites à la « Google™ isation » des personnes ?

Pierre Trudel*

Rapport présenté au Colloque international **La sécurité de l'individu numérisé – Réflexions prospectives et internationales**, Paris, CNRS, 22 et 23 novembre 2007.

* 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 .

Sommaire

Le phénomène Google évoque à lui seul un vaste ensemble d'enjeux et inquiétudes sucités par le développement d'Internet. Fondée en 1998, Google s'est imposé comme le principal moteur de recherche sur le net. Fort de ce succès, l'entreprise a étendu ses activités à plusieurs autres fonctions d'Internet.

À l'égard des personnes, les activités d'une société comme Google présentent des enjeux importants : qu'advient-il des données générées par les multiples requêtes que les internautes introduisent quotidiennement sur le moteur de recherche ? Quels enjeux pour les droits des individus découlent des activités telles que *Google Earth* qui diffuse des vues aériennes des multiples lieux sur la planète, que dire de *Google Street View* qui capte des images des rues des grandes viloles pour les rendre disponibles sur le web ? Qu'il s'agisse de la collecte de données personnelles ou de la mise à disposition d'oeuvres protégéers par le droit d'auteur, les enjeux juridiques posés par les moteurs de recherche et singulièrement par le plus important d'entre eux sont majeurs.

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 moteurs de recherche sur Internet est essentiellement une démarche continue de prise en compte et de gestion des risques perçus à l'égard des activités de recherche.

Par leur activité, les moteurs de recherche et les autres fonctions d'Internet génèrent des risques pour les internautes. Les solutions techniques et les configurations peuvent augmenter ou minimiser les risques pour les usagers. La réglementation étatique peut venir augmenter les risques des internautes ou ceux des exploitants de moteurs de recherche. Alors ces derniers auront à gérer les risques de se retrouver en non conformité avec la législation nationale d'un État ou de plusieurs. Il revient à l'entreprise et aux usagers de gérer ces risques. En somme, la régulation d'internet peut s'envisager comme un ensemble de règles découlant de la technique ou des normes étatiques et non étatiques. Ces normes créent des risques pour les usagers et les autres acteurs. Ceux-ci gèrent les risques associés à leur activité sur le réseau. Il en résulte une régulation caractérisée par le souci des acteurs de transférer ou relayer les risques qu'ils percoivent vers les autres participants au réseau.

Dans un réseau, les régulateurs et les acteurs sont en position d'accroître ou de réduire les risques pour eux-mêmes ou pour d'autres. La technique produit des situations qui augmentent ou diminuent les risques. II en est de même pour les lois étatiques principalement celles des entités dominantes comme l'Union européenne ou les États-Unis. Les acteurs du net 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 dans le cyberespace est essentiellement la résultante des stratégies de gestion des risques des acteurs et des régulateurs.

Introduction

Internet serait d'un usage infiniment plus difficile sans les divers outils permettant aux usagers de repérer les pages d'informations pertinentes à leurs intérêts. Les moteurs de recherche rendent visibles ce qui serait pratiquement introuvable sur le réseau. C'est une ressource essentielle pour assurer une réelle possibilité d'accès aux informations par les utilisateurs.[1]

En rendant visibles des informations qui ne le seraient pas autant, les outils de recherche contribuent à braquer les projecteurs aussi bien sur les informations qui font partie du domaine public que celles qui s'inscrivent dans des domaines réservés. Les outils de recherche accroissent les risques pour les usagers d'Internet et même des autres personnes[2]. Une proportion considérable des requêtes de recherche effectuées sur Internet le sont sur les sites de Google, l'entreprise a connu une progression fulgurante[3]. Sa valeur boursière s'est multipliés par des facteurs à faire rêver les investisseurs les plus audacieux. L'entreprise à mis de l'avant divers projets dont plusieurs soulèvent d'importants enjeux pour la vie privée des personnes.[4] Il n'en faut pas plus pour poser la question des limites au phénomène de googleisation de l'individu. Jusqu'où est-il envisageable de tolérer quune seule entreprise détienne autant de données sur les internautes de la planète entière ? Dans quelle mesure est-il acceptable que l'on diffuse à la grandeuur de la toile des images de allées et venues des individus circulant sur les rues des villes du monde entier ?

À la vérité, Google, à l'instar des autres moteurs de recherche, apparaît comme une infrastructure critique d'Internet : elle en possède l'ubiquité et se révèle emblématique des enjeux et risques que pose le réseau des réseaux. Les multiples applications de Google sont en voie de se généraliser et de se banaliser. Yves Poullet observe qu'Internet favorise une double globalisation. Dans un premier sens par la dimension internationale des réseaux et leur convergence et dans uns second sens, dans la mesure où l'ensemble des activités est traduite en information numérique[5]. Internet prend l'aspect d'un lieu d'interactions ayant vocation à embrasser la presque totalité des dimensions de la vie sociale.

---

1 James GRIMMELMANN, « The Structure of Search Engine Law », [2008] 93 *Iowa L.Rev*. à paraître ; Bostjan BERCIC, « Protection of Personal Data and Copyrighted Material on the Web : The Cases of Google and Internet Archive », [2005] 14 *Information & Communications Technology Law*, 17-24.

2 Laurent CARON, « Protection des données personnelles et moteurs de recherche : quels sont les réels enjeux ? » *Légipresse*, no. 244, septembre 2007, p. 111 ; Jayni FOLEY, « Are Google Searches Private ? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases », [2007] 22 *Berkeley Tech, L.J.,* 447-475.

3 AFP, « Google leader écrasant de la recherche sur internet mondial », 9 octobre 2007, < http://afp.google.com/article/ALeqM5hmg2WxR4pLsvDGhzplle3bZWfcxg >.

4 Voir, « Who's afraid of Google ? » *The Economist*, September 1, 2007.

5 Yves POULLET, « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », [2005] 5 *Revue Lamy Droit de l'immatériel*, 47, note 66.

Devant une telle globalisation[6], - qui tend vers une « googleisation » ! - 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 instituer les limites à la « googleisaton » des individus dans le cyberespace et ailleurs. Le droit étatique n'est pas seul à encadrer les activités des moteurs de recherche sur Internet : la normativité de ces ressources procède aussi de ce que la technique permet ou prohibe de même que des pratiques observées par les différents acteurs.

À l'instar de plusieurs observateurs, il faut parler d'une multirégulation, de coexistence sur le réseau de plusieurs types de régulation répondant à des objectifs différents, par des méthodes différentes et également légitimes[7]. La régulation des activités se déroulant sur Internet peut être envisagée selon le modèle du réseau. Le cyberespace, constate Thomas Schultz constitue un laboratoire intéressant des phénomènes juridiques contemporains[8]. Le fonctionnement de la régulation doit être examiné en portant attention aux flux de normativité qui constituent la base du droit effectivement appliqué dans le cyberespace.

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[9]. 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 des ces phénomènes paraît bien être le risque juridique : 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[10].

Philippe Amblard observe que la régulation de l'Internet se caractérise par le pluralisme de son processus normatif qui tendrait à promouvoir l'efficacité sociale d'un droit vivant par opposition à « l'artificialité positiviste de la loi étatique »[11]. Michel Vivant, après avoir pris acte des divers modèles de régulation agissants sur Internet constate que « c'est bien de régulations -au pluriel-

---

6 Le mot est ici utilisé pour désigner le processus d'interconnexion croissante des économies et sociétés résultant du développement des technologies de l'information. Cynthia GHORRA-GOBIN, *Dictionnaire des mondialisations*, Paris, Armand Colin, 2006, p. 185.

7 Thomas SCHULTZ, *Réguler le commerce électronique par la résolution des litiges en ligne*, Bruxelles, Brulant, 2005, p. 162. Cet auteur rapporte les points de vues de la Mission interministérielle français sur l'Internet et du Conseil supérieur de l'audiovisuel français. Il relate les observations de Marc MAESSCHALCK et Tom DEDEURWAERDERE, « Autorégulation, éthique procédurale et gouvernance de la société de l'information », dans Jacques BERLEUR Christophe LAZARO et Robert QUECK, *Gouvernance de la société de l'information*, Bruxelles, Bruylant- Presses Universitaires de Namur, 2002, 77-103.

8 Thomas SCHULTZ, « La régulation en réseau du cyberespace », [2005] 55 *R.I.E.J.*, 31, p. 32.

9 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 ».

10 Voir, pour une méthodologie d'analyse des risques juridiques : Franck VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, pp. 39 et ss.

11 Philippe AMBLARD, *Régulation de l'Internet l'élaboration des règles de conduite par le dialogue internormatif*, Bruxelles, Bruylant, 2004, no. 80.

qu'il convient de parler, de modes de régulation qu'il convient d'articuler au mieux de combiner en raison.[12] »

Envisagée dans la logique du réseau la régulation des outils de recherche sur Internet 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.

1. Les risques découlant des activités des moteurs de recherche

La problématique des outils de recherche doit être abordée en tenant compte du fait que leur usage suppose la collecte et la conservation de données pouvant être rattachées à des personnes. Il faut aussi garder à l'esprit que les usagers d'internet sont forcément impliqués à divers degrés dans la vie de la cité et mènent de ce fait des activités qui concernent les autres. Ces derniers peuvent avoir un intérêt légitime à acéder aux informations, même celles que l'on voudrait camoufler afin de mieux paraître. À l'instar de l'environnement physique, le cyberespace est constitué de lieux publics et de lieux privés, l'expectative légitime de vie privée devrait varier en fonction du contexte dans lequel se trouve l'usager.

Les moteurs de recherche 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 ressources publiques. L'agglomération de données sur les requêtes de recherche introduites par les internautes augmente les risques de transfert préjudiciable de ces informations. Au nombre des risques souvent signalés à cet égard, il y a la constitution de répertoires d'informations disponibles aux forces de police

Il faut tenir compte des possibilités réelles que les forces de police demandent d'accéder à ces données à des fins d'enquête ou dans le cadre d'activités visant à prévenir le crime. Afin de protéger le lien de confiance entre les moteurs de recherche et les usagers, il paraît approprié de conserver les renseignements uniquement pour les besoins démontrés du système de recherche et de les détruire dès que ces besoins sont satisfaits. L'agglomération et la persistance de l'information emportent la constitutions de répertoires qui pourraient devenir accessibles aux autorités policières ; c'est là un risque d'Internet. Mais le droit des forces de police d'exiger de telles informations est une question qui relève essentiellement de la régulation de la police. Réclamer des mesures de censure des informations circulant sur Internet au seul motif que celles-ci pourraient intéresser les forces de police, c'est imposer à tous les usagers légitimes de l'information, des contraintes découlant des possibles abus de quelques uns.

---

12 Michel VIVANT, « Internet et modes de régulation », dans Étienne MONTERO, *Internet face au droit*, Bruxelles, Story Scientia, 1997, 215, p. 229.

Si les informations peuvent être conservées et mises à disposition, il y a risque de décontextualisation de ces données et une réelle possibilité de perte de confiance dans les environnements du cyberespace.

L'accumulation et l'agglomération de données sur les personnes par les moteurs de recherche et d'autres fonctions disponibles sur Internet emporte la constitution de répertoires importants d'information potentiellment disponibles aux activités de surveillance de toutes sortes. C'est un risque qui paraît inhérent aux modes de fonctionnement actuel des outils de recherche sur Internet. C'est dire à quel point une approche fondée sur la gestion des risques apparaît comme étant la plus à même de faciliter l'idntification de stratégies pour la régulation efficace des activités des moteurs de recherche.

1.1 La vie privée et la protection des données personnelles

Sur Internet, il y a des activités publiques tandis que d'autres supposent un certain nombre d'intérêts relatifs à la vie privée. Pour fonder une approche conforme à l'impératif d'équilibre entre l'ensemble des droits fondamentaux, il faut tenir compte de l'aspect en continuum des situations publiques et de situations privées. Dans le cyberespace, tout n'est pas que public ou que privé comme s'il n'y avait que le noir et le blanc. L'intensité publique et privée des situations est en nuances variables selon les contextes et les circonstances. C'est dans ce cadre que doit être abordé la régulation des outils de recherche et autres infrastructures d'Internet.

Le droit à la vie privée est parfois présenté comme un droit omnipotent à être protégé contre un ensemble infini d'inconvénients de la vie sociale. Tant et si bien que pour échapper aux exigences d'équilibre que comporte le droit à la vie privée, on en est venu à mettre de l'avant la notion de « protection de la vie personnelle » afin de justifier des régulations faisant prévaloir le désir des personnes de contrôler toutes les informations qui leur déplaît. À ce jour, l'approche induite par le droit de la protection des données personnelles est loin de constituer une régulation suffisamment nuancée pour assurer les équilibres essentiels entre le privé et le public.

À moins d'en faire le droit qui éclipse tous les autres, le droit à la vie privée est un rempart garantissant la dignité des personnes dans des contextes multiples et infiniment variables. Ainsi compris, le droit à la vie privée est un droit aux contours flous faisant appel à des seuils mobiles de compatibilité dans le temps et dans l'espace[13].

La régulation équilibrée des outils de recherche doit tenir compte à la fois de la nécessité d'assurer l'accès des usagers aux informations et la protection de la vie privée des personnes. Il est donc essentiel de tenir compte du caractère essentielement nuancé du droit à la vie privée plutôt que de privilégier une conception de celui-ci qui conduit à éclipser les autres valeurs.

1.1.1 Un sens variable selon les époques et les tissus culturels

Le droit à la vie privée connaît un sens qui varie selon les époques et les cultures. Son contenu est variable selon les circonstances, les personnes concernées et les valeurs d'une société ou d'une

---

13 Jean-Louis HALPERIN, « L'essor de la 'privacy' et l'usage des concepts juridiques », *Droit et Société*, 61/2005, 765, p. 781.

communauté[14]. Généralement, on inclut dans la vie privée les informations relatives à la vie sentimentale ou sexuelle, l'état de santé, la vie familiale, le domicile et même les opinions religieuses, politiques ou philosophiques lorsqu'on choisit de ne pas les exprimer publiquement. On peut également y inclure l'orientation sexuelle d'une personne, son anatomie ou son intimité corporelle. La vie privée se présente comme étant la «zone d'activité» qui est propre à une personne et qu'elle est maître d'interdire à autrui[15]. On admet aussi généralement que le domaine de la vie privée d'une personnalité publique peut, en certaines circonstances, être plus restreint que celui d'un simple citoyen[16]. Or, il y a sur Internet des situations dans lesquelles une personne est en position publique. On ne peut se mettre à publier son profil personnel sur Internet et exiger que cela n'emporte aucun risque.

Pour établir s'il y a atteinte à la vie privée, il est nécessaire de déterminer si une divulgation d'information ou une intrusion porte sur un élément de la vie privée. Le domaine de la vie privée regroupe certains types d'informations qui y sont, en principe, rattachées mais il connaît aussi des variations selon les qualités et la situation des personnes. Le contenu concret du domaine de la vie privée varie suivant les personnes, la position qu'elles occupent dans la société et d'autres circonstances. Cette prise en compte du contexte est inhérente à la notion de vie privée. Cela permet de délimiter le contenu du domaine de la vie privée en fonction des circonstances, notamment la participation de l'individu à la vie de la collectivité[17].

Tout ce qui touche les personnes ne peut logiquement relever de leur vie privée. Le droit à la vie privée concerne les informations qui affectent l'autonomie d'une personne, sa capacité à exercer un contrôle sur les informations qui concernent son intimité ou ses choix de vie. Mais dès lors qu'une personne exerce des activités qui en concernent d'autres, le champ de sa vie privée est forcément restreint par les intérêts légitimes des autres.

Il est bien établi que les personnalités publiques ont une vie privée plus limitée que les autres citoyens. Les personnalités publiques sont celles qui décident, de leur propre chef ou en raison de circonstances particulières, de participer à des activités se déroulant en public ou pour lesquelles elles recherchent la confiance ou l'attention du public. Il peut s'agir de membres du gouvernement, de personnalités artistiques ou sportives, mais également de dirigeants d'organisations ou de professionnels qui interviennent dans l'espace public. Cette distinction pourtant essentielle en démocratie est souvent ignorée dans l'application des lois sur la protection des données personnelles.

Par exemple, le fait de prendre part à une compétition sportive en public suppose que l'on accepte de respecter les règles du jeu. L'information de nature à assurer la probité du déroulement de compétitions sportives devrait avoir un caractère public. Malheureusement, l'application stricte

---

14 Pierre TRUDEL et France ABRAN, *Droit du public à l'information et vie privée : deux droits irréconciliables?*, Montréal, Thémis, 1992.

15 Bernard BEIGNIER, «Vie privée et vie publique», (sept. 1995) 124 *Légipresse* 67-74.

16 André BERTRAND, *Droit à la vie privée et droit à l'image*, Paris, Litec, 1999.

17 Patrick A. MOLINARI et Pierre TRUDEL, « Le droit au respect de l'honneur, de la réputation et de la vie privée : aspects généraux et applications », BARREAU DU QUÉBEC, *Application des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 1988, 211.

de certains principes du droit de la protection des données personnelles tend faire prévaloir une conception de la vie privée laissant peu de place aux impératifs de transparence. Par exemple dans un avis rendu en juin 2005, la CNIL censure la diffusion d'un annuaire recensant plus de 1000 coureurs cyclistes ayant reconnu s'êtres dopés ou avoir été contrôlés positifs[18].

Le sort qui a été fait à une liste de notaires publiée sur Internet fournit une autre illustration du caractère excessif de certaines applications du droit de la protection des renseignements personnels. La publication d'une liste noire de notaires sur un site Internet sans permettre à ces professionnels de s'opposer à ce que leurs coordonnées y figurent a été jugée contraire à la loi française « Informatique et libertés ». La cour d'appel de Bourges dans un arrêt du 11 janvier 2007 a confirmé la condamnation prononcée par le tribunal correctionnel de Bourges le 5 juillet 2006 contre la Ligue européenne de défense des victimes de notaires. Cette association, aujourd'hui liquidée, avait autorisé sa secrétaire générale à créer et mettre en place un site web au nom de l'Association. L'objectif du site était critique à l'égard de certains membres de la profession notariale. Sur la page d'accueil, on pouvait lire que la profession de notaire faisait courir « les plus grands risques aux clients ». Ce propos était accompagné d'une liste de 2 500 notaires dont il était affirmé que « le fait d'être inscrit sur le site de la Ligue européenne de défense des victimes de notaires n'implique aucun préjugé ni pré-jugement ; cela implique simplement que notre association a un dossier concernant un client ou plusieurs clients de l'étude de notaire ». Certains officiers publics qui n'ont pas accepté de voir leur compétence et leur honnêteté mises en doute ont écrit au site pour faire retirer leur nom de cette liste. Mais la secrétaire générale de l'Association a refusé d'accéder à leur demande car cette diffusion servait les buts qu'elle s'était fixée. Saisie de cette affaire, la Commission nationale sur l'informatique et les libertés (Cnil) a dénoncé les faits au parquet. La Commission a estimé que l'association n'avait pas respecté le droit des personnes à s'opposer, pour des motifs légitimes, à ce que leurs coordonnées soient traitées, droit énoncé à l'article 38 de la loi « Informatique et libertés ». Le tribunal puis la cour de Bourges ont confirmé l'analyse de la Commission[19]. Cet exemple indique que le droit de la protection des données personnelles est si peu nuancé et si biaisé en faveur du respect des caprices des individus exerçant des charges publiques qu'il peut être détourné afin de faire taire les activités relevant de la liberté de critique sur Internet.

La conception démocratique de la vie privée postule que les personnes occupant une fonction publique ou exerçant une activité sollicitant la confiance du public sont en général soumises à un devoir plus intensif de transparence. Les personnes impliquées de leur plein gré ou involontairement dans un événement public doivent aussi s'attendre à une vie privée moins étendue, du moins tant que dure cet évènement. Or, sur Internet, il existe des lieux et des évènements publics. On s'y engage avec les avantages qu'on en retire mais aussi avec les risques et inconvénients qui les accompagnent.

---

18 CNIL, *Suite à l'information donnée sur son site par l'intéressé lui-même, la CNIL confirme qu'elle a mis en demeure le responsable de ce site de cesser la publication d'un annuaire du dopage*, Communiqué du 30 juin 2005, < http://www.cnil.fr/index.php?id=1843&news[uid]=271&cHash=a9b6482b22 >.

19 *Gisèle N., Ligue européenne de défense des victimes de notaires / Ministère public*, Cour d'appel de Bourges 2ème chambre Arrêt du 11 janvier 2007, < http://www.legalis.net/jurisprudence-imprimer.php3?id_article=1903 >

La vie privée possède une intensité variable selon les contextes. Sur Internet, comme ailleurs, l'intensité du droit à la vie privée varie en fonction d'une pluralité de facteurs. Selon les contextes, il existe des situations différenciées délimitant des espaces de vie privée et l'évaluation de la présence d'impératifs de dignité de la personne et des exigences d'information auxquelles les autres peuvent légitimement prétendre conduit à reconnaître que certains espaces et informations sont publics. Ce phénomène est d'ailleurs pris en compte selon les systèmes juridiques au moyen de divers concepts et standards. Par exemple, en droit pénal canadien, on a recours à des notions comme l'expectative raisonnable de vie privée afin de délimiter les situations où doivent prévaloir le droit à la vie privée ou d'autres impératifs[20].

1.1.2 Les intérêts différenciés à connaître des usagers d'Internet

La vie privée se présente avec des intensités variables dans les multiples contextes qui coexistent sur Internet. Les situations relationnelles dans lesquelles chacun est engagé engendrent des intérêts différenciés à connaître certaines informations pour les personnes se trouvant dans l'environnement. Par exemple, le conjoint à un intérêt légitime à connaître certains éléments de la vie de l'autre conjoint alors que cet intérêt n'est pas présent chez le voisin de palier. De même, l'employeur a intérêt à connaître certaines informations relatives à l'employé pour certaines fins mais pas pour d'autres. Ces intérêts différenciés à connaître constituent autant de facteurs de limitation de la vie privée. Lorsque de tels intérêts existent, c'est-à-dire lorsque sont réunies les conditions y donnant ouverture, le droit à la vie privée cède le pas puisqu'il existe un intérêt légitime à connaître.

Ce phénomène peut être illustré en représentant les informations protégées par le droit à la vie privée en cercles concentriques. De tels cercles délimitent les informations qui peuvent demeurer du domaine privé et par le fait même, celles qui peuvent licitement circuler. Ces informations ne coïncident pas nécessairement avec ce que nous consentons à rendre disponible. Kaiser démontre bien que le consentement n'est pas le concept approprié afin de rendre compte de la légitimité de la circulation des informations concernant les personnes. Il écrit que l'explication consistant à postuler que la personne consent tacitement à des investigations et divulgations est inexact puisque « la personne qui sort de sa vie privé pour se livrer à une activité publique ne songe pas à donner son consentement à la divulgation de cette activité. Elle pense encore moins à donner son autorisation à des recherches relatives à ses activités publiques. » Kayser ajoute que :

> *L'explication présente le défaut plus grave de se révéler inexacte car, si elle rendait compte de la réalité, une personne pourrait s'opposer, par une manifestation de volonté à des investigations et à des divulgations relatives à ses activités publiques. Elle pourrait même s'opposer à la réalisation et à la publication d'images la représentant dans une de ces activités. Or, elle n'a pas ce pouvoir.*[21]

---

20 *La Reine* c. *Dyment*, [1988] 2 R.C.S. 417. L'arrêt *Dyment* a reconnu une facette informationnelle au droit à la vie privée. Voir à cet égard Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992, p. 29.

21 Pierre KAYSER, *La protection de la vie privée par le droit*, 3e ed., Paris Economica-Presses universitaires d'Aix-Marseille, 1995, no. 134.

La doctrine s'est attachée à décrire le cercle de la vie privée en rapport avec la vie publique[22]. Une jurisprudence abondante examine les critères permettant de déterminer si l'on se trouve dans une situation publique ou privée[23]. Ainsi, lorsque l'on s'engage dans une activité publique, on sort du champ de sa vie privée. On ne peut, sans ignorer l'existence de la liberté d'expression revendiquer la protection de la vie privée allant jusqu 'à conférer un droit de veto sur l'information relevant de la vie publique. Par exemple, on ne peut à la fois se présenter comme un vendeur fiable sur un site d'enchères en ligne et s'opposer à ce que les autres fassent part de leur expérience lorsqu'ils ont transigé avec nous[24].

On peut aussi relever qu'il existe des situations qui, sans se rattacher à la vie publique, supposent un intérêt à connaître pour un tiers. Par exemple, le droit à l'intimité peut être balisé par le droit des enfants à connaître leurs origines ; ce qui peut aller jusqu'à connaître l'identité de leurs parents biologiques. L'employeur peut, en raison des impératifs de l'emploi, avoir un intérêt légitime à connaître certaines informations relevant autrement de la vie privée d'un employé. Mais pour les personnes situées en dehors du cercle parental ou de la relation d'emploi, l'information demeure confidentielle.

La variation dans le caractère public ou privé d'une information peut découler des choix que fait l'individu. Ces choix peuvent différer selon les personnes et selon les contextes. Par exemple, on pourra trouver normal de se confier à un ami intime d'avantage qu'à son employeur ! Ces phénomènes expliquent qu'une information peut légitimement circuler dans un cercle familial ou un cercle d'amis ou un milieu de travail alors qu'elle sera tenue pour une intrusion dans la vie privée lorsqu'elle circule auprès de personnes appartenant à un cercle plus large.

Sur Internet, il est possible de rendre disponibles certains renseignements à certaines personnes mais pas à d'autres. Par exemple, dans les sites dits de « réseautage social » diverses fonctionnalités permettent d'autoriser différents niveaux de divulgation des renseignements que l'on choisit de consigner sur son espace personnel.[25]

Le champ de la vie privée peut être représenté comme étant constitué en espaces publics, semi-publics et semi-privés. Cela reflète la diversité des cercles de partage d'information associés à chacun des milieux de vie comme le cercle familial ou ceux découlant du milieu de travail ou

---

22 Voir notamment : Frederick SCHAUER, « Internet Privacy and the Public-Private Distinction », [1998] 38 Jurimetrics, 555-564 ; Daniel SOLOVE, Marc ROTENBERG & Paul M. SCHWARTZ, *Information Privacy Law,* 2d ed. 2006 ; François RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, Paris LGDJ, 1990 ; Emmanuel DREYER, « Le respect de la vir privée, objet d'un droit fondamental, *Communication commerce électronique*, mai 2005, pp. 21-26.

23 Cette jurisprudence est analysée en droit français par Pierre KAYSER, *La protection de la vie privée par le droit*, 3e ed., Paris Economica-Presses universitaires d'Aix-Marseille, 1995 ; Voir aussi : Nathalie MALLET-POUJOL, « Vie privée et droit à l'image : les franchises de l'histoire », *Légicom*, 1994/4, 51.

24 Bob RIETJENS, « Trust and Reputation on eBay : Towards a Legal Framework for Feedback Intermediaries », (2006) vol. 15, no. 1, *Information & Communications Technology Law* 55.

25 Alain LEFEBVRE. « Guide pratique des réseaux sociaux virtuels », In *Place des réseaux*, [En ligne]. http://www.placedesreseaux.com/dossiers/reseau-relationnel/reseaux-sociaux-virtuels-sommaire.htm, (Page consultée le 23 mai 2007)

professionnel. Dans ces cercles, on observe une intensité variable du caractère privé et public de l'information.

La délimitation de la vie privée résulte aussi de la présence de cercles d'informations découlant des évènements ponctuels. Les personnes, même si elles exercent aucune charge publique, peuvent se retrouver dans l'espace public à l'occasion d'évènements ayant un caractère public.

La portée du droit à la vie privée est ainsi fonction de la détermination de l'intérêt qui peut exister à la divulgation. On va se demander à quelle fin et pour servir quels intérêts fait-on la divulgation. On postule que la seule existence d'une information n'est pas en soi suffisante pour en rendre la diffusion licite. C'est dire l'importance que prennent les processus de détermination de ce qui est tenu pour correspondre à l'intérêt à connaître. De ces processus, découle l'ampleur qui sera respectivement donnée au droit à la vie privée et au droit de divulguer.

La variabilité de l'intensité du caractère privé de certaines informations doit se refléter dans les résultats produits par les outils de recherche. Cela suppose des règles réduisant la visibilité de certaines informations en fonction de l'intensité de leur rattachement à la sphère privée des individus.

1.2 La diversité des cercles d'intimité sur Internet

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, nommés « social networking websites » en anglais, permettent la rencontre et la mise en relation de personnes via leurs réseaux sociaux. Des sites tels *MySpace* (http://www.myspace.com) et *LinkedIn* (http://www.linkedin.com/) 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, faire connaître des groupes musicaux, mettre en relation avec des gens qui partagent les mêmes intérêts, 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 contacts d'une adresse de courriel déjà existante dans le but d'envoyer à toutes ces personnes des courriels d'invitation. Si les personnes concernées se joignent au site, elles apporteront à leur tour leurs contacts et le réseau grandit de cette façon.

Ces cercles différenciés d'intimité sont diversement protégés par des barrières techniques, des protections *a priori*, etc.. Mais l'existence de ce type d'activités dans lesquelles les usagers

décident de consigner certaines informations personnelles donne à penser qu'il est nécessaire de poser la prémisse qu'il existe sur Internet, à côté des informations relevant de la vie intime de chacun, des informations relevant de la vie collective. Par contraste : ce qu'on fait sur Internet, les données de connexion et les mots-clés que l'on a utilisés sont *a priori* privés et en général n'ont aucunement vocation à devenir publics.

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[26]. 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. Ce phénomène appelle une gestion des risques qui s'opère forcément en réseau.

2. La gestion réseautique des risques

L'encadrement normatif d'Internet peut s'envisager dans le contexte des risques que la technologie paraît induire. La régulation d'Internet se présente comme un ensemble de décisions de gestion des risques qui sont perçus par les acteurs au sein du réseau.

L'espace auquel on a affaire est un ensemble interconnecté constitué de pôles interagissants de normativités. Il est constitué d'espaces dans lesquels prévalent en tout ou en partie des normes qui s'imposent aux usagers. Un ensemble de systèmes de normes se discutent et s'appliquent dans le cyberespace. Aux réglementations étatiques et des acteurs s'ajoutent des processus ayant vocation à procurer les encadrements pour des activités qui ne peuvent être entièrement régies par les droits territoriaux. La technique et les contraintes qu'elle induit est aussi source de normativité dans les réseaux.

L'ensemble des normativités agissantes sur Internet peut être représenté selon un modèle réseautique. Les activités se déroulant sur Internet sont ainsi encadrées par une normativité en réseau dont le caractère effectif est largement fonction de la capacité des producteurs de normes à créer des risques suffisants pour les autres entités afin de motiver chez les autres acteurs une volonté de les gérer. Tout se passe comme si le réseau était un vaste lieu au sein duquel les acteurs gèrent les risques qu'ils perçoivent en produisant ou en relayant des obligations à ceux avec lesquels ils viennent virtuellement en contact.

Le risque en tant que construction sociale sera apprécié de façon différente selon les époques et selon le contexte culturel, politique ou social[27]. Les représentations des dangers et des bienfaits des technologies contribuent à la construction des perceptions collectives des risques et des bénéfices des objets techniques. Ces perceptions varient dans le temps : elles ne sont pas identiques à toutes les époques. Elles diffèrent également selon les contextes sociaux : le droit et

---

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

27 Christine NOIVILLE, *Du bon gouvernement des risques*, Paris PUF, les voies du droit, 235 p.

les autres normativités procèdent en grande partie de ces perceptions variables reflétant les contextes sociétaux et historiques.

Les acteurs d'Internet évaluent les risques qu'une mesure ou une règle s'applique à leur activité. La décision de se conformer à telle règle et pas à d'autres procède d'une démarche d'évaluation des risques juridiques. Le potentiel d'application du droit de tel ordre juridique est évalué par chacun des acteurs en fonction de divers facteurs. tels que les possibilités effectives de poursuites, la possession d'actifs sur le territoire étatique concerné, le désir d'inspirer confiance ou de se comporter en « bon citoyen ». Ces facteurs concourent aux analyses par lesquelles les acteurs orientent leurs stratégies de gestion de risques.

2.1 Le risque

Internet est un environnement entièrement 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. La régulation d'Internet trouve une grande partie de ses justifications dans les risques perçus à l'égard de ce que peut causer son utilisation mal encadrée. Maryse Deguergue relève que le risque peut être classé parmi les notions axiologiques qui traduisent le réel tout en portant sur lui un jugement de valeur, lequel permet de poser des règles juridiques[28]. Dans l'environnement en réseau, le risque concerne aussi bien le péril justifiant la mise en place de la norme elle-même que les sanctions et autres contraintes qu'engendre cette dernière. C'est la normativité qui crée, accentue, réduit ou transfère les risques. Les risques à gérer sont à ce titre des risques juridiques.

Les perceptions diverses ou convergentes au sujet des risques d'Internet contribuent à construire les légitimations sur lesquelles se fondent les règles de droit qui prétendent en encadrer le fonctionnement. L'anticipation, la gestion et la répartition des risques figurent parmi les grandes préoccupations des systèmes juridiques. Ulrich Beck explique que :

> *La société moderne s'est transformée en société du risque (…) parce que le fait de discuter des risques que la société produit elle-même, le fait de les anticiper et de les gérer est progressivement devenu l'une de ses principales préoccupations*.[29]

La normativité relative à Internet est en grande partie motivée par le souci de réduire, gérer et répartir les risques découlant de la disponibilité d'informations sur le réseau. Dans son acception générale, le risque peut être envisagé comme un objet social. Yvette Veyret observe que « le risque objet social se définit comme la perception du danger. Le risque n'existe que par rapport à un individu, à un groupe social ou professionnel, une communauté, une société qui l'appréhende […] et le traite par des pratiques spécifiques. Il n'y a pas de risque sans une population ou un

---

28 Maryse DEGUERGUE, « Risque » dans Denis ALLAND et Stéphane RIALS, *Dictionnaire de la culture juridique*, Paris, Quadridge, Lamy, PUF, 2003, p.1372.

29 Ulrich BECK, « Risque et société » dans Sylvie MESURE et Patrick SAVIDAN, *Le dictionnaire des sciences humaines*, Paris, Quadrige, PUF, dicos poche, 2006, p. 1022.

individu qui perçoit et pourrait subir ses effets »[30]. Le risque n'existe pas dans le vide : il découle forcément d'un contexte sociétal donné.

La protection des informations faisant partie de la vie privée relève bien d'une logique de gestion de risques. Les conséquences de la circulation des informations ne sont pas nécessairement connues des protagonistes lorsque l'information est mise en circulation. C'est souvent l'agglomération d'informations qui est considérée comme porteuse de dangers. Par exemple, une information personnelle anodine peut être diffusée puis se retrouver combinée avec un autre élément d'information et entraîner de ce fait une divulgation d'un élément de l'intimité d'une personne. Dans une pareille situation, l'intéressé a consenti à la divulgation ou encore le caractère public de la situation faisait sortir l'information du champ de la vie privée. Mais l'intrusion dans la vie privée survient quand même.

Une fois reconnu, le risque emporte des obligations de précautions. Le risque juridique découle en effet des situations où la 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. Le risque juridique, en toute hypothèse, résulte des situations dans lesquelles la responsabilité d'une personne peut être mise en cause.

Ceux qui prennent part à des activités dans le cyberespace 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. La régulation des outils de recherche sur Internet s'inscrit dans le tissu des impératifs de modulation et de gestion des risques.

2.2 Le changement de l'échelle des risques

Les outils de recherche contribuent à modifier les repères spatiaux et temporels. Ils 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[31]. Le *Rapport sur l'application transfrontière de la législation relative à la vie privée* de l'OCDE relève que la circulation accrue de l'information notamment sur Internet accroît les risques pour la vie privée. On ajoute que :

> *La multiplication des flux transfrontières de données, à des débits plus élevés, couvrant des zones géographiques plus étendues, et englobant des données alphanumériques, de la voix et des images entre une multiplicité croissante d'acteurs est susceptible d'augmenter le nombre et le coût des violations de la vie privée subies par les individus et les organisations.*[32]

---

30 Yvette VEYRET, « Les risques », *Dossier des images économiques du monde*, FEDES, cité par Franck VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, p. 11.

31 Frederick SCHAUER, « Internet Privacy and the Public-Private Distinction », [1998] 38 *Jurimetrics* 555 ;

32 OCDE, *Rapport sur l'application transfrontière de la législation relative à la vie privée,* Paris, OCDE, 2006, p. 8, < http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119666_1_1_1,00.html >.

Les risques pour la dignité humaine se présentent à des échelles différentes. Il y a reconstruction des cercles de la vie privée. Il y a décentrage et recentrage des cercles de la vie privée.

On observe un décentrage spatial : l'espace physique semble se dissoudre dans le cyberespace : le lieu dans lequel est située l'information a désormais peu d'impact sur son accessibilité. Dès lors qu'un document est disponible sur un serveur, les outils de recherche couramment utilisés sur Internet ou certains outils spécialisés sont en mesure de le retrouver. L'éloignement dans l'espace de même que le passage du temps semblent avoir beaucoup moins de prise sur la disponibilité effective de l'information.

Internet banalise la diffusion : l'information peut aisément se trouver à être diffusée en dehors des cercles de circulation légitime ; d'où l'accroissement des risques. Certes, le cyberespace est constitué de lieux publics et de lieux privés. Mais les repères permettant de délimiter le privé du public sont brouillés. Belgum rappelle que :

Personal data, such as address, phone number, income, poperty value, and marital status have always been avalable to those willing to dig. The Internet can make it possible for a much wider class of persons – essentially all internet users – to gain access to similar types of personal information at little or no cost.[33]

Internet modifie l'échelle spatiale à partir de laquelle s'apprécient les risques pour la vie privée. En dehors du monde en réseaux, l'accessibilité à une information demande 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. Solove observe que :

> *Until recently, public records were difficult to access. For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records. But with Internet revolution, public records can be easily obtained and searched from anywhere.*[34]

La problématique de l'accès aux documents rendant compte du déroulement des processus judiciaires est emblématique des changements quantitatifs et qualitatifs générés par Internet. Natale M. Gome-Velez relève que :

> *Providing Internet access to court records increases exponentially the availibility of court records, including any sensitive information they contain. Examples of sensitive informaion that might be found in court records include : social security numbers, home addresses, names of minor children financial account numbers, and medical information.*[35]

---

33 Karl D. BELGUM, « Who leads at Half-time ?: Three Conflicting Visions of Internet Privacy Policy [1999] 6 *Rich. J.L. & Tech*. 1.

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

35 Natalie M. GOMEZ-VELEZ, « Internet Access to Court Reports- Balancing Public Access and Privacy, » [2005] 51 *Loyola L.Rev*., 365-438, p. 371.

Il y a aussi décentrage temporel : la persistance de l'information emporte que celle-ci traverse les cercles dans lesquelles elle était tenue pour légitime. Par exemple, une information peut être légitimement disponible au public en raison de l'actualité de l'événement. L'archivage et la disponibilité virtuellement permanente sur Internet irait au-delà de ce qui est nécessaire afin de rendre compte de l'actualité.

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. En somme la disparition des efforts à consacrer pour trouver l'information emporte la disparition d'une protection par défaut pour la vie privée. Cela porte à revoir les raisonnements qui permettaient de déterminer si on se trouvait dans le domaine de la vie privée ou dans le domaine de l'espace public.

Tous ces changements dans les dimensions des enjeux relatifs à la vie privée indiquent des modifications dans les niveaux de risques causés par la circulation de l'information dans le réseau. Ces dimensionnements nouveaux des risques pour la vie privée induisent des mutations au niveau de la raison d'être des règles de droit. Là où l'on prenait pour acquis que le niveau de risques pour la vie privée demeurait faible ou aisément maîtrisé, les mutations dans l 'échelle qualitative et temporelle qu'induit la généralisation d'Internet, conduit à postuler que les risques sont accrus. D'où les revendications pour un renforcement de la protection de la vie privée des personnes lors de la mise en place des environnements de traitement de l'information.

Mais un tel renforcement doit se concevoir dans le contexte d'une normativité en réseau.

2.3 La normativité en réseau

La gestion des risques s'inscrit dans un processus de régulation en réseau[36]. Les réseaux sont le résultat d'interactions entre personnes se trouvant en relation. Le phénomène de réseautage suppose des environnements interconnectés unissant les acteurs, les régulateurs de même que les entités jouant un rôle dans la gouvernance d'Internet[37]. Dans les espaces constitués par les réseaux, le cyberespace, la normativité s'élabore et s'applique selon un mode réseautique[38]. Renaud Berthou voit en Internet « un facteur de développement d'une pluralité de processus

---

36 Katherine J. STRANDBURG, Gabor CSARDI, Jan TOBOCHNIK, Peter ÉRDI & Laszlo ZALANYI, « Law and the Science of Networks : An Overview and an Application to the 'Patent Explosion' », [2006] 21 *Berkeley Technology L.J.*, 1293-1351 ; Andrea M. MATWYSHYN, « Of Nodes and Power Laws : A Network Theory Approach to Internet Jurisdiction through Data Privacy », (2003) 98 *Nw.U.L.Rev.*, 494-544 ; Avitai AVIRAM, « Regulation by Networks », [2003] *Brigham Young U. L.Rev.*, 1180-1238 ; Lior Jacob STRAHILEVITZ, « Asocial Networks Theory of Privacy », [2005] 72 *U. Chi.L.Rev.*, 919-988.

37 Manuel CASTELLS, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998; François OST et Michel de KERCHOVE, *De la pyramide au réseau : pour une théorie dialectique du droit*, Bruxelles, Publications des facultés universitaires Saint-Louis, 2002.

38 Pierre TRUDEL, « Un 'droit en réseau ' pour le réseau : le contrôle des communications et la responsabilité sur internet, » dans INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne : Éthique et mondialisation,* Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

réseautiques ». Sans être la seule cause du développement réseautique que connaissent les processus de création du droit à l'ère postmoderne, il est un outil majeur d'évolution[39].

Au sein du réseau, l'acteur gère ses risques et va chercher à les limiter ou les transférer à un partenaire. Par exemple, l'exploitant d'un site de réseautage social va prévoir des mises en garde afin d'amener les usagers à accepter consciemment les risques découlant de la mise en ligne de leur profil personnel. D'autres acteurs pourront songer à mettre en place des mécanismes afin de consigner les consentements aux traitements de données personnelles aux fins de limiter leurs risques résultant de l'application des lois nationales sur la protection des données personnelles qui seraient susceptibles de trouver application à leurs activités.

Les régulations peuvent découler de normativités technologiques, de normativités gestionnaires ou de normativités juridiques. Rien n'indique que la normativité juridique ou une autre logique normative soit invariablement en position dominante. Il y a en effet concurrence entre les diverses logiques en vertu desquelles se produisent les régulations : les logiques technologiques, celles du marché et les logiques du droit ne concordent pas toujours. Dans certaines situations, les référents juridiques demeurent absents des débats qui sont perçus comme relevant essentiellement d'une problématique de gestion ou d'agencement technique. Dans d'autres contextes, l'enjeu technique est fortement capté par les logiques juridiques.

L'État ou un autre acteur 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 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 des acteurs. Si dans le cyberespace, l'État semble avoir perdu de son pouvoir, il conserve habituellement encore une importante influence sur les entités situés sur son territoire et même sur ceux qui sont susceptibles d'être indirectement visés par ses lois.

Dans un réseau, chacun des acteurs en mesure d'imposer sa volonté dispose 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.

En somme, le système de régulation vise à rétablir les équilibres entre les risques et les précautions. Il doit fonctionner de façon à inciter l'ensemble des acteurs à minimiser les risques qui relèvent de situations sur lesquelles ils sont effectivement en mesure d'avoir une prise, et à accroître le plus possible les risques des acteurs qui choisissent d'avoir des comportements dommageables ou qui augmentent indûment les risques des usagers légitimes. C'est dans une telle logique que s'inscrit la régulation des outils de recherche.

---

39 Renaud BERTHOU, *L'évolution de la création du droit engendrée par Internet : vers un rôle de guide structurel pour l'ordre juridique européen*, Thèse pour le doctorat de l'Université de Rennes I, mention Droit, Rennes, 2 juillet 2004, p. 373.

2.3.1 Les relations multiples entre les normativités

Internet peut être envisagé comme un univers constitué de nœuds et de relais de normativité qui sont en lien d'interinfluence. L'enjeu n'est pas de savoir si c'est la loi, la technique ou l'autoréglementation qui assure le mieux la protection des équilibres. La normativité effective est une résultante du dialogue entre les acteurs et de leur capacité à relayer les normes et principes. Pour connaître les normes qui ont vocation à régir un environnement raccordé à Internet, il faut identifier les nœuds au sein desquels s'énonce la normativité qui s'applique effectivement[40]. Par exemple, un État énonce des lois qui seront obligatoires pour ceux qui sont situés sur son territoire.

Ainsi, une stratégie d'encadrement des activités d'Internet comme les moteurs de recherche s'envisage comme un ensemble de mesures conçues de manière à se renforcer les unes et les autres afin de limiter les risques tels que ceux relatifs à la vie privée des internautes qui s'adonnent à des activités licites. La stratégie doit se déployer en réseau : imposer des règles aux acteurs et inciter ces derniers à relayer ces exigences à tous ceux à l'égard desquels ils exercent une influence.

Dans une logique de gestion de risques, les mesures étatiques seront plus efficaces si elles sont assorties de politiques dynamiques de surveillance et de poursuites dans les cas où cela est possible. Une législation notoirement innappliquée pourra plus aisément être perçue par les acteurs comme engendrant moins de risques.

Pour les acteurs dans le cyberespace, le droit énoncé et appliqué par les États fournit une part importante du cadre délimitant leurs actions et prescrivant l'étendue de leurs obligations. C'est pour gérer leurs risques et limiter la mise en cause possible de leur responsabilité que les acteurs, tant collectifs qu'individuels, se donnent des règles de conduite. Ainsi, se relaient les exigences énoncées dans les pôles de normativité. Au niveau de chaque environnement, les principes énoncés dans les pôles de normativité comme les lois des États et les principes largement reconnus sont relayés en micro régulation ou en auto réglementation.

La structure en réseau du droit du cyberespace permet de rendre compte des relations multiples qui existent entre les différents ordres normatifs agissant sur le net. Le paradigme de la gestion du risque procure une hypothèse explicative au regard de l'effectivité des normes. L'effectivité des règles serait fonction de leur capacité à promouvoir une gestion optimale du risque qu'elles permettent aux acteurs de visibiliser. Le risque concernant ici aussi bien le péril justifiant la mise en place de la norme elle-même que les sanctions et autres contraintes qu'engendre cette dernière.

Les moteurs de recherche, par leurs façons de faire, leurs modes de fonctionnement ou les outils techniques utilisés peuvent accroître ou limiter les risques des internautes. À ce titre, ils mettent en place une normativité « par défaut » qui est d'application immédiate. Une telle normativité est forcment porteuse de risque pour les usagers.

---

40 Pierre TRUDEL, « Un 'droit en réseau' pour le réseau : le contrôle des communications et la responsabilité sur Internet », dans INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne : Éthique et mondialisation,* Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

De leur côté les usagers ont à gérer les risques découlant de la normativité accompagnant le fonctionnement des outils de recherche.

Les États sont en mesure d'intervenir dans les processus de gestion des risques inhérents aux environnements d'Internet comme les outils de recherche. La réglementation étatique peut moduler les risques : par exemple rendre obligatoire la divulgation des risques découlant des fonctions des outils de recherche. Les législations peuvent également interdire la collecte ou la conservation de données. À l'inverse, les États peuvent augmenter les risques en imposant des obligations de conservation de données afin que celles-ci demeurent disponibles aux forces de police.

2.3.2 Les normes sont proposées, imposées et relayées

Dans le réseau, on observe des interrelations diversifiées entre les normes. Les normes sont proposées voire imposées dans divers nœuds de normativité; ces nœuds de normativité sont en concurrence ou en complémentarité avec d'autres. Les relais de la normativité assurent l'application effective des règles. Dans les relais s'explicitent et se diffusent les normativités et les conséquences de celles-ci.

On peut identifier plusieurs rapports entre les normativités. Dans la plupart des situations, on se trouvera en présence d'un rapport d'obligation : une loi est obligatoire à l'égard d'une personne située sur le territoire d'un État : cette dernière – au risque de devoir subir des sanctions - doit forcément relayer les obligations découlant de la loi. On voit ici l'importance du risque découlant de l'effectivité de la loi. Une loi non appliquée par les autorités pourra être perçue comme engendrant un risque négligeable. C'est dire l'importance de limiter la quantité de lois à ce qu'on est en mesure d'appliquer effectivement. La multiplication des textes ne visant que des effets d'annonce sans les ressources assurant l'effectivité de son application contribue à affaiblir l'efficacité de la loi étatique.

Dans d'autres situations, l'application indirecte de normes émanant en tout ou en partie d'autres ordres juridiques sera envisagée comme un risque. Par exemple, les directives européennes ont des effets non seulement sur le droit des pays membres mais aussi sur les obligations des acteurs situés dans des pays entretenant des relations importantes avec les ressortissants de cette entité. Il en est de même des lois américaines : plusieurs sites exploités partout dans le monde considèrent qu'il est de bonne pratique de se conformer à certaines lois américaines puisqu'ils ambitionnent de rejoindre des ressortissants de ce pays.

En fin de compte, lorsqu'on s'engage dans une activité sur Internet, il faut habituellement envisager les risques de possible non-conformité à une gamme étendue de normes. Si les lois du territoire sur lequel on se trouve s'imposent d'office, on peut aussi avoir à composer avec des règles, légales, techniques ou des pratiques qui émanent d'un vaste ensemble de lieux normatifs engendrant plus ou moins de risques juridiques.

Conclusion

La question des limites à la « googleisation » des personnes peut être envisagée selon un modèle de gestion des risques. Sur Internet, l'usager gère ses risques : il les accepte ou les transfère, il peut choisir de les limiter ou de les minimiser.

La portée et la teneur effective des réglementations balisant la collecte et l'utilisation des données par les outils de recherche sont la résultante des décisions de gestion des risques. Les usagers et autres acteurs ont à décider s'ils acceptent les risques pour la vie privée ou le cas échéant comment ils les transfèrent. 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 net, 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.

L'approche selon le modèle du risque indique que la question n'est pas tellement de savoir si la Loi ou l'autoréglementation devrait être utilisée dans le cadre de stratégies de régulation comme si l'un excluait l'autre. Au contraire, comprise comme un ensemble de risques à gérer, la régulation d'Internet se comprend comme un ensemble de normes qui 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.

La normativité issue de la technique peut engendrer des risques ou procurer des solutions en limitant l'incidence. L'État et les autres régulateurs peuvent accroître ou limiter les risques tels que ceux qui découlent des activités d'une entité telle Google. 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 la vie privée. Sur Internet, ces mesures seront à leur tour généralement perçues par les acteurs comme autant des risques à gérer et à transférer aux cocontractants.

Sur Internet, la régulation s'élabore et s'applique selon un mode réseautique. Les acteurs sont en mesure d'accroître, de transférer ou de limiter les risques. L'efficacité de la régulation est fonction de la capacité effective d'accroître les risques de ceux qui mènent des activités à risque et à gérer les risques des utilisateurs légitimes. Plus on comprend les relations qui existent entre ces divers processus de gestion de risques, plus on accroît les chances d'une régulation effective des activités qui engendrent des risques sur Internet.