Travail de session

Présenté à

Me Vincent Gautrais

De l'urgence d'un cadre juridique international du cyberespace

de

Michel Leblanc

En ce 3 octobre 2001

Table des matières

Introduction

Je suis d'emblée convaincu de la pertinence d'un débat sur l'appropriation législative, exécutive et judiciaire effective et permanente de l'espace cybernétique par une agence gouvernementale de l'ONU à être créé spécifiquement pour ce besoin.

Pour alimenter ce débat je vous propose une réflexion sur des facteurs incitatifs à l'action. Je vous parlerai donc des conditions démontrant l'urgence du débat. Ces conditions découlent du contexte sociopolitique particulier dans lequel nous nous trouvons. À savoir, le climat de paranoïa résultant de l'acte de guerre qu'a subit l'Amérique ce 11 septembre, les iniquités du ¨digital divide¨, la confiance des consommateurs et la régulation de facto que nous subissons présentement. Je vous présenterai aussi des arguments de structures et de compétences. Je survolerai les arguments en défaveur d'un tel débat et je vous résumerai pourquoi il y va de la préservation de nos acquis en matière de liberté civile de confié notre web à l'ONU.

1. Contexte sociopolitique

a. La Paranoïa

Le terrible choc du 11 septembre dernier nous a tous plongé dans un état de stupéfaction total. La tristesse et l'incompréhension ont vite cédé la place à la mise sur pied d'une stratégie globale de renforcement des mesures de sécurité étatique. La protection du territoire américain voire continental et occidental de même que la recherche de coupables, la guerre contre le terrorisme qui s'engage et la prévention d'autres actes de terrorisme d'état poussent le gouvernement américain à réagir avec vigueur et fermeté. La liste des interventions de même que les méthodes qui seront utilisées pour soutenir et gagner cette guerre ne nous sont pas encore connues. Cependant un certain nombre d'événements nous confrontent à la fragilité des acquis quant à la libre circulation des informations sur internet. Le gouvernement américain dans sa légitimité de légiférer sur son territoire entraîne de facto le monde dans sa vision des choses et inflige à celui-ci les mesures qu'il aura choisi d'édicter. Cela entraîne inévitablement des conséquences majeures sur l'état du droit privé international.

En effet depuis le 11 septembre 2001 le FBI peut enregistrer les communications sur Internet. Le FBI a déjà installé des logiciels ¨carnivores ¨ sur les serveurs d'AOL, Earthlink et Hotmail. Mon Hotmail est sur écoute! ¨Ceux qui n'ont rien à cacher n'ont rien à craindre ¨, peut-on déjà entendre. Mais qu'en est-il de notre droit à la vie privée?

Internet privacy threatened by the war against terrorism
According to information obtained by RSF, the US Senate passed a law, on 13 September 2001, allowing the Federal Bureau of Investigation (FBI) to install e-mail monitoring software on ISPs for 48 hours without requiring a court order. The Senate passed this law, the "Combating Terrorism Act", after debating it for a half hour.

During the debate on the Senate floor, Democratic senator Patrick Leahy opposed the Combating Terrorism Act in the name of the defense of individual liberties. "We are going to [vote on this bill] with no hearings, no debate," he said in anger, after pointing out the seriousness of the changes this law would bring about. On 17 September, Attorney General John Ashcroft asked that measures to reinforce the powers of the Justice Department in the fight against terrorism be taken as soon as possible.

The Combating Terrorism Act is actually an amendment to bill H.R. 2500, dealing with appropriations for the Departments of Commerce, Justice and State, approved by the House of Representatives in July 2001. A joint conference committee, made up of senators and representatives, was set up to select the amendments to the final bill that will be presented in the two houses. This committee will present the definitive bill to Congress at the end of this week or the beginning of next week.

RSF points out that, on 11 September 2001, just a few hours after the attack, FBI agents went to offices of the ISPs AOL, Earthlink and Hotmail to install the Carnivore program on their servers. This program is used to intercept e-mail messages. The goal of the visits was to search for any traces that might have been left by the perpetrators of the attacks.

Many American civil liberties organizations fear that the fight against terrorism may lead authorities to prohibit encryption, which allows Internet users to guarantee the confidentiality of their e-mail messages.[1]

Le Combating Terrorism act dont il est question est pratiquement identique quant à ces énoncés sur l'écoute électronique qu'un autre projet de lois qui est présentement à l'étude. Il s'agit de : "Anti-Terrorism Act of 2001." Cette loi n'est pas encore active mais on peut supposer qu'elle sera adoptée pratiquement sans opposition. Cette législation donne aux juges américains des pouvoirs de contrôle et d'écoute sur les réseaux, les serveurs et les lignes téléphoniques sans précédent dans l'histoire américaine. Voici d'ailleurs quelques passages de cette lois.

[1] http://www.rsf.fr/uk/homennemis.html

Subtitle A--Electronic Surveillance

SEC. 101. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(…)

"(a) IN GENERAL- (1) Upon an application made under section 3122(a)(1), the court shall enter an ex-parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order shall, upon service thereof, apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.

(…)

"(2) Upon an application made under section 3122(a)(2), the court shall enter an ex-parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law-enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.".

(…)

"(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and".[2]

---

[2] H.R.2500
Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2002. (Engrossed Senate Amendment)
THOMAS -- U.S. Congress on the Internet

Nous pouvons comprendre à ces textes juridiques l'ampleur des moyens qui sont mis à la disposition des procureurs du gouvernement et des agences de renseignement et de polices qu'ils représentent. Ce nouvel outil d'analyse et de surveillance des communications sous quelle que forme qu'elle soit est sûrement justifié étant donné l'ampleur de la tâche antiterroriste. Cependant il serait bon de se demander, si une fois la ou les menaces jugées sous contrôle, le législateur reviendra en arrière pour rétablir les acquis de protection de la vie privée?

Un autre phénomène d'écoute et d'enregistrement électronique a fait couler beaucoup d'encre. Il s'agit du programme échelon.

ECHELON is the term popularly used for an automated global interception and relay system operated by the intelligence agencies in five nations: the United States, the United Kingdom, Canada, Australia and New Zealand (it is believed that ECHELON is the code name for the portion of the system that intercepts satellite-based communications). While the United States National Security Agency (NSA) takes the lead, ECHELON works in conjunction with other intelligence agencies, including the Australian Defence Signals Directorate (DSD). It is believed that ECHELON also works with Britain's Government Communications Headquarters (GCHQ) and the agencies of other allies of the United States, pursuant to various treaties.[3]

Chaque nation peut débattre de l'importance du respect de la vie privée. Elles peuvent aussi dans leurs constitutions et autres documents législatifs offrir un cadre de protection et d'enchâssement de ces droits. Mais comment un gouvernement national peut-il garantir à ces citoyens la confidentialité d'un message transitant sur AOL, sur le territoire américain ou sous le rayonnement d'échelon?

D'ailleurs Lessig dans *The Laws of cyberspace*[4] a longuement discouru sur l'utilisation de l'architecture comme moyen de contrôle étatique; il nous mettait en garde contre la propension de son gouvernement à vouloir l'utiliser comme outil régulateur du cyberespace ; il nous mettait

[3] Echelon Watch | FAQ <http://www.aclu.org/echelonwatch/faq.html>

[4] http://cyberlaw.stanford.edu/lessig/content/works/laws_cyberspace.pdf

aussi en garde contre le monopole de son gouvernement sur ces moyens de contrôles et sur l'exportation probable de ceux-ci. Il nous parlait aussi de deux architectures l'une ouverte et l'autre contrôlée.

These two architectures reflect two philosophies about access. They reflect two sets of principles, or values, about how speech should be controlled. They parallel, I want to argue, the difference between political regimes of freedom, and political regimes of control. They track the difference in ideology between West and East Germany; between the United States and the former Soviet Republic; between the Republic of China, and Mainland China. They stand for a difference between control and freedom - and they manifest this difference through the architecture or design of code. These architectures enable political values. They are in this sense political. Now I don't offer this example to criticize Harvard. Harvard is a private institution; it is free, in a free society, to allocate its resources however it wishes. My point instead is simply to get you to see how architectures are many, and therefore how the choice of one is political. And how, at the level of a nation, architecture is inherently political. In the world of cyberspace, the selection of an architecture is as important as the choice of a constitution. For in a fundamental sense, the code of cyberspace is its constitution. It sets the terms upon which people get access; it sets the rules; it controls their behaviour. In this sense, it is its own sovereignty. An alternative sovereignty, competing with real space sovereigns, in the regulation of behaviour by real space citizens.

De plus, Lessig prévient contre l'absence des juristes dans le débat et il écrit :
le code constitue la Constitution d'Internet et celle-ci, laissée aux intérêts de l'argent et du gouvernement américain, a déjà amorcé un glissement dangereux menant à un espace d'identification, de surveillance et de contrôle sans précédent dans l'Histoire.[5]

Pour conclure sur cette question de l'utilisation d'instrument d'écoute et d'enregistrement ou comme je l'ai affectueusement appelé la paranoïa, je vous propose une remarque tiré du site Reporter Sans Frontière.

[5] Lawrence Lessig : étude de la paternité d'une théorie normative du Cyberespace. Stéphane DESROCHERS

Even the most sophisticated signal interception technology available will hardly be able to thwart stone age style secure channels used by terrorists, such as human couriers and confidential face-to-face meetings.[6]

b. Digital divide

Un autre facteur déterminant pouvant nous motiver à envisager l'ONU comme régulateur d'internet, est la division qui s'opère à l'échelle de la planète entre les pays branchés et non branchés. Ce que Mark Malloch Brown administrateur du Programme de développement des nations unies (UNDP) appelle le ¨ Digital divide¨. Lors d'une conférence du G-8, Brown a informé les leaders du fossé grandissant entre les pays riches et pauvres en ce qui a trait à l'accès des technologies de l'information.

"If we fail to act now the Information Gap risks being widened into an uncrossable gulf that increases global inequality and leaves the poor further behind,"[7]

Quel organisme ou structure étatique autre qu'Onusienne pourrait coordonner les efforts pour combler se vide ?

c. Confiance des consommateurs

L'un de mes confrères étudiants de droit prenait l'exemple du faible pourcentage d'échange Business to Consumer au niveau international comparativement aux échange Business to Business pour me convaincre de l'inutilité des lois internationales en ce qui a trait au cyberespace. Il me soulignait que les entreprises se servent d'internet comme d'un MatchMaker et que leurs transactions qui sont encadrées par de nombreux traités se réalisent le plus souvent par contrat

[6] http://www.fitug.de/news/pes/fitug-010918.en.html

[7] DPA- Newsfront for United Nations Development Programme

papier et hors du cadre du cyberespace. Je lui donnais raison sur son analyse de la situation. Cependant je lui faisais aussi remarquer que ce qu'il dépeignait illustrait peut-être le peu de confiance des consommateurs face aux transactions Business to Consumer. À mon avis il s'agit là du plus grand défi que nous pose le cyberespace. Soit, comment convaincre le consommateur de la sécurité des transactions et de la facilité de règlement de différends lors de tels achats. Une panoplie d'outils législatifs ont été mis de l'avant par l'ONU, et autres instances internationales de même que par certains groupes de travail et groupes de pression spécialisée. Cependant malgré tout cet attirail le potentiel économique fabuleux du commerce électronique n'est encore qu'un rêve. Nous pouvons tenter de coordonner les législations nationales potentiellement divergentes sur la base de modèles communs (comme la loi type de la CNUDCI sur le commerce électronique), la certitude de recevoir un produit acheté à l'autre bout du monde et d'avoir un recours applicable en cas de litige restera fortement hypothétique. Pouvons-nous en tant que consommateur et même en tant qu'administrateur d'entreprise connaître l'état du droit de chacune des localités d'un marchand potentiel? Je crois que les différents cadres législatifs proposés par les intervenants serviront de balises psychologiques essentielles au développement d'une structure de commerce électronique locale. Pour ce qui est d'une structure internationale je ne vois qu'une instance telle que l'ONU pour m'assurer d'une certaine homogénéité des cadres législatifs.

Plus un cadre international de droit privé d'internet prendra de temps à se structurer plus l'explosion du commerce électronique prendra de temps à se matérialiser.

d. Etre régulé de Facto

i. Monopole technologique

Comme nous l'avons vu précédemment le gouvernement américain à décider unilatéralement de mettre le cyberespace sur écoute. Lessig dans Cyberspace's Architectural Constitution nous parlait d'AOL en ces termes :
AOL is not the Internet, though half the dial-up customers in the world get access to the Internet through AOL. It has its own code, its own ability to control. And it controls which code runs on

its platform. [8]

Maintenant que nous savons que AOL est sous écoute pouvons-nous croire avoir un contrôle législatif sur nos communications qui transitent par ce site?

Microsoft, AOL, Netscape, Cisco et al sont des entreprises américaines assujetties au droit américain. Ai-je besoin de démontrer l'écrasante supériorité technologique américaine en ce qui a trait à l'informatique et internet? Ces entreprises technologiques de même que le gouvernement américain sont d'ailleurs les principaux bailleurs de fonds des différentes associations professionnelles investit de l'autorité de développer, de maintenir d'implanter et de réguler ce qu'il est maintenant convenu d'appeler ¨le code¨ d'internet¨. Vous serez d'accord avec moi que le monopole technologique américain est tout à fait déterminant dans les enjeux de régulation d'internet au niveau mondial.

ii. Monopole ¨Internet Governance¨

Parlons maintenant de ce que l'on appelle ¨l'internet governance¨ ou la gestion des noms de domaine. Une structure nouvelle a pris le contrôle de ce secteur en pleine explosion. Il s'agit de l'ICANN Me Gautrais dans sa chronique de cyber-presse nous parle de l'ICANN en ces termes :

En ce moment, le courroux des « cyberpeuples » passe par la critique acerbe de l'ICANN (Internet Corporation for Assigned Names and Numbers) qui est notamment responsable de la gestion des noms de domaine « .com », « .net » et « .org ». En tant que rare organisme centralisé, et bien que son rôle soit supposée être seulement technique, cette institution prête le flanc à la critique de tous bords.

D'abord, on lui reproche des liens privilégiés avec le gouvernement américain qui est à l'origine de sa création en 1998 et qui n'a pas brisé tous les liens, ainsi qu'avec l'industrie qui dispose de « strapontins » confortables pour faire valoir ses intérêts. Ensuite, ICANN dispose d'une structure byzantine, complexe et peu transparente. Ses élections de l'automne dernier ont en effet montré

[8] http://cyberlaw.stanford.edu/lessig/content/works/AmAcd1.pdf

un manque de maturité qui, il est vrai, n'est pas étonnant eu égard à l'ampleur de la tâche et à la nouveauté de l'institution.[9]

Un deuxième élément d'importance est associé au concept d'internet Governance. Il s'agit de DNS Domain Name System. Ce système de nom de domaine a pour fonction de relier un nom de domaine à l'adresse IP de son serveur hôte. Encore une fois le monopole américain se manifeste de manière indéniable selon Eugene Kashpureff dans une entrevue qu'il donna au magasine WIRED.

The domain-name system (DNS) connects an Internet address like ibm.com with the numerical IP address that identifies its host server. Until 1993 the number of domain-name registrants was a mere 200 to 300 per month. Today that volume has exploded to an average of more than 3,000 per day. And as the mainstream has discovered the Internet, it has seen the inevitable fallout of the virtual world colliding with the real world, of board-game manufacturer Hasbro, for instance, learning that a porn purveyor holds the domain name candyland.com. To a large extent, whoever controls the DNS - and the root server, the holy temple in which all names are housed - also controls the Internet. (…)

"As the Internet is the communications medium of the future, it is most important that we fight for our rights there," he says. And what's wrong with the domain-name system? "Lack of choice," Kashpureff replies. "The fact that the control of domain-name space still lies with the US government. Every other country in the world has to settle for their two-letter International Organization for Standardization code. The US gets to sit on and allocate a whole bunch more than that."[10]

iii. Monopole jurisprudentiel

Plusieurs magistrats de différents pays puisent dans la jurisprudence américaine pour motiver

[9] Cyberpresse | ICANN : le chef du « web »?
[10] Feature

leurs argumentations de droits. Cette tendance est particulièrement vérifiée pour les pays de common Law. La jurisprudence américaine particulièrement en ce qui a trait aux droits du cyberespace fait figure de ¨Pharmacie Jean-Coutu¨ de la jurisprudence. Le corpus législatif américain est lui-même alimenté de sa jurisprudence. Or, il appert, que de plus en plus les juristes américains se présentent en cours avec des statistiques quant aux fréquences des jugements en leur faveur versus ceux en leur défaveur. Étant donné l'influence prépondérante de l'expérience jurisprudentielle américaine comme source de nouveau droits de différents pays serait-il encore une fois opportun de se questionner sur l'importance d'établir un cadre législatif international du droit privé du cyberespace? Devrions-nous aussi nous questionner sur cette nouvelle tyrannie du sondage jurisprudentiel pour guider nos décisions?

iv. Monopole économique, géopolitique

Cette section se passe de démonstration. Nous savons tous l'influence économique, politique, stratégique, militaire et j'en passe des Américains. Devons-nous en plus de subir ses divers monopoles aussi subir ses diktats dans le cyberespace sans nous prononcer? Je crainds qu'il ne soit déjà trop tard et que par faute d'avoir globalement pensé et mis sur pied une structure législative réellement supranationale nous n'ayons à vivre par défaut celle des Américains.

e. Sauvons les meubles

Je suis d'avis qu'à défaut de pouvoir mettre sur pied des structures supranationales, il faut le plus rapidement possible légiférer au niveau local pour pouvoir avoir un cyberespace national sous notre pleine juridiction. Nous pourrons aussi à l'aide de ces législations locales telles que la Loi concernant le cadre juridique des technologies de l'information (Assemblée Nationale du Québec) permettre un essor considérable de notre commerce électronique national. Le sentiment d'urgence au niveau local se fait plus sentir en termes psychologiques que juridiques. Je crois que les lois ayant pour but d'encadrer internet favoriseront la confiance des consommateurs et des investisseurs dans la pertinence du commerce électronique. J'ajouterai aussi qu'une économie numérique locale forte et dynamique sera le plus sûr rempart contre l'envahissement américain.

Me Ejan Mackaay lors d'une allocution à l'Université de ParisII-Assas :
Dans l'ensemble, il paraît permis de conclure que le droit commun, à condition d'en voir la dynamique et de lui laisser le temps de s'accomplir, comporte bien les ressorts requis pour faire face aux défis de l'Internet. Les appels à l'intervention réglementaire paraissent prématurés.[11]

Je suis de l'avis de Me Ejan Mackaay à l'effet que le nouveau droit peut très bien s'en tirer sans l'intervention de l'état. C'est pour la dimension du contexte psychologique favorable au commerce que je m'inquiète. Par contre, à l'encontre de Me Mackaay, je me questionne sur la pertinence de la charte des droits et libertés pour me protéger du viol de mon Hotmail ? Je me demande de plus si une quelconque intervention réglementaire pourrait y faire quelque chose.

2. Arguments de structures et de compétences

a. Compétences juridictionnelles

L'OCDE[12] dans ses recommandations du conseil relatives aux lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique, termine en insistant sur la nécessité de la coopération internationale et insiste sur le besoin pour la communauté de développer un consensus sur la compétence juridictionnelle et de trouver des mécanismes facilitant les recours des consommateurs. Ma conclusion quant à ces lignes directrices est qu'elles sont un pas dans la bonne direction mais qu'elles ne représentent pour l'instant que les vœux pieux de l'OCDE vers l'établissement ultérieur d'un cadre légal international, aboutissement ultime du dialogue international valorisé.

En ce qui concerne le besoin de développer un consensus sur la compétence juridictionnelle au niveau international il semble que même au niveau national nous ayons encore du pain sur la planche. Lors d'une conférence pour l'harmonisation des lois au Canada, les avocats de l'étude

[11] Ejan Mackaay : faut-il réglementer l'internet ?
[12] http://www.bamako2000.org/REFERENCES/DOC67.PDF

Ogilvy Renault semblaient nous mettre en garde contre la possible guerre de tranché que se livreront les provinces et le fédéral afin de déterminer la constitutionnalité des pouvoirs de légiférer de chacun. Ils sont d'avis que :

(...) une argumentation solide pourrait être développée pour soutenir que le Parlement est investi de la compétence législative exclusive de réglementer les travaux et entreprises qui font partie intégrante du réseau de communication Internet, tout comme il a le pouvoir de réglementer les travaux et entreprises qui sont reliés aux communications par téléphone. Une fois ce principe établi, il devient possible de dire que, sur le fondement de la jurisprudence actuelle, la compétence du Parlement s'étend aux questions qui, comme les relations de travail, constituent un élément essentiel de la gestion et de l'exploitation de ces travaux et entreprises. Le Parlement a donc, selon certains, le pouvoir de réglementer le contenu des communications par Internet, tout comme sa compétence à l'égard des entreprises reliées à la télévision s'étend à la réglementation du contenu des programmes de télévision .[13]

b. Compétence judiciaire

Pour ce qui est de la compétence judiciaire à l'égard des différends reliés à internet, leurs conclusions nous renvoient à l'harmonisation des compétences juridictionnelles au niveau international.

La question plus difficile est de savoir l'utilité d'une règle qui s'applique uniquement au Canada. Les règles canadiennes n'empêchent pas aux tribunaux étrangers d'exercer une compétence exorbitante sur des résidents ou des entreprises canadiens, ni garantissent aux Canadiens du recours juste et raisonnable contre les internautes étrangers. Cependant le marché canadien reste le plus important pour les entreprises et les consommateurs canadiens. Le commerce sur internet bénéficiera de la capacité de faire des transactions à l'intérieur du Canada avec de la confiance en les règles sur la compétence; cette confiance pourrait inspirer le choix de faire affaires avec des sites qui sont identifiables comme canadiens. Il est également possible qu'un

ensemble de règles bien conçues puisse inspirer d'autres pays à en adopter aussi. La Conférence pour l'harmonisation des lois devrait collaborer aux efforts internationaux pour étudier et résoudre les questions de compétence, mais si une loi canadienne s'impose, les limites sur une telle loi ne devraient pas détourner la Conférence de l'effort requis.[14]

c. Problèmes structuraux

De par sa nature intrinsèque le cyberespace a besoin d'un nouvel environnement législatif international. Pour démontrer mon point de vue j'utiliserai les arguments présentés par Me Gautrais [15] lors d'une conférence du Barreau du Québec sur les relations juridiques dans le ¨ cyberespace ¨.

Me Gautrais nous fait valoir la prépondérance du contrat papier sur le contrat cyberspatial en ce qui a trait à la preuve. Ces arguments reposent sur la nature intemporelle, immatérielle et internationale voire anationale des contrats cyberspatiaux. En effet, le contrat cyberspatial a une nature intemporelle. Prenons l'exemple d'un grossiste en alimentation de Montréal qui s'approvisionne directement chez un distributeur de pamplemousse du Maroc et qui utilise l'EDI pour ses transactions courantes. Lors des commandes et livraisons subséquentes le processus s'actualise sans intervention humaine. Plusieurs mois plus tard si un retard dans la livraison ou si un pépin quelconque arrive il sera bien difficile de déterminer le moment précis où ce sous contrat a pris forme. La nature immatérielle du contrat se présente dans l'exemple que nous venons de faire lorsque le sous-contrat est activé par l'EDI. Il n'y a pas de contact entre les intervenants vivants, ce sous-contrat n'est pas matérialisé sur papier et avec une signature. Pour illustrer encore mieux ce phénomène, prenons l'exemple de l'auteur :

Voici un exemple encore plus incontestable d'immatérialité.

Avec la vente et le contrat de services (accès, publicité), on retrouve typiquement sur l'Internet, le

---

[13] COMPÉTENCE JUDICIAIRE ET INTERNET
[14] COMPÉTENCE JUDICIAIRE ET INTERNET
[15] Les relations juridiques dans le cyberspace

contrat de licence. Conclu en cyberespace, ce dernier contrat est entièrement dématérialisé. Les prestations respectives de la livraison de l'objet de la licence et du paiement s'effectuent sans contact physique des cocontractants ni échange concret ou matériel.[16]

Finalement Me Gautrais nous parle d'internationalité voire d'anationalité. Il nous mentionne que 80% des contrats cyberspatiaux ne renferment pas de clause compromissoire qui ancrerait ce contrat dans une réalité géographique voire territoriale ce qui a pour effet de rendre ces contrats anationaux. Je vous souligne enfin le caractère obligatoirement international d'un contrat entre deux contractants de juridiction différente et attire votre attention sur le formalisme contractuel qui est préconisé par Me Gautrais afin d'encadrer les relations juridiques.

La conclusion logique de ce qui précède plaide amplement en faveur de l'utilité de lois internationales pour baliser le commerce électronique. Si le contrat papier a préséance sur le contrat cybernétique comment pouvons-nous envisager avec confiance le développement du commerce électronique? La pratique courante nous indique qu'en commerce Business to business le contrat papier et les contrats cadres d'échange EDI sont utilisés et ne font pas obstacle au développement du commerce électronique. Nous croyons cependant que pour le Business to consumer si le contrat cybernétique n'est pas efficace et efficient cela ralentira le sain développement du commerce électronique. Une autre particularité qui découle des arguments légaux de Me Gautrais et l'aspect territorial du commerce électronique. En effet, si le contrat cybernétique est immatériel, intemporel et international voire anational où se situe son territoire, son temps et sa nationalité ?

David R. Johnson et David Post[17] nous aide à cerner cette question. Le droit s'exerce sur un territoire, sur une juridiction. La juridiction s'exerce à l'intérieur d'une frontière. Or, dans le cyberespace il n'y a plus de frontière et nous devrions même faire l'exercice de se demander s'il y avait une frontière dans le cyberespace où serait-elle? Serait-elle à la frontière d'un état lorsque les bits traversent un conducteur fibre optique, serait-elle dans le modem de réception, dans le CPU, sur l'écran? Les auteurs nous proposent une solution :

[16] Les relations juridiques dans le cyberspace
[17] Law And Borders--The Rise of Law in Cyberspace

Treating Cyberspace as a separate "space" to which distinct laws apply should come naturally, because entry into this world of stored online communications occurs through a screen and (usually) a "password" boundary. There is a "placeness" to Cyberspace because the messages accessed there are persistent and accessible to many people. You know when you are "there." No one accidentally strays across the border into Cyberspace. To be sure, Cyberspace is not a homogenous place; groups and activities found at various online locations possess their own unique characteristics and distinctions, and each area will likely develop its own set of distinct rules. But the line that separates online transactions from our dealings in the real world is just as distinct as the physical boundaries between our territorial governments--perhaps more so. Crossing into Cyberspace is a meaningful act that would make application of a distinct "law of Cyberspace" fair to those who pass over the electronic boundary.

Si nous optons pour la frontière du mot de passe, déjà nous avons territoire pour lequel légiférer. Cependant ce territoire ne fait pas partie du monde physique et la tentative de légiférer ce territoire non physique ou même de tenter de contrôler le flux d'information entre ce territoire non physique et le territoire physique peut s'avérer vaine et illusoire.

Because the Net is engineered to work on the basis of "logical," not geographical, locations, any attempt to defeat the independence of messages from physical locations would be as futile as an effort to tie an atom and a bit together. And, moreover, assertions of law-making authority over Net activities on the ground that those activities constitute "entry into" the physical jurisdiction can just as easily be made by any territorially-based authority.

Et:

Because controlling the flow of electrons across physical boundaries is so difficult, a local jurisdiction that seeks to prevent its citizens from accessing specific materials must either outlaw all access to the Net--thereby cutting itself off from the new global trade--or seek to impose its will on the Net as a whole. This would be the modern equivalent of a local lord in medieval times either trying to prevent the silk trade from passing through his boundaries (to the dismay of local customers and merchants) or purporting to assert jurisdiction over the known world. It may be most difficult to envision local territorial sovereigns deferring to the law of the Net when the perceived threat to local interests arises from the very free flow of information that is the Net's most fundamental characteristic--when, for example, local sovereigns assert an interest in seeing

that their citizens are not adversely affected by information that the local jurisdiction deems harmful but that is freely (and lawfully) available elsewhere.

Nous devons donc considérer le Net comme un territoire à part entière défini à partir de règles spéciales hors du contexte physique dans lequel nous nous trouvons et d'où nos lois s'appliquent. Si nous recadrons le cyberespace dans un nouveau contexte légal (international) nous pourrons plus facilement contrôler et définir les paramètres d'analyse des particularités de frontières, de temps et de matière qui influeront sur les aspects de nature intemporelle, immatérielle et internationale voire anationale des contrats cyberspatiaux dont nous parlait Me Gautrais.

3. Arguments contre l'établissement d'un cadre juridique Onusien

Étant donné la nouveauté du débat dont je me fais le défenseur et la récente violation des droits à la vie privée que nous subissons, peu d'intellectuels et de théoriciens du droit se sont encore penchés sur la question. D'ailleurs, à la lumière de ces événements, je me demande si ceux qui valorisent la non-ingérence législative sont toujours du même avis ?Cependant j'ai pu trouver un commentaire de la présidente par intérim de l'Icann sur le sujet :

Esther Dyson est la présidente par intérim de l'Icann (Internet Corporation for Assigned Names and Numbers).
Internet n'a pas beaucoup de « corps gouvernants » et n'en a pas besoin. La plupart des choses peuvent être décidées localement. C'est le cas par exemple du contenu et de la défense de la vie privée. L'internationalisation de l'Internet est la raison pour laquelle il ne serait pas bon d'avoir un « corps gouvernant ». Il y a beaucoup de cultures différentes et l'Internet doit fonctionner différemment dans chaque endroit. Les problèmes qui doivent être abordés au niveau global sont très limités. C'est le cas pour les protocoles, mais pas pour la résolution des conflits à propos des noms de domaine. On n'a pas besoin d'avoir les mêmes lois partout. L'homogénéisation n'est pas bonne. (…)

Que pensez-vous de la suggestion de confier la régulation de l'internet à l'OCDE ou à l'OMC ? Vouloir réglementer (regulate) Internet, c'est comme vouloir réglementer l'air. La régulation est nécessaire, mais elle ne doit pas se faire au niveau d'une entité internationale. Elle doit surgir au niveau des juridictions locales. On ne peut pas réglementer l'ensemble. Je ne pense pas que ce soit une bonne idée. Et j'ajouterai que les deux organismes cités ont encore beaucoup de progrès à faire en matière de transparence et de démocratie.
Mais, même l'Icann ne devrait pas essayer de réglementer Internet. Au moins nous nous efforçons d'atteindre consensus et transparence, et tous les problèmes que nous avons sont un signe de santé. Une grande partie de nos problèmes sont inévitable, du fait de ce que nous sommes et de notre façon d'opérer. Nous représentons des intérêts très divers et nous nous efforçons de parvenir à un équilibre entre les grands et les petits. Chaque consensus fait plaisir à certains, et il est accepté par la plupart, mais il ne rend personne heureux. Les compromis sont nécessaires. Ce qui compte, c'est le processus qui nous permet d'y parvenir.[18]

À la lumière des nombreux exemples monopolistiques fournit dans la première partie de ce texte il est risible de prétendre qu'internet n'a pas de corps gouvernants. Il est aussi absurde de croire que localement les nations pourront légiférer en matière de vie privée sur internet. Pour ce qui est de l'analogie entre internet et l'air, plusieurs traitées internationaux régule déjà l'espace aérien (l'air), les couches stratosphériques, l'espace et les corps célestes. Finalement, pour ce qui est de la question de la représentativité et des ¨intérêts divers¨, à mon avis la diversification des intérêts devrait se traduire plutôt comme la diversité des intérêts américains.

D'autres théoriciens du droit contre la régulation d'internet font valoir que le nouveau droit est très bien capable de générer ses propres solutions sans interventions étatiques. Il nous parlent aussi de la difficulté et de la lenteur des processus de régulation international. Finalement, ils valorisent les normes, les codes et l'architecture d'internet comme outil d'autorégulation. Tout ces arguments dans un contexte où la régulation de facto américaine n'existe pas seraient parfaitement valables. Cependant, comme ce n'est pas le cas, l'urgence de se réapproprier collectivement notre cyberespace m'apparaît primordial.

[18] Le Monde Interactif

Epilogue philosophique.

Le cyberespace n'a pas de frontière, l'ONU non plus ; le cyberespace est une création virtuelle, l'ONU aussi. Le cyberespace en lui-même et certains de ses sites font désormais partie du patrimoine mondial, comme d'ailleurs plusieurs sites écologiques, historiques ou même marin. L'héritage intellectuel, technologique et multimédia de même que les divers bienfaits économiques, sociaux, culturels (et j'en passe) que le cyberespace apporte et apportera appartient à tous, nous devons participer à l'élaboration des moyens de la protéger. Il ne faudrait pas que nos gouvernements capitulent devant la montagne de travail qu'il reste à faire ou pire devant les pressions américaines. Je valorise la création spécifique d'une agence Onusienne à cette fin car l'ampleur de la tache à accomplir et les liens déjà douteux de certaines agences existantes avec des acteurs majeurs du monde internet et du gouvernement américain le justifie amplement. J'anticipe le plaisir de recevoir et d'envoyer des messages Hotmail sans avoir à me soucier de l'interception de ceux-ci par un état sur lequel les politiciens qui me représentent n'ont aucun pouvoir d'intervention législatif, exécutif ou judiciaire.

Annexe

How Does Window Washer Work?

Many people do not realize that Microsoft Windows, Internet Explorer, Netscape, NeoPlanet and America Online as well as many other software products store information about what they have been doing on their computer systems. This includes what documents they have used, which pictures they have viewed, which web sites they have visited, and various other activities they have been performing. Anyone can simply turn on your system and see exactly what you have been doing on your computer. This can infringe on an individual's privacy. Also, the tracks that are left behind can take up large quantities of valuable hard drive space. Recovering this space can be very beneficial by improving the overall speed and performance of a computer. Cleaning up the history of your activities can be a tedious chore of manually removing each history file or entry. If privacy and disk space are to be maintained, this process must be performed every time you use your computer. Window Washer can automatically clean up your browser's cache, cookies, history, recent document list, and much more! Window Washer can run in the background and clean up your tracks when you are done surfing the Internet or any other time you choose.

Window Washer - Cleans up your tracks and preserves drive space.
<http://www.webroot.com/washer.htm>