Réflexions

Le commerce électronique: pourquoi Industrie Canada n'y comprend pas grand-chose

Robert Cassius de Linval

Introduction

Le constat est à la fois troublant et inquiétant: Industrie Canada ne semble pas comprendre grand-chose au commerce électronique sur Internet. Pourquoi? Comme je l'explique dans la première partie du présent article, le médium est perçu de façon tellement négative par les autorités fédérales qu'elles lui prêtent, sans égard à la réalité, tous les vices de la terre.

Cette perception d'Internet, comme un environnement sale entraîne les responsables du dossier de l'inforoute sur un sentier malheureux. Toutes les transactions sont également menacées, par conséquent méritent la même protection. Or, telle analyse est défectueuse. La sécurité en matière informatique est affaire de choix: quel degré de sécurité puis-je me permettre, compte tenu de l'importance attachée aux informations à protéger. Bref, à chaque transaction correspond un degré de sécurité justifié. Vouloir tout protéger de la même façon n'est pas une solution viable ou efficace: certaines transactions ne justifieront pas le degré de protection érigé en norme. J'aborde cette question dans la seconde partie du présent texte.

Enfin, la lecture de la troisième partie du présent article suffira, j'ose le croire, à illustrer comment la réalité du commerce sur le Net diffère de la perception qu'en a Industrie Canada. Contrairement au portrait sombre que le ministère responsable de l'autoroute de l'information en brosse, Internet est une place commerciale sûre. L'engouement grandissant des cyberconsommateurs pour le médium, malgré l'absence des mesures préconisées par les autorités fédérales, semble le démontrer.

1. Internet est-il le Far West que croit devoir civiliser

Industrie Canada?

Internet est un monde d'une richesse sans bornes. Malheureusement, les médias ont eu tôt fait de mettre en exergue ce qu'il a de plus scabreux. Résultat? L'attention des citoyens s'est trouvée détournée du vrai défi qu'il pose: le commerce électronique. Aux transactions électroniques on a préféré une espèce d'hystérie collective qui accable le réseau d'opprobre. Comme à l'époque des actions *in rem*, l'objet inanimé qui transporte le matériel offensant est lui aussi accusé. Le messager se fait condamner, comme le matériel qu'il transporte.

Industrie Canada, ministère responsable des dossiers relatifs à l'autoroute de l'information, semble aussi reléguer les questions relatives au commerce électronique au second plan. Vie privée et matériel offensant apparaissent beaucoup plus préoccupants. La réglementation de ces sujets est considérée comme une condition préalable à l'émergence et à la croissance du commerce électronique au Canada. Dans *La société canadienne à l'ère de l'information: Pour entrer de plain-pied dans le XXI^{e} siècle* on peut lire:

> Les Canadiens ne pourront toutefois profiter pleinement de l'autoroute de l'information que lorsque certaines conditions auront été remplies. D'abord et avant tout, ils doivent avoir accès à l'autoroute. Ensuite, ils doivent être sûrs que leur vie privée sera protégée dans ce nouveau contexte électronique. Enfin, il faut s'occuper de la question du contenu offensant sur l'autoroute. Le plan d'action du gouvernement aborde toutes ces questions.

Ces ∗préalables+ servent d'assise à la philosophie d'hyper-sécurisation prônée par les autorités fédérales. Sans nécessairement sombrer dans l'exagération, on peut même aller jusqu'à affirmer que le gouvernement canadien est d'avis que sans sécurité quasi absolue pour toutes leurs transactions électroniques, les Canadiens ne pourront jamais vraiment profiter d'Internet comme place commerciale.

Une telle vision du commerce sur Internet est erronée. Si elle aboutit sur l'adoption de normes législatives ou réglementaires, comme le promet Industrie Canada, celles-ci ne seront pas optimales et pourraient même nuire à l'essor du cyber commerce.

Pourtant, la philosophie d'hyper-sécurisation des transactions commerciales préconisées par le gouvernement canadien ressort clairement des publications d'Industrie Canada relatives aux inforoutes. Le prosélytisme des autorités fédérales est provoqué par une perception excessivement négative d'Internet et des risques y associés, notamment en matière de sécurité.

L'attitude n'est pas surprenante. Il suffit de rappeler que, selon Industrie Canada, les Canadiens ne pourront pas jouir pleinement du réseau tant que la question des contenus offensants n'aura pas été réglée. Bref, le Net est perçu comme un univers pollué, voire monstrueux, qu'il faut assainir et aseptiser pour être en mesure d'en profiter.

Les craintes exprimées dans le rapport *La société canadienne à l'ère de l'information: Pour entrer de plain-pied dans le XXI^e siècle* sont un produit de cette perception. Voici le portrait des risques relatifs à la sécurité tels que perçus par Industrie Canada:

> À l'heure actuelle, les transactions financières ne sont sûres que sur les réseaux privés ou sur les réseaux informatiques bancaires fermés. Les transactions financières conclues par Internet ne sont ni faciles ni entièrement sûres. Ainsi, l'identité d'une personne avec laquelle on traite à distance n'est pas toujours claire. Vu la nature publique d'Internet, la sécurité est imparfaite, et rien ne garantit que les messages ne sont pas surveillés ou modifiés clandestinement ou que les numéros de carte de crédit ne sont pas enregistrés dans la base de données d'un tiers. La légalité des transactions électroniques peut aussi être mise en doute, vu que le droit canadien ne reconnaît peut-être pas la validité des signatures numériques. Celles-ci doivent en outre être protégées contre les fraudeurs et codées pour en empêcher la reproduction.

Comme nous le verrons plus bas, le tableau brossé par les auteurs de ce rapport ne reflète la réalité vécue sur Internet. Pour obtenir un portrait fidèle de la situation il est préférable de s'en remettre à d'autres études sur le commerce électronique. Elles sont issues de l'industrie et du milieu académique. Elles confirment que la perception d'Industrie Canada est fausse.

Contact, Communauté, Contenu: Le défi de l'autoroute de l'information B le rapport final du Comité consultatif sur l'autoroute de l'information B s'inscrit dans la même lignée. La conclusion est claire: sans infrastructure de sécurité à clé publique le commerce électronique ne pourra pas se développer. Voici comment les auteurs du rapport final s'expriment à ce sujet:

> La sécurité est une caractéristique essentielle de toute infrastructure de communications publiques. Elle vise à rassurer le consommateur, à susciter des possibilités sur le plan économique et à protéger les valeurs démocratiques (rec. 10.8). La sécurité établit les conditions propices pour protéger la vie privée et le caractère confidentiel des transactions de nature délicate, que celles-ci soient d'ordre financier, médical ou autre, qui s'effectuent sur l'autoroute de l'information.
>
> [...]
>
> Le fait que les échanges commerciaux électroniques puissent créer un secteur économique entièrement nouveau souligne la nécessité de prévoir des mesures de sécurité électronique pour le commerce et la protection de la vie privée (rec. 10.11). La libre circulation des renseignements et les échanges d'information sur l'autoroute favorisent le commerce électronique. Mais, il faut que les entreprises soient en mesure de vérifier l'identité des clients ou des entreprises avec lesquelles elles font des affaires. Cette vérification pourrait s'effectuer par l'entremise d'un mécanisme indépendant qui aurait la capacité de certifier l'identité des personnes concernées. Ce mécanisme, qui pourrait correspondre à un réseau d'authentification appelé infrastructure de sécurité à clé publique, se composerait d'un ou de plusieurs réseaux interfonctionnels qui relieraient des services d'authentification. Le Comité encourage le gouvernement, qui utilise lui-même une infrastructure de sécurité à clé publique, à prendre la tête du mouvement pour instaurer un mécanisme canadien commun et indépendant, doté de la capacité d'authentification (rec. 10.14). Il l'encourage aussi à favoriser la création de services de protection dans les domaines du secteur privé qui en ont besoin.
>
> Le gouvernement, de concert avec le secteur privé et les défenseurs de la confidentialité, doit favoriser l'élaboration de politiques, de normes et de pratiques uniformes pour les infrastructures de sécurité à clé publique au Canada. Le Comité recommande au gouvernement d'examiner immédiatement les dispositions législatives afin de pouvoir les appliquer aux infrastructures de sécurité à clé publique (recs. 10.13 et 10.15).

Les préoccupations du Comité consultatif sur l'autoroute de l'information et d'Industrie Canada sont nobles: protection de la vie privée et des valeurs démocratiques. Nous sommes tous pour la vertu. Malheureusement, l'idée qu'une hyper-sécurisation du commerce électronique est requise pour assurer son essor a bien peu à voir avec la réalité commerciale d'Internet.

2. À chaque transaction son degré de sécurité

Les longues citations livrées plus haut à une seule conclusion: les autorités fédérales et les spécialistes qu'elles ont consultés sont d'avis que le commerce électronique ne pourra pas se développer sans l'édification d'une infrastructure à clé publique ou de normes spécifiques visant à protéger les participants à l'économie d'Internet. Séduisante, la proposition n'est pas tout à fait exacte. Elle procède d'une analyse tronquée de la réalité du commerce électronique et des questions de sécurité qui s'y rattachent.

Industrie Canada a une perception du degré de sécurité nécessaire au succès du commerce électronique qui est exagérée et irréaliste. Viable au pays de cocagne, elle ne l'est pas dans un monde, le nôtre, où les ressources sont limitées B temps et argent B et où la sécurité est nécessairement un coût supplémentaire qu'il faut ajouter à celui de la transaction.

Toutes les transactions ne requièrent pas le même degré de sécurité. Plusieurs achats faits sur le Net n'ont rien à voir avec la transmission de données hautement sensibles, un dossier médical par exemple. La transmission de ce dernier exige un haut niveau de confidentialité. Cela justifie l'investissement des sommes nécessaires pour assurer cette confidentialité.

Cependant, lorsqu'il est question de transactions commerciales la situation est bien différente. Si la valeur de la transaction en termes de dollars est faible, peut-on se permettre d'investir des sommes importantes pour en protéger le caractère confidentiel? Et si elle n'a que peu ou pas d'impact sur la vie privée d'un consommateur, pouvons-nous avoir les mêmes exigences quant à la confidentialité et la sécurité de la transaction que dans le cas d'un dossier médical?

Par conséquent, toutes les transactions ne justifient pas le même degré de protection ou de sécurité. Pourquoi? Parce que les coûts associés à la sécurité doivent être assumés par quelqu'un et que dans certains cas l'investissement n'est pas justifié. Chaque cas est un cas d'espèce.

Si les velléités d'hyper-sécurisation d'Industrie Canada aboutissent à l'élaboration d'un carcan normatif obligatoire pour transiger sur le Net, l'utilisation de clés publiques par exemple B une infrastructure dont la gestion pose de nombreuses difficultés qui demeurent, à ce jour, non résolues, cela risque d'avoir un impact négatif sur le commerce électronique. Une foule de transactions ne vaudront peut-être plus la peine d'être conclues parce que devenues trop chères. Les coûts associés à la sécurité imposée feront grimper le coût de la transaction bien au-delà de la valeur du bien transigé.

Industrie Canada semble ignorer un principe fondamental applicable en l'espèce. La sécurité en matière de technologies de l'information ne peut pas s'exprimer en termes absolus. Elle est toujours une affaire de choix, un arbitrage entre deux pôles: l'investissement nécessaire pour atteindre un degré de protection donné et la valeur des informations à protéger. Et comme je l'écrivais plus haut, ce constat entraîne nécessairement le suivant: différentes informations justifient des degrés de protection différents. Les auteurs Cheswick et Bellovin, deux spécialistes de la sécurité sur Internet, s'expriment ainsi à ce sujet:

> The third question one must answer [la première est quelle information je veux protéger, la seconde contre les attaques de qui] before deploying a security mechanism represents the opposite side of the coin: how much security can you afford? Part of the cost of security is direct financial expenditure...But there is a more subtle cost, a cost in convenience and productivity, and even morale. Too much security can hurt as surely as too little can. Finding the proper balance is tricky, but utterly necessary B and it can only be done if you have properly assessed the risk to your organization from either extreme.
>
> [...]
>
> One cannot have complete safety; to pursue that chimera is to ignore the costs of the pursuit.

3. L'engouement pour le Net est clair et le commerce électronique se développe sans que des normes de protection particulières n'aient été adoptées

Internet pénètre dans les foyers québécois et du monde entier à un rythme effréné. Et la tendance semble irréversible. Comme l'exprime si bien William Blundon, malgré les divergences d'opinions entre les différentes études, leur nombre impressionnant est symptomatique de l'importance du phénomène:

> Despite the often wide range of numbers B whether of users, dollars, or growth B one thing remains clear: The Internet continues to grow at an astounding rate as more users, countries, and companies come online. (An indication of how large the Net has become is the number of surveys that are being performed to measure it!) It is a growing market that effects a myriad of satellite industries, generating jobs and growth in software, advertising, banking, fiber optics, publishing, broadcasting, communications, sales, and research. It has caused change and adaptation in almost every walk of life, from grade school students to corporate CEOs. And its size and impact will only get larger.

Malgré l'absence d'une infrastructure à clé publique ou de normes spécifiques de protection, les menaces perçues par Industrie Canada n'empêchent pas Internet de continuer sa progression dans les habitudes d'achat des cyberconsommateurs. Internet est un lieu d'échange de plus en plus prisé par les consommateurs. Il semble que les citoyens ne partagent pas les craintes des autorités fédérales. Les chiffres mis de l'avant par les auteurs de nombreuses études sur le commerce électronique confirment la tendance: l'importance du commerce électronique est aujourd'hui indéniable.

Le groupe Cowles/Simba, dans un communiqué de presse rendu public le 30 janvier 1997, rapporte que la valeur des transactions électroniques en 1996 représente 993,4$ US millions. Il s'agit d'une augmentation de 61,8% sur les résultats de 1995. Les auteurs de l'étude prévoient que la valeur totale des transactions électroniques dépassera le cap de 5$ US milliards d'ici l'an 2000. Ils attribuent cette hausse marquée des transactions électroniques à l'importance sans cesse grandissante que prend Internet comme lieu d'échanges commerciaux. Selon eux, les transactions conclues par le biais d'Internet représentent 73,8% de toutes les transactions électroniques conclues en 1996. Cette proportion passera à 85% de toutes les transactions électroniques d'ici l'an 2000. La valeur des transactions commerciales conclues sur Internet s'établira donc à 4,27$ US milliards au tournant du millénaire. En 1996, la valeur des transactions sur le Net se chiffre déjà à 733,1$ US millions.

Les conclusions de la sixième enquête menée par le *Graphics, Visualization and Usability Center (GVU)* de l'Université Georgia Tech vont dans le même sens. Les auteurs de l'étude concluent que:

> As reported in Primary Uses of the Web, shopping has nearly doubled to roughly one out of every five users shopping via the Web. The Web is truly becoming a viable medium for electronic commerce albeit slowly but surely.

Notamment, les auteurs de l'étude rapportent que les consommateurs sont de moins en moins réticents à transmettre leur numéro de carte de crédit à un vendeur sur le Net. Cette observation s'inscrit dans la lignée d'une déclaration d'un représentant de Visa selon lequel le risque de fraude de carte de crédit est plus grand quand on règle l'addition dans un restaurant que lors d'une transaction *non sécurisée+ par le biais du Net. La journaliste Catherine Buzzell résume bien la situation:

> We seem to be chewing on a problem that doesn't really exist. People are purchasing on the Web. I haven't heard any horror stories about crackers harvesting credit card numbers from merchant sites and buying Game Boys for all their friends. Using credit cards works just fine, and if it ain't broke, don't fix it. Consumers will buy more stuff online when there's more stuff to buy online. And more big-name retailers are on the Web B Macy's. Bloomingdale's, and granddaddy Wal-Mart. The Web won't be as big as mail order until computers with Net access are as commonplace in households as telephones and postage stamps.

Bref, contrairement à la perception d'Industrie Canada, Internet n'est pas une jungle où le danger se terre derrière chaque routeur. Aussi, la thèse alarmiste B symptôme de l'hystérie collective mentionnée plus haut B ne se confirme pas dans les faits. Les consommateurs ne sont pas réfractaires à transiger sur le Net à cause des supposés risques qu'on voudrait lui attribuer. Déjà en 1995, une étude mettait cette hypothèse, pourtant encore très répandue, en doute.

Vince Emery, auteur du très populaire ouvrage *Faire des affaires sur Internet*, est aussi d'avis que ce n'est pas la crainte qui retient les consommateurs d'effectuer leurs achats sur le Net. Selon ce spécialiste, ∗the biggest obstacle for electronic consumer transactions on the Internet is that people aren't used to buying things on the Net. The security issue is overplayed in the media. Individual consumers aren't really worried about security+

Le niveau des achats de produits informatiques effectués par l'entremise du Web laisse croire que la thèse de Emery est exacte. En effet, les individus les plus férus d'informatique, donc ceux qui sont les plus susceptibles d'acheter de tels produits, n'ont pas peur d'un médium qui, après tout, est le leur. Et puisqu'ils consomment dans des conditions semblables à celles offertes aux autres consommateurs, il est difficile de blâmer la peur pour la retenue de ces derniers. Ils consomment moins sur le Net parce qu'ils sont moins habitués au médium.

La croissance des achats de consommation sur le Net se fait plus rapidement pour les produits qui participent au médium (le ∗hardware+) ou qui s'y meuvent facilement (le ∗software+: logiciels, données en format électronique B articles de journaux, photos, textes divers, bientôt de la musique, éventuellement des films). En d'autres mots, la pertinence immédiate d'Internet pour le commerce électronique est directement proportionnelle au type de produit dont il est question. Mais n'est-ce pas aussi vrai dans le monde des atomes? Le ∗mail order+ ou la commande téléphonique sont des médiums d'échanges très prisés dans certains domaines de l'activité économique: à chaque produit son marché... pour l'instant. En effet, Internet devrait devenir un lieu d'échange de plus en plus commun pour à peu près tous les produits. Les auteurs du *GVU's 6th WWW User Survey* concluent sur le sujet en ces termes: ∗Just about all other areas, including apparel, legal services, and personal items have also shown increases in gathering and purchases through the Web.+

Par exemple, le 20 mars 1997, une entreprise américaine annonçait le lancement de sa salle de montre virtuelle, par le biais de laquelle les internautes pourront acheter des voitures neuves et d'occasion. Pour l'instant, les produits de consommation les plus populaires sur le Net sont les produits informatiques, suivis par les produits touristiques B billets d'avion, réservations d'hôtel, etc., les livres et les magazines et, enfin, les disques compacts ou vinyle et les cassettes de musique.

Conclusion

Les consommateurs n'attendent pas que les voeux pieux du gouvernement se concrétisent avant de se lancer dans l'aventure du commerce électronique. Ce constat est important. En surestimant les risques posés par le commerce électronique, le gouvernement risque d'intervenir dans le marché pour rien. Une telle intervention serait nécessairement inefficace et ralentirait peut-être le développement d'un lieu d'échanges commerciaux qui, tout virtuel qu'il soit, fait de plus en plus partie du ∗vrai monde+.

La méprise du gouvernement tient probablement à sa vision du Net comme d'un repère de dangereux pirates. Industrie Canada perçoit tellement de risques qu'il conclut à un besoin élevé de moyens de protection. Malheureusement, dans ce contexte, on aboutit à une conception trop

univoque des questions relatives à la sécurité. Comme je l'écrivais plus haut, la sécurité est une affaire de compromis entre l'objectif à atteindre et les coûts nécessaires pour y arriver. Mettre toutes les transactions effectuées sur le Net sur le même pied c'est ignorer cette réalité et se condamner à une intervention qui ne peut pas être optimale. Pour se défaire de cette mauvaise habitude, les autorités fédérales devront d'abord et avant tout cesser de percevoir le Net comme la tanière du diable.