HEC MONTRÉAL

LA PERCEPTION DES CONSOMMATEURS QUÉBÉCOIS SUR L'IMPACT DE LA CONFIANCE ET DU CONTRÔLE EN COMMERCE ÉLECTRONIQUE

Par

Mathieu Arles-Dufour

Sciences de la gestion

Mémoire présenté en vue de l'obtention
du grade de maîtrise ès sciences
(M.Sc.)

Mai 2006

Comité d'éthique
de la recherche

HEC MONTRÉAL

AVIS DE CONFORMITÉ À LA POLITIQUE EN MATIÈRE D'ÉTHIQUE DE LA RECHERCHE AVEC DES ÊTRES HUMAINS DE HEC MONTRÉAL

La présente atteste que le projet de recherche décrit ci-dessous a fait l'objet d'une évaluation en matière d'éthique de la recherche avec des êtres humains et qu'il satisfait les exigences de notre politique en cette matière.

Titre du projet de recherche:
La perception des consommateurs québécois sur l'impact de la confiance et du contrôle en commerce électronique

Chercheur principal:
Chercheur : Mathieu Arles-Dufour
Titre : Étudiant(e) Maîtrise
Service/Option : Marketing

Directeur : Jacques Nantel
Titre : Professeur(e) titulaire
Service/Option : Marketing

Date de déclaration du projet au Comité d'éthique de la recherche:
24 janvier 2006

Date d'approbation du projet:
03 février 2006

Date de publication de l'avis:
03 février 2006

Céline Bareil

Céline Bareil, Présidente
Comité d'éthique de la recherche

Sommaire

Le commerce électronique apparaît aujourd'hui comme le média le plus perméable à l'économie de la trace née de la saturation des marchés. Bien suivre le consommateur afin de mieux le connaître devient une condition indispensable à la réussite de la mise en place d'offensives de commercialisation. De nos jours, il existe un marketing de pointe qui pose de plus en plus la problématique de la protection, et ce en raison de l'appréhension que suscite le média Internet et ses pratiques auprès du consommateur. Des appréhensions dont la plus importante conséquence est la diminution de confiance du consommateur vis à vis des entreprises alors qu'en fait l'objectif de ces dernières est de toujours mieux le comprendre afin de mieux le satisfaire. Cette situation s'avère particulièrement conflictuelle puisque les pratiques des marchands, censées répondre aux attentes des consommateurs, augmentent le sentiment de non contrôle des individus sur leurs renseignements personnels et influencent a contrario les comportements.

La présente recherche s'appliquera donc à déceler les politiques que les entreprises devraient mettre en place et communiquer aux consommateurs afin de renforcer leur sentiment de contrôle sur les informations privées. Autrement dit, dépendamment de la lecture et de la perception du contenu des politiques sur la protection des informations personnelles, nous nous appliquerons à saisir quelle est l'influence de la perception du contrôle sur la sécurité et la vie privée. L'autre objectif majeur est de comprendre la relation entre le sentiment de contrôle étudié, le sentiment de confiance envers le cybermarchand et le comportement effectif lié à l'utilisation d'un site Internet marchand.

Le cadre conceptuel exposé est donc construit sur les variables indépendantes des caractéristiques du cybermarchand, sur la collecte de données et du traitement des renseignements personnels. Les variables dépendantes à l'étude se basent sur le contrôle comportemental perçu sur les renseignements personnels, la confiance interpersonnelle, la confiance institutionnelle, la confiance de disposition et enfin l'attitude et l'intention comportementale envers l'utilisation d'un site Internet.

La méthodologie imaginée et appliquée à notre étude repose sur une expérimentation en ligne dans un environnement non contrôlé. Trois sites Internet ont été créés en ce sens dont la seule variation concernait le traitement des renseignements personnels et les caractéristiques sur la collecte de données. Dans ce dessein, un des sites ne comprenait aucune politique sur la protection des renseignements personnels, tandis que les autres proposaient des politiques en format dynamique en opt-in ou statique en opt-out. Chaque politique était construite autour de quatre dimensions prônées par le FTC (The Federal Trade Commission), à savoir : la notification, la sécurité, l'accès et le choix. Il a été ainsi demandé aux 209 internautes ayant participé à l'expérience, de s'inscrire à un programme de recherche sur la musique en ligne, de naviguer sur un site Internet marchand proposant la radio satellite (siriuscanada.ca), et enfin de répondre à un questionnaire final.

Les résultats établissent, comme nous en avions émis l'hypothèse, que la seule présence d'un lien menant vers une politique sur la protection des renseignements personnels influe positivement sur le contrôle que ressent le cyberconsommateur au sujet de ses informations privées. Par ailleurs, il semble qu'une politique dynamique basée sur le consentement préalable de l'internaute (opt-in) augmente sensiblement le contrôle perçu par rapport à une politique statique fondée sur le consentement implicite (opt-out). Néanmoins les analyses démontrent aussi que le format statique en opt-out permet d'obtenir en plus grand nombre l'acception des internautes à ce que leurs informations privées soient diffusées dans un but promotionnel.

Par ailleurs, nous observons de nombreuses corrélations entre les différents construits à l'étude. C'est ainsi que le contrôle comportemental, outre son influence faible mais positive sur la confiance interpersonnelle et l'intention comportementale, intervient comme variable modératrice dans la relation qui unit confiance interpersonnelle et comportements ultérieurs (cf. Attitude comportementale). De plus, nous constatons une forte corrélation entre la confiance interpersonnelle et le comportement ultérieur démontrant, comme nous l'indique la revue de littérature, l'importance du construit dans la construction de l'attitude et de l'intention comportementale.

Autrement dit, cette recherche semble avoir démontré une fois de plus le conflit qui confère avec la récolte de données sur le nouveau média. D'un côté, nous remarquons l'efficacité des politiques statiques fondées sur le consentement implicite (opt-out) en termes de récolte de données privées utilisables pour la promotion, et de l'autre, nous notons la force du consentement préalable (opt-in) en format dynamique dans le développement d'une attitude et d'une intention positive envers l'utilisation d'un site Internet marchand.

Cette recherche a permis de comprendre les mécanismes en jeu dans l'acceptation de divulguer des renseignements privés ainsi que dans la formation d'un comportement. Par ailleurs, elle a également permis de conseiller au gestionnaire d'accorder au consommateur un pouvoir de contrôle propre à lui apporter confiance et sérénité; une stratégie sans aucun doute payante pour l'acceptation d'une économie de la trace naissante et tellement prometteuse.

Mots clefs : Commerce électronique, Marketing relationnel, Confiance, Contrôle, Sécurité, Vie privée, Renseignements personnels, Internet, Politique sur la protection des renseignements personnels, Opt-in, Opt-out, Économie de la trace.

Table des matières

Liste des tableaux

Liste des figures

Remerciements

Je tiens à remercier l'ensemble des personnes qui ont permis à cette recherche de se réaliser, et en premier lieu Monsieur Jacques Nantel, mon directeur de recherche, pour sa gentillesse, sa considération, son attention, sa disponibilité et tous les moyens qu'il a su mettre en œuvre pour le bon déroulement de cette recherche. Je retiendrai plus particulièrement sa grande humilité au service d'une extrême compétence. Sans l'aide précieuse de la chaire RBC Groupe Financier, ce mémoire n'aurait jamais pu aboutir.

Je souhaite également remercier très chaleureusement le concepteur des sites expérimentaux Mr Abdelouahab Mekki Berrada pour sa patience, sa serviabilité, sa grande aide dans la collecte de données, et son expertise dans le domaine des nouvelles technologies.

Je remercie mes grands parents Arles-Dufour pour l'aide qu'ils m'ont apportée afin de rendre mon projet canadien réalisable.

Je suis très reconnaissant envers mes parents de m'avoir aidé tout au long de ce mémoire et surtout de m'avoir toujours soutenu durant toute ma formation académique. Leur générosité, leur bienveillance, leur appui dans les moments difficiles ont rendu possible la réalisation de ce mémoire vécu par son auteur comme un aboutissement. Sans eux et leur amour, cette recherche n'aurait jamais pu voir le jour.

Enfin, je souhaite remercier tous mes amis à la maîtrise pour toute l'aide et le soutien qu'ils ont su m'apporter lors des différentes étapes de la recherche.

Je vous remercie tous du fond du cœur ...

Introduction

Au cours des dernières années, les moyens de production n'ont cessé d'évoluer conduisant logiquement à des économies d'échelles dans la majorité des secteurs. Le résultat de cette recherche de profit et d'une concurrence toujours plus accrue est que le marché connaît aujourd'hui une forte saturation rendant le consommateur de plus en plus rare.

Dans ce contexte assez difficile pour les entreprises, et afin de gérer cette rareté, les gestionnaires ont su mettre en place un marketing fondé sur la relation individualisée dans le but de connaître de façon intime chaque consommateur. Dans ce sens, l'Internet est sans aucun doute l'endroit se prêtant le mieux au marketing relationnel tant les possibilités techniques sur le « nouveau média » sont grandes. Aujourd'hui, la plupart des organisations collectent les informations de milliers de consommateurs à travers l'enregistrement, l'achat, les sondages, ou bien encore en utilisant la récupération de courriels, cookies, et autres logiciels de surveillance. Des données qui permettent tout d'abord la personnalisation afin de vendre les produits ou les services adaptés aux besoins de chacun, mais aussi dans un second temps, la création de nouveaux revenus par la vente de ces informations si recherchées.

Ce marketing dit « one to one », « permission marketing » ou bien encore « ciblage comportemental » soulève les problématiques de la sécurité et de la vie privée. En effet, il a été démontré que ces deux dernières dimensions sont un réel obstacle à l'émergence d'un comportement positif vis à vis du cybermarchand faisant pratique de ce marketing relationnel très sophistiqué. Une situation qui s'avère donc particulièrement contradictoire puisque les pratiques des marchands censées répondre aux attentes des consommateurs augmentent les préoccupations, et, impactent sur la confiance allouée au site Internet concerné (Liu et al. 2005).

Par conséquent, les dimensions de la sécurité et de la vie privée s'inscrivent comme les fondements de la confiance. Un construit très travaillé dans le domaine du commerce électronique et dont le lien avec l'attitude et l'intention comportementale a

été démontré (Suh et Han, 2003, Liu et al., 2005). Sans confiance, l'attitude et l'intention d'utiliser un site Internet marchand sont quasiment nulles (Suh et Han, 2003). Autant dire, que le marketing relationnel sur le média Internet, de par sa complexité et les craintes qu'il entraîne, est une arme à double tranchant qui certes personnalise les échanges mais dérange aussi les cyberconsommateurs limitant ainsi l'énorme potentiel du commerce électronique.

0.1 Positionnement de l'étude et objectifs

Pister les individus afin de les atteindre au bon moment, à la bonne place et avec les bons arguments est sans aucun doute le défi marketing que bon nombre de gestionnaires se lancent en ce début de 21^{ième} siècle. Aussi, lors de cette recherche, nous avons souhaité comprendre ce que ressent le consommateur dans une économie de la trace naissante, mais toujours plus perfectionnée ; appliquée à l'Internet, média très perméable au ciblage comportemental des consommateurs, l'objectif principal est de comprendre la perception de ces derniers vis-à-vis de l'impact du contrôle comportemental et de la confiance sur les comportements ultérieurs. Il est alors question de mesurer la réaction des individus québécois dépendamment de l'ensemble des processus de régulation impliqués lors d'une divulgation de renseignements personnels. Par conséquent, les domaines de la sécurité et de la vie privée faisant référence à la protection des renseignements personnels sont au centre l'étude.

L'objet de la recherche est également de développer des implications managériales appliquées aux pratiques liées à la récolte de données sur l'Internet, susceptibles d'optimiser la confiance et les comportements ultérieurs des individus. Nous pensons que cette recherche aidera les praticiens à se faire une idée des mécanismes en jeu dans la formation d'une attitude et d'une intention lorsqu'il est demandé au consommateur de divulguer des informations privées. Enfin, nous croyons que les résultats de la recherche devraient aider les gestionnaires de la toile à établir et communiquer des politiques de sécurité et de confidentialité susceptibles de rassurer

les individus, de les motiver à utiliser le site concerné, et, par la suite de les encourager à divulguer leurs renseignements personnels.

Dans le dessein d'une compréhension approfondie des mécanismes de la formation du comportement, nous traiterons, dans un premier chapitre, des craintes des consommateurs vis-à-vis de la sécurité et de la vie privée sur le media Internet. La forte appréhension quant à la divulgation des renseignements personnels y sera analysée de manière détaillée et nous nous attarderons finalement sur les processus de régulation mis en place pour atténuer les inquiétudes des consommateurs relatives à la divulgation des informations privées. Par la suite, nous examinerons le construit du contrôle, variable centrale dans la planification d'un comportement, influençant logiquement les attitudes et les intentions. La notion de contrôle définie, nous discuterons alors de cette variable par rapport aux services de sécurité et de vie privée en commerce électronique. Le contrôle est, dans le contexte de cette recherche, expliqué par rapport au contrôle comportemental que le consommateur ressent sur ses renseignements personnels lors d'une demande de divulgation d'informations privées. Enfin, nous terminerons ce premier chapitre en définissant la confiance, dépendamment des découvertes faites sur le construit, dans des domaines aussi variés que l'économie, la finance, le marketing, la philosophie, la sociologie, ou bien encore la psychologie sociale.

Par la suite, le chapitre suivant fera état d'un cadre conceptuel regroupant les notions précédemment étudiées. D'après le TAM (Technology Acceptance Model), le TPB (Theory of Planned Behavior) ou le TRA (Theory of Reasoned Action), les deux variables du contrôle comportemental et de la confiance ont un impact significatif sur le comportement du consommateur. Notre modèle s'inspire, de fait, des modèles de Mcknight et Chervany (2002) dans l'étude de la confiance et de leurs conséquences sur le comportement ainsi que du modèle TPB (Ajzen, 1991) dans l'étude du contrôle comportemental.

La particularité de notre modèle conceptuel et les objectifs de la recherche impliquent le recours à une méthodologie expérimentale expliquée en détail dans notre troisième

chapitre. L'objectif avoué de cette investigation scientifique est de créer une variation du contrôle comportemental perçu sur les renseignements personnels. Pour ce faire nous avons créé trois sites Internet expérimentaux dont la seule variation concernait les caractéristiques sur la collecte des données et le traitement des renseignements personnels. En d'autres termes, seule la présence et le contenu des politiques sur la protection des informations privées subissait des variations.

Cette démarche empirique contribue à la bonne compréhension des mécanismes intervenant dans le renforcement du sentiment de contrôle ainsi que dans la construction de la confiance, susceptible d'aboutir à un comportement positif vis-à-vis de l'utilisation d'un site Internet marchand. Il est alors question de découvrir quelles pratiques assurant, à la fois sécurité et vie privée, sont les plus à même d'influencer positivement les antécédents du comportement.

Par conséquent, nous pensons que cette recherche aidera les praticiens à mieux comprendre l'importance de ces deux construits ainsi que leurs mécanismes afin d'aboutir à une attitude et à une intention comportementale positive chez les consommateurs. Enfin, nous croyons que les résultats de la recherche devraient aider les gestionnaires de la toile à établir et communiquer des politiques de sécurité et de confidentialité efficaces dans le but de rendre les internautes confiants avec le sentiment d'être encore maîtres de leurs données privées.

Chapitre 1 : Revue de la littérature

David Herbert Lawrence (1885–1930), dans un texte provenant de son livre « The Letters of D.H. Lawrence » (1922), écrit que l'on ne peut croire à la vie sans la contrôler. Cette citation s'applique également au consommateur dans le monde du commerce électronique et de l'Internet. Un cybermarchand peut il être crédible sans livrer au consommateur un message sécurisant visant à lui donner le sentiment de rester maître de son environnement ?

Cependant, pour tout gestionnaire, on se doit de contrôler un minimum l'environnement que l'on met à disposition des consommateurs sans en perdre totalement la maîtrise. Il s'agit d'un défi pour tout cybermarchand, qui consiste à gagner la confiance des consommateurs. La littérature elle-même a souvent traité de la notion de contrôle et de la notion de confiance comme des construits intimement corrélés. Knights et al. (2001) considèrent ces deux notions comme interdépendantes, et opposées ; quant à Castelfranchi et Falcone (2000) (voir Skinner et Spira, 2003), ils résument très bien cette idée d'alternatives opposées :

"*if you control me you don't trust me! and it is true that if you do not trust me enough ... you would like to monitor, control and enforce me in some way*".[1]

Dans le même ordre d'idée, Tan et Thoen (2001) ont mis l'accent sur la dualité entre les deux construits. Ainsi expliquent-ils que dans n'importe quelle situation donnée, les parties négociantes peuvent se fier l'une à l'autre ou s'en remettre à des mécanismes de contrôle fonctionnellement équivalents. Le contrôle, dans le cas présent, serait supporté par un ensemble de processus de régulation qui surveillent la performance réussie de l'échange d'information entre les deux parties négociantes.

---

[1] Notre traduction : Si vous me contrôlez vous ne me faites pas confiance ! Et il est vrai que si vous ne me faites pas assez confiance .... Vous aurez envie de me suivre de près, de me contrôler et de me forcer.

Aussi, la revue de littérature présentée nous permettra de clarifier les deux construits du contrôle et de la confiance s'appliquant au domaine du commerce électronique. Pour ce faire, nous allons tenter dans un premier temps d'identifier les craintes des consommateurs liées à la sécurité et à la divulgation de renseignements sur la vie privée. Celles-ci apparaissent comme étant la notion fondamentale et centrale dans le contrôle comportemental perçu du consommateur sur l'ensemble des processus de régulation. Nous nous intéresserons de fait aux pratiques touchant aux processus de régulation en cours sur le nouveau média. Dans notre seconde partie, nous examinerons la notion de contrôle perçu de façon globale et théorique, puis, la confiance perçue dans le contrôle des services de sécurité et de vie privée. Finalement, dans une dernière partie, il sera question de comprendre la variable de la confiance perçue relative à la transaction sur un site Internet marchand.

1.1 Les craintes des consommateurs en commerce électronique vis à vis de la sécurité et de la vie privée

Dans ce chapitre, nous analysons les craintes que peuvent ressentir les internautes. Dans un premier temps, nous tentons de comprendre les antécédents du sentiment de contrôle sur la sécurité et la vie privée. Dans un second temps, nous abordons l'ensemble des processus de régulation permettant de garantir la sécurité et la vie privée lors d'une divulgation de renseignements personnels, y compris les renseignements bancaires, comme par exemple l'authentification de la source informationnelle, la garantie sur l'intégrité ou bien encore la confidentialité des données fournies dans le but d'empêcher toute divulgation publique ou privée. Cette partie est l'occasion d'étudier le comportement du consommateur face aux processus de régulation assurant sécurité et vie privée lors de la divulgation d'informations personnelles dans le domaine du commerce électronique.

1.1.1 La forte appréhension des consommateurs vis-à-vis de la divulgation d'informations personnelles en commerce électronique

Depuis une quinzaine d'année, l'usage de l'Internet se démocratise et le nombre de personnes utilisant ce nouveau media n'a cessé d'augmenter. D'après les dernières statistiques que nous avons pu recenser, on estime à 938 millions le nombre de personnes ayant utilisé l'Internet en 2005, alors qu'ils étaient seulement 544 millions en 2002. D'après les données publiées par INTERNET WORLD STATS, on évalue qu'entre 2000 et 2005, le taux d'usagers a augmenté de 160%. Et si on note un fort taux de pénétration en Amérique du nord (68%), en Europe (36,8%) et en Océanie (49,2), on peut sans doute prévoir que le nombre d'internautes dans le monde augmentera encore significativement dans les prochaines années tellement le taux de pénétration est faible dans certaines régions du globe. En ce qui concerne le Canada, on évalue à 20,450 millions le nombre d'internautes, avec un taux de pénétration à 63,8 % et une augmentation significative entre 2000 et 2005 du nombre d'utilisateurs (+ 61%). Finalement, si l'on s'intéresse au commerce électronique et au marché des ventes en ligne des entreprises privées au Canada, on évalue à 8,5 milliards $CAN la valeur des ventes réalisées par les cybermarchands en B2C sur un total de 28,3 milliards $CAN si l'on y inclut le commerce interentreprises en 2004 (INDUSTRIE CANADA, 2004). Pour donner une idée de l'avènement du commerce électronique au Canada, cette même valeur des ventes par Internet incluant commerce Entreprise-Consommateur et commerce interentreprises était estimée à 5,6 milliards $CAN en 2000, puis 11 milliards $CAN en 2002, pour atteindre en 2004 le chiffre de 28,3 milliards $CAN cité auparavant.

Cependant les craintes des consommateurs vis-à-vis du commerce électronique ne faiblissent pas malgré des ventes (tous secteurs confondus) en continuelle croissance. En effet, une étude des plus récentes menée par STATISTIQUE CANADA (2005) révélait que plus de 41,8% des Internautes canadiens restaient très préoccupés par la confidentialité contre 34,7% en 2001. Toujours d'après la même étude, en 2003, 42,3% se disaient toujours très préoccupés par la sécurité.

Ces chiffres rejoignent d'ailleurs les tendances d'une étude menée en 2005 par le GARTNER GROUP sur le marché Américain. En effet, INFOWORLD (2005) cite que les bénéfices sur les ventes des compagnies privées américaines dans le domaine du B2C pourraient se voir amputer de 0,3% à 1% chaque année par rapport aux prévisions établies. Ce phénomène serait dû à la lente montée de l'inquiétude des consommateurs vis-à-vis de la sécurité. Pour information, il était prévu par GARTNER (INFOWORLD, 2005) que les bénéfices sur les ventes en B2C atteindraient 18% en 2005, 15% en 2006 et 11% en 2007.

Quant à ERNST & YOUNG (BETTER BUSINESS BUREAU, 2001), le groupe rapportait en 2001 que pour des millions d'internautes, la vie privée était un sujet d'inquiétude majeur et qu'ils souhaitaient acquérir l'assurance d'une protection sur leurs historiques, ainsi que sur tous leurs comportements liés à la navigation et leurs propres données. Cette même étude révèle que 72% des répondants se disent « extrêmement concernés » à « très concernés » du contrôle qu'ils ont sur l'utilisation secondaire des informations personnelles après une divulgation de celles-ci.

Outre les préoccupations liées à la vie privée que peuvent exprimer les consommateurs à l'égard du commerce électronique, Gefen (2000) mentionne d'une part la gène des internautes à procurer des informations sensibles comme un numéro de carte de crédit, et d'autre part, un certain confort à procurer de l'information générale comme par exemple les préférences. Dans le même ordre d'idée, Warrington (1999) dans le domaine de la banque en ligne, ajoute que les utilisateurs s'inquiètent davantage du niveau de la sécurité lorsqu'ils communiquent de l'information sensible. Les consommateurs paraissent donc peu enclins à livrer un certain type d'informations ; néanmoins, ceci n'est pas dû au seul fait de la sécurité et de la vie privée sur l'Internet, mais aussi à la confiance accordée aux cybermarchands. Parmi les facteurs qui influent sur l'inquiétude des internautes, nous noterons les peurs liées au paiement sécurisé en ligne, la fiabilité des compagnies ou bien encore la vie privée.

De plus, INFOWORLD (2005) révèle la montée croissante des menaces de sécurité sur Internet. C'est ainsi qu'entre la seule période de Mai 2004 et Mai 2005, on a constaté que les attaques de phishing par courriel avait augmenté de 28%. Le phishing est une technique qu'emploient les pirates pour voler , le plus souvent, les informations bancaires de particuliers. On a aussi observé qu'une des grandes inquiétudes des consommateurs concernait les logiciels espions capables de voler les informations sensibles et autres mots de passe. Enfin, les techniques commerciales par courriel et les fameux pourriels impactent de façon négative sur les craintes des consommateurs, leurs perceptions de l'Internet et du commerce électronique.

Dans une étude récente, Tsiakis et Stephanides (2005) révèlent que ces peurs sont également dues à un vide relationnel avec les cybermarchands du fait même de la particularité du média. Cette particularité engendrerait, chez les consommateurs, des craintes par rapport à la sécurité et à la vie privée. En effet, Internet représente une association complexe d'acteurs humains et de systèmes technologiques qui rend difficile la construction de la confiance du fait même d'un vide relationnel (Friedman et al., 2000). Ces résultats confirment les travaux de Jones et Vijayasarathy (1998) qui ont étudié en laboratoire le comportement des consommateurs. Ils ont constaté qu'il y a plus de risque perçu à magasiner en ligne qu'à feuilleter un catalogue papier. On peut, de fait, logiquement imaginer que ces craintes par rapport au média affectent clairement la volonté d'acheter sur Internet.

Quant à Phelps et al. (2000, voir Vincent, 2004), ils établissent que le niveau d'alerte des consommateurs par rapport aux informations fournies s'articule autour de quatre facteurs : le type d'information récoltée, le degré de contrôle sur les renseignements fournis, les avantages et désavantages possibles de l'envoi de ces informations, et les caractéristiques individuelles. Il apparaît que ces facteurs sont perçus comme étant les antécédents des inquiétudes des consommateurs. Enfin, il est à noter que d'autres variables affectent significativement la perception qu'ont les consommateurs du traitement de l'information livrée à l'entreprise. Dans le marketing direct, selon l'étude de Phelps et al. (2000, voir Vincent, 2004), trois antécédents seraient aussi fortement corrélés avec l'inquiétude des consommateurs concernant la vie privée. Ces

antécédents se fonderaient sur les croyances à l'égard du marketing direct, l'attitude par rapport au marketing direct et enfin les comportements antérieurs quant au retrait des listes de distributions.

1.1.2 L'ensemble des processus de régulation mis en place pour atténuer les craintes des consommateurs

Tout d'abord, comme le soulignent Suh et Han (2003), la sécurité et le contrôle perçu de cette sécurité par le consommateur sont un pré requis crucial pour le bon fonctionnement du commerce électronique et pour son acceptation par le grand public. Ils sont aussi un pré requis pour la confiance que l'on accorde en fonction des moyens mis en place pour assurer la confidentialité, la fiabilité et la protection de l'information. Dans cette seconde partie, nous nous attachons à mieux comprendre l'ensemble des processus de régulation mis en place pour minimiser les inquiétudes des consommateurs ainsi que les comportements qui en découlent. Il est à noter que cette partie traite des mécanismes liés à la sécurité et à la vie privée nécessaires à la mise en place de services de sécurité efficaces.

Neuman (1991) énumère un certain nombre de conditions que tout individu exige de la sécurité dans le domaine particulier des systèmes d'informations s'appliquant parfaitement au commerce électronique :

- Premièrement, l'observance des droits privés et des intérêts de l'individu. En d'autres termes les individus se doivent d'être avertis du traitement qui sera fait de leurs renseignements personnels, ainsi que de la possibilité d'avoir accès aux informations pour les modifier ou les supprimer.
- Deuxièmement, la prévention par la mise en place de technologies et de politiques destinées à empêcher des comportements humains indésirables. Tout ceci inclut les procédures mises en place pour empêcher l'intrusion de scripts malveillants, de virus espions, de sabotages ou d'actes antisociaux .
- Troisièmement, la prévention face aux accidents de systèmes. En commerce électronique, nous pouvons associer cela à la permanence d'un service irréprochable en termes d'accessibilité au site Internet, au paiement en ligne et à la livraison.

- Dernièrement, un système qui permet l'équilibre des droits entre les individus et les cybermarchands, autrement dit un recours légal pour combattre la non répudiation.

Par exemple, la première des techniques liée au paiement sécurisé en ligne et protégeant le consommateur dans l'environnement électronique se base sur le cryptage (Encryption) des données. D'après Tsiakis et Stephanides (2005), ce programme permet d'assurer un service de confidentialité, d'authentification et d'intégrité. La seconde de ces procédures réside dans les signatures digitales (Digital Signatures). Toujours d'après Tsiakis et Stephanides (2005), celles ci permettent l'authentification, la protection de l'intégrité et la non répudiation. Cette technique permet de protéger l'anonymat du consommateur lors de la divulgation de renseignements personnels dits sensibles. Dans ce type de système, une personne appelée signataire est désignée à produire une signature digitale; d'autre part, nous avons les demandeurs réclamant la signature de l'information envoyée au signataire (Juang et al., 2002). Cette signature électronique permet donc d'identifier le signataire d'un document électronique par l'utilisation d'un algorithme de chiffrement, basé sur des clefs, qui rend possible la vérification de l'intégrité du document et l'assurance de la non répudiation (Office Québécois de la langue Française). Enfin, la dernière procédure est l'algorithme de hachage (Hash algorithms) qui fait aussi partie intégrante des signatures digitales avec l'algorithme de chiffrement, basé sur des clefs que nous avons mentionnées précédemment. Elle assure de la même manière l'intégrité et l'authentification.

Néanmoins, des failles majeures concernant ces techniques ont été plusieurs fois décelées de nature à inquiéter le public par rapport au média et au commerce électronique. Ainsi, Suh et Han (2003) mentionnent les cas de Microsoft Hotmail et de leur fameuse brèche sur la sécurité du mot de passe ou bien encore l'attaque dont avait été victime Amazon sur sa page d'accueil.

Les procédures de cryptage et autres signatures digitales se basant sur des algorithmes complexes ne sont pas les seules solutions qu'utilisent les marchands électroniques pour réduire les craintes des consommateurs et assurer un service de confidentialité,

de non répudiation ou bien encore d'intégrité des données et d'authentification. Parmi les techniques que nous pouvons rencontrer sur Internet destinées à vendre de la confiance, nous mentionnerons les tiers partis ou labels de sécurité. Pour exemple, TRUSTe Trustmark, CPA Web Trust, BBBOnline ou bien encore Web Shield sont les assureurs les plus connus pour tenter de limiter les craintes des consommateurs. Ces différents labels s'acquièrent par la juste rédaction d'une politique de confidentialité par un cybermarchand. Celui-ci doit clairement la faire apparaître et mentionner le fait que de l'information privée est recueillie lors d'une transaction. La politique de confidentialité doit aussi faire apparaître de quelle manière les renseignements personnels des consommateurs seront utilisés et dans quel but.

Bélanger et al. (2002) ont très largement étudié l'efficacité de ces tiers partis et des politiques de confidentialité. Ils ont découvert que ces techniques ont un effet positif sur la confiance interpersonnelle que l'on alloue au cybermarchand et plus particulièrement les dimensions de l'intégrité et la compétence perçues. Cependant, ils nous mentionnent aussi que pour qu'un label soit efficace lors de la relation entre un consommateur et un cybermarchand, le tiers parti se doit aussi d'être cru et reconnu par l'individu magasinant.

En ce qui concerne Moores (2005), il explique que bien que l'existence des labels chez le cybermarchand soit comprise par les consommateurs comme une nécessité de survie pour ce dernier - à savoir la promotion d'une sécurité d'achat - les consommateurs s'interrogent sur l'acquisition de ces labels par le cybermarchand. De plus, alors que la totalité de l'échantillon de Moores (2005) avait déjà acheté sur Internet, seulement une personne sur trois tendait à croire un cybermarchand uniquement dans la mesure où il figurait un label de confidentialité. Un résultat qui minimise fortement l'efficacité de ces labels par la non-compréhension des consommateurs des processus d'acquisition des labels.

En plus de la sécurité et des labels des tiers partis qui limitent sensiblement les craintes des consommateurs, les inquiétudes liées à la vie privée semblent avoir une corrélation négative sur l'adoption de l'Internet en tant que media pour magasiner.

Hoffman et al. (1999) démontrent dans une étude que les plus grandes craintes des consommateurs sont rattachées aux informations privées et au contrôle que l'on a sur ces dernières. L'étude démontre aussi que les raisons premières de certains consommateurs pour ne pas acheter sur Internet n'étaient pas fonctionnelles, mais uniquement dues à un contrôle perçu sur les informations personnelles insuffisant. De même, beaucoup de recherches ont permis d'établir que les préoccupations vis-à-vis de la vie privée ont un impact négatif sur l'intention comportementale surtout lorsque les consommateurs ne se sentent pas en contrôle au sujet des informations qu'ils fournissent (Phelps et al. 2000).

1.2 Le contrôle et le commerce électronique

Dans le but de mieux comprendre la notion du contrôle ainsi que son importance dans le milieu du commerce électronique, il nous semble primordial de devoir s'attarder sur les aspects théoriques de la notion de contrôle perçu qui ont été étudiés dans divers domaines de recherche. Il sera alors question dans cette section, de mieux saisir ce construit qui forme le centre de notre recherche. De fait, ce chapitre nous permettra de déterminer quelle définition donner au sentiment de contrôle lorsque l'on traite de la divulgation de renseignements personnels sur le media Internet.

1.2.1 Le concept du contrôle perçu

Le concept du contrôle perçu a pris, ces dernières années, une importance considérable et toujours grandissante dans la recherche et dans des disciplines telles que le marketing, la psychologie ou bien encore le comportement organisationnel (Friedman & Lackey, 1991; Lacey, 1979; Sargent & Terry, 1998; Skinner, 1995).

Selon Ajzen (1985, 1991), le contrôle perçu est la façon dont la personne perçoit la difficulté ou la facilité d'une tâche dans le but d'aboutir à un comportement effectif. White (1959) définit le sentiment de contrôle comme un facteur essentiel de satisfaction dans les relations interpersonnelles. Le contrôle est expliqué, par ce

dernier, comme étant le besoin de démontrer une compétence, une supériorité et une maîtrise d'un environnement donné. Pour leur part Friedman et Lackey (1991) font du contrôle, le motivateur universel pour toute activité humaine. Dans la suite logique des choses, Deci et Ryan (1991) indiquent que les individus ont un besoin intérieur d'autodétermination, et que celui-ci passe nécessairement par la liberté de pouvoir contrôler pour aboutir à un comportement. En d'autres termes, l'être humain doit se sentir en contrôle. D'ailleurs Janis et Lager (1975) résument le construit ainsi, en parfaite application à l'environnement du commerce électronique :

«*La perception de contrôle se réfère aux attentes d'avoir la capacité de participer aux prises de décision dans le but d'obtenir une conséquence désirable ou d'éviter une conséquence indésirable. En somme la perception d'un individu du contrôle qu'il ou elle peut exercer s'est avérée être un très grand prédicateur du comportement et des émotions qui allaient s'en suivre.* »

A ce propos, d'après Parker et Price (1994), le sentiment de contrôle s'accompagne d'un renforcement de la concentration, de la persévérance par rapport à une tâche donnée, de l'engagement, de l'implication, de la motivation et de la performance. Tous ces facteurs, par la suite, augmentent la probabilité que la perception d'avoir le contrôle des événements aboutira à un sentiment d'indépendance et d'autonomie. Les recherches démontrent que plus grand sera le contrôle perçu, plus l'individu performera. Enfin, le contrôle perçu semble accroître la confiance d'un individu dans un environnement donné, rendant les tâches à effectuer moins stressantes et plus gratifiantes (Parker et Price, 1994).

Par ailleurs, les travaux de Bateson et Hui (1991) sont porteurs en termes d'évidences théoriques sur le rôle du contrôle perçu et celui de son influence sur le ressenti émotionnel lors d'une expérience de service. Leurs conclusions confirment les travaux effectués auparavant en psychologie environnementale, suggérant que les gens tendent à ressentir et à croire plus positivement quand ils perçoivent l'environnement sous contrôle.

De plus, il nous semble intéressant de mentionner les travaux de Rotter (1966) réalisés sur le « locus of control ». Le chercheur mentionne que le contrôle de l'individu dépend des croyances de ce dernier selon une échelle bipolaire allant du contrôle interne au contrôle externe. C'est ainsi que les personnes en contrôle interne attribuent le contrôle à leurs propres personnes et pensent êtres responsables du résultat de leurs actions tandis que les personnes en contrôle externe attribuent le résultat d'un événement à d'autres personnes, à la foi ou bien encore à la chance. Autant dire que l'attribution du contrôle (soit interne, soit externe) détermine la vision que l'individu se fait d'un événement et influence donc logiquement son comportement.

Outre le fait que la notion de contrôle perçu puisse être mesurée de façon unidimensionnelle, il est à noter que beaucoup de chercheurs se sont intéressés au construit de façon multidimensionnelle suite aux travaux de Averill (1973). Ce dernier avança la thèse que le concept du contrôle s'opérationnalise de trois façons différentes : le contrôle comportemental, le contrôle décisionnel, et le contrôle cognitif. Le contrôle comportemental se réfère à la croyance d'une personne d'avoir la capacité d'influer ou de modifier un événement. Le contrôle décisionnel concerne la possibilité de choisir parmi différentes actions qui influeront sur le cours d'un événement. Enfin, le contrôle cognitif est défini par la façon dont l'événement est interprété, évalué et intégré sur un plan cognitif.

Cette tridimensionnalité du contrôle perçu est d'ailleurs reprise par Morris et Marshall (2004) dans le milieu même des systèmes d'informations qui confirment la multidimensionnalité au niveau du contrôle cognitif et décisionnel supportant les travaux de Karasek (1979). Cependant les résultats des recherches de Morris et Marshall (2004) ne sont pas aussi satisfaisants concernant le contrôle comportemental. De fait, il apparaît que la capacité à prendre des décisions pour une action à performer (contrôle décisionnel) et la capacité à faire ces actions (contrôle comportemental) ne sont pas aussi distinctes que dans les travaux de Averill (1973). Ceci dit, Morris et Marshall (2004) insistent sur le fait qu'il n'est pas très étonnant

que la plupart des utilisateurs de systèmes d'informations ne prennent aucune décision pour accomplir une tâche si ils savent qu'ils n'en ont pas les compétences.

En ce qui concerne la dimension du contrôle cognitif, il semble qu'un sujet en situation de contrôle cognitif parvient à rassembler en un tout cohérent la plupart, si ce n'est la totalité, des données d'un problème. Au contraire, une personne en non contrôle cognitif n'a pas cette faculté, de fait « *au plan affectif, on ressent anxiété et sentiment d'impuissance ; au plan motivationnel, on renonce à résoudre le problème et, enfin, d'un point de vue cognitif, on ne parvient plus à se concentrer et l'on est moins apte à analyser les données* » (Deconchy, 2005).

Averill (1973) perçoit cette dimension du contrôle cognitif sous composée de l'évaluation et du gain d'information. Ces deux composantes déterminent donc par la suite comment un événement est interprété. Dans le cas d'un gain informationnel, l'évaluation d'un événement est relativement objective ; dans le cas d'une évaluation, l'événement est modifié par une réinterprétation cognitive pour se conformer aux besoins et aux désirs d'un individu (Averill, 1973, Faranda, 2001). Les différents travaux en psychologie démontrent d'ailleurs qu'un grand contrôle cognitif exerce un impact positif sur le bien être d'un individu et vice-versa (Averill, 1973, Langer et al., 1975). Enfin, Guseman (1981), dans le domaine du marketing, établit que les consommateurs associent le risque avec des services de nature complexe. En l'occurrence le milieu Internet, considéré comme nouveau, semble assez concerné par ce problème.

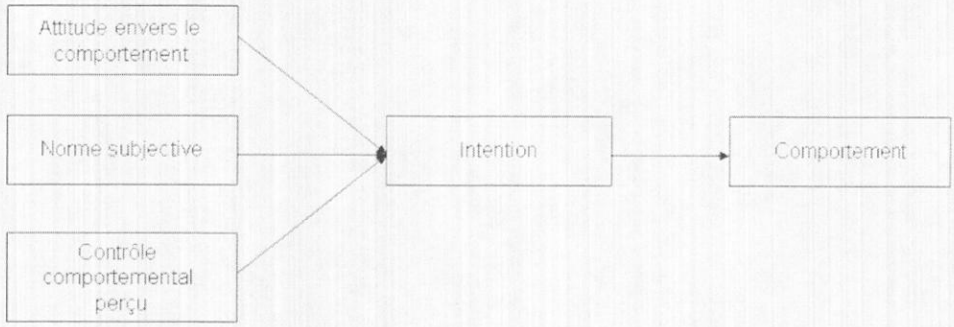
Plus concrètement, dans le contexte Web, le contrôle cognitif dépend donc de l'information que fournit le cybermarchand. Par exemple, l'internaute, considérant les renseignements fournis lors de sa navigation comme rassurants et conformes à ses attentes se sentira en contrôle. Dans le cas présent, c'est l'interprétation de la situation qui construit le sentiment de contrôle. Un individu en contrôle cognitif assimile la compétence du cybermarchand à maîtriser l'environnement comme sa propre maîtrise de la situation.

Pour ce qui touche au contrôle décisionnel, beaucoup de recherches se sont portées sur la façon de mesurer ce dernier unidimensionnellement et multidimensionnellement parlant (Smith et al., 1997). En outre, le construit a été longuement étudié par Karasek (1979) dans sa fameuse théorie sur le contrôle de l'employé sur son travail. Il circonscrit la dimension par l'autorité de décision et la liberté de décision. Quant à Nataraajan et Angur (1997), ils appellent à considérer le construit du contrôle perçu global dans le contexte du choix du consommateur. C'est ainsi qu'en raisonnant de façon plus approfondie sur l'impact du contrôle perçu sur la confiance du consommateur dans la décision, ils démontrent que la mesure spécifique du contrôle perçu accroît l'aptitude prédictive basée sur les modèles du choix d'attitudes. (Ajzen et madden, 1986, voir Faranda, 2001)

Outre mesure, le contrôle décisionnel est expliqué comme la capacité à sélectionner parmi plusieurs choix. Par exemple, si un site marchand propose une multitude de garanties par rapport à la sécurité et à la vie privée, le consommateur se sentira en contrôle décisionnel car il a le choix d'expliquer ses préférences parmi les options proposées.

Concernant le contrôle comportemental, il a été étudié et intégré comme nouvelle variable influente dans le modèle de la théorie du comportement planifié (TPB) (Ajzen, 1991). Le modèle de Ajzen (figure 1) inclut donc le contrôle comportemental comme un antécédent de la variable qui influence les intentions et le comportement. D'après le modèle TPB de Ajzen (1991), le comportement effectif individuel est déterminé par son intention de vouloir performer ce comportement. Le modèle inclut l'intention, suite logique de l'attitude envers le comportement, des normes subjectives à s'y engager, et de la perception qu'à l'individu d'être capable de s'investir dans ce dernier.

Figure 1 : Modèle de Ajzen



Source: AJZEN, I. (1991). « The theory of planned behavior », *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp.179-211.

Le contrôle comportemental dépend donc des croyances sur le contrôle et des conditions facilitatrices perçues (Ajzen et Madden, 1986). La perception du contrôle comportemental a donc une incidence sur l'intention comportementale ainsi que le comportement effectif (Chang, 1998). La définition que donne Bandura (1982) sur le concept de la maîtrise personnelle est d'ailleurs assez proche du contrôle comportemental « à la Ajzen » ; selon lui « *Le jugement de maîtrise personnelle détermine la quantité d'effort et le temps qu'on passe à faire face aux obstacles et aux expériences désagréables* ».

Par exemple, dans le contexte de l'Internet et de la protection des renseignements personnels, le fait pour un cybermarchand de communiquer une politique fondée sur le consentement préalable contribuera au contrôle comportemental des utilisateurs. En effet, le fait de pouvoir choisir ou modifier le traitement des renseignements personnels augmente le sentiment de contrôle à travers la tâche effectuée. Dans le cas contraire, le consentement implicite abaisserait le niveau du contrôle comportemental car ce format limiterait le pouvoir de l'individu à influer sur le traitement de ses renseignements personnels.

De plus, le contrôle comportemental perçu est dépendant de la facilité d'utilisation perçue d'Internet en tant que media de magasinage, du contrôle perçu dans

l'interaction, ainsi que des risques perçus liés au commerce électronique (sécurité et vie privée) (Shim et al., 2001). L'étude du contrôle comportemental et de son impact sur le media Internet semble donc plus que d'actualité et il apparaît logique que les inquiétudes des consommateurs liées à la sécurité et à la vie privée en commerce électronique soient intimement unies au construit.

1.2.2 Le contrôle perçu par rapport aux mécanismes de régulations

Comme nous avons pu le constater précédemment, le commerce électronique se porte bien malgré des craintes grandissantes vis-à-vis de l'ensemble des processus de régulation mis en place sur la grande toile qui confèrent à la sécurité. Aussi dans cette section, il sera question de bien assimiler les aspects théoriques des notions de contrôle relatifs au commerce électronique et à la divulgation de renseignements personnels. De fait, nous discuterons de la notion de contrôle perçu par rapport aux renseignements personnels ainsi que de diverses autres raisons subjectives de confiance comme antécédentes au contrôle perçu.

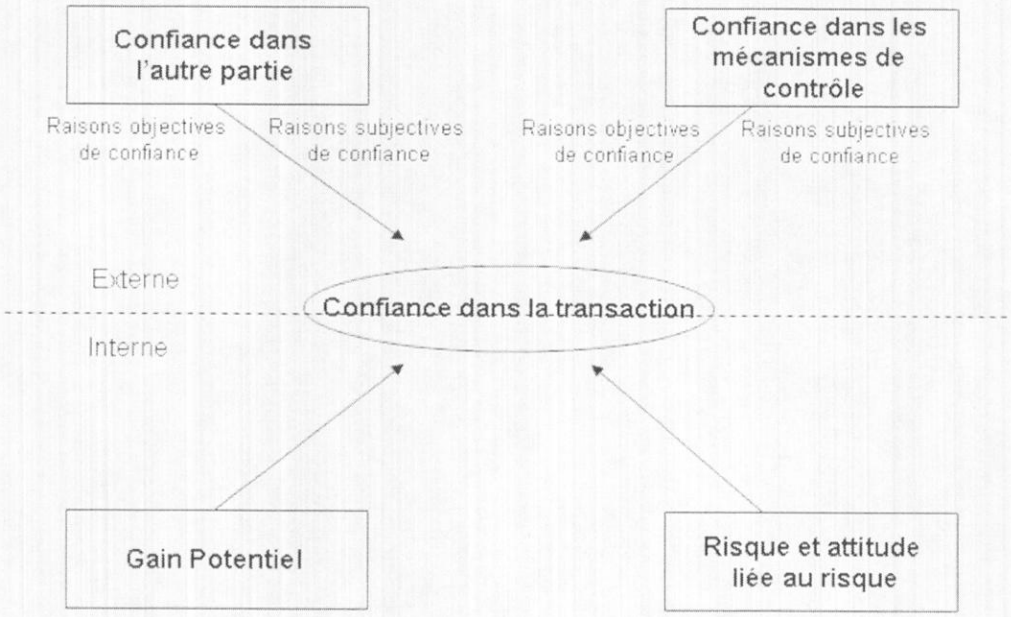
Premièrement, nous citons Tan et Thoen (2001) qui s'intéressent à ce type de contrôle sous le nom de « confiance dans le contrôle » lors de la proposition d'un modèle générique ayant trait à la confiance en commerce électronique (figure 2). Les auteurs, dans le domaine du commerce électronique expliquent qu'il existe deux sources à la notion de confiance dans la divulgation de renseignements personnels qui s'établit entre le consommateur et le cybermarchand. La première est la confiance dans le cybermarchand, la seconde est celle que nous avons mentionné précédemment, à savoir la confiance dans le contrôle, qui se fonde sur des mécanismes de régulation. Aussi la confiance dans le contrôle se base sur deux types de raisons : les raisons objectives et les raisons subjectives. Premièrement, dans les raisons objectives, nous pouvons nommer les indicateurs sociaux ; Tan et Thoen (2001) pensent que l'on croit de façon objective au contrôle des procédures car l'échange d'information s'effectue sous certification. Par exemple, on croit être sous contrôle car il y a présence d'un logo TRUSTe Trustmark ou BBBOnline. Cette dimension de croyances objectives est importante puisqu'elle s'assimile pour d'autres chercheurs à la notion de contrôle par

rapport à la sécurité (Spinellis et al., 1999, Suh et Han, 2003). De la même façon, les chercheurs Leifer et Mills (1996) perçoivent ce contrôle par rapport à l'ensemble des processus de régulation qui font que les éléments d'un système sont plus prévisibles à travers la mise en place de standards pour aboutir aux objectifs désirés.

Deuxièmement, dans les raisons subjectives nous pouvons citer l'expérience personnelle, la compréhension et la communauté.

- L'expérience personnelle : le consommateur se base sur son expérience dans le media Internet et le commerce électronique.
- La compréhension : le consommateur a tendance à se sentir sous contrôle lorsqu'il comprend les mécanismes liés à la divulgation de ses renseignements personnels chez un cybermarchand.
- La communauté : le consommateur possède une prédisposition plus ou moins grande à se croire sous contrôle dépendamment des autres gens de sa communauté.

Figure 2 : Modèle de Tan et Thoen (2001)



Source: TAN, Y-H. et THOEN, W. (2001). « Toward a Generic Model for Electronic Commerce», *International Journal of Electronic Commerce*, vol. 5, no.2, p.61-74.

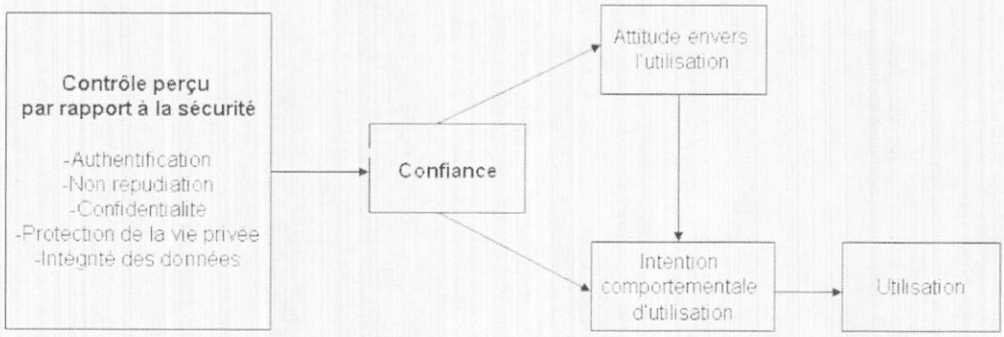
Concernant les raisons objectives mentionnées précédemment par Tan et Thoen (2001), Tsiakis et Stephanides (2005) établissent, suite aux travaux de Spinellis et al. (1999), l'existence de trois dimensions qui confèrent à la sécurité et au paiement électronique. Premièrement la sécurité du système qui concerne plus particulièrement la sécurité et l'infrastructure mise en place ainsi que ses implémentations. Deuxièmement, la sécurité des transactions qui implique la sûreté des paiements en ligne définie selon des règles spécifiques et non transgressables. Troisièmement, la sécurité légale qui indique la présence d'une structure légale autour des paiements électroniques.

D'ailleurs Spinellis et al. (1999), énumèrent plusieurs conditions requises applicables aux besoins de ce contrôle sur la sécurité. Les auteurs citent l'identification, l'authentification, le contrôle d'accès, la confidentialité, l'intégrité, la non répudiation et la disponibilité. L'identification sert seulement à identifier une personne ou une entité. L'authentification électronique permet la vérification de l'identité par l'information fournie, elle permet la juste transaction. Le contrôle d'accès est le contrôle qu'une personne possède sur les actions qu'elle entreprend. En ce qui concerne la non répudiation, elle est définie par l'impossibilité de pouvoir nier une transaction effectuée par un individu ou une entité. Enfin, la disponibilité est définie par le service continu. Pour information, en 1989, l'organisation internationale de normalisation (ISO) avait elle-même énumérée cinq des six critères que Spinellis et al. (1999) mentionnent ; à savoir l'authentification, le contrôle d'accès, la confidentialité, l'intégrité des données et la non répudiation.

Plus récemment, Suh et Han (2003) se sont penchés sur l'impact de la confiance et de la perception du contrôle par rapport à la sécurité dans le domaine des services de banque en ligne. Ils ont étudié le rôle médiateur de la confiance ainsi que l'effet de cinq sous dimensions du contrôle perçu envers la sécurité. De fait, ils ont travaillé sur l'authentification, la non répudiation, la confidentialité, la protection de la vie privée et enfin l'intégrité des données (voir figure 3). Concernant l'authentification et la non répudiation, elles ont été expliquées précédemment (Spinellis et al., 1999). En ce qui touche à la confidentialité, cette dimension assure qu'aucune information ne

transigeant entre les parties pendant une transaction ne sera utilisée par une autre partie non impliquée dans la transaction grâce, en particulier, au cryptage (Ratnasingam et al., 2005). La protection de la vie privée garantit que les renseignements personnels ne seront pas échangés après la divulgation d'informations personnelles. Enfin, l'intégrité des données signifie le juste emploi des données lors de la divulgation des renseignements personnels ; cela signifie également que ces données ne seront ni créées, ni interceptées, ni modifiées illicitement. Ces cinq sous dimensions, sur lesquelles Suh et Han (2003) ont travaillé, sont soutenues par la mise en place des mécanismes de régulation que nous avons décrits dans le chapitre précédent, à savoir, le cryptage des données, les labels des tiers partis, les signatures digitales ou bien encore les politiques de confidentialité conformes aux attentes des consommateurs. Concernant les résultats obtenus, les auteurs démontrent qu'il existe une relation positive entre trois des cinq dimensions traitées. En d'autres termes la confidentialité perçue ainsi que l'authentification perçue n'ont eu aucun effet sur la confiance. L'explication possible de ce résultat par rapport à la confidentialité s'explique sans doute par l'importance de cette dernière en tant que pré requis sur l'intégrité des données et la protection de la vie privée (Bhimani, 1996). Pour les trois dimensions ayant une relation significative avec la confiance perçue, à savoir la non répudiation, la protection de la vie privée et l'intégrité des données, on constate que les consommateurs comprennent l'importance d'être en contrôle de l'information qu'ils publient en raison des pratiques frauduleuses sévissant sur l'Internet et aux menaces par rapport à la vie privée (Suh et Han, 2003). Il est à noter cependant que 60% de la variance de la confiance est expliquée par les cinq sous dimensions étudiées dans le contrôle perçu lié à la sécurité. On peut donc en conclure que la confiance dans l'environnement, qu'elle soit institutionnelle (Internet et commerce électronique) ou interpersonnelle (le cybermarchand), dépend fortement du contrôle perçu lié à la sécurité des informations divulguées.

Figure 3 : Modèle de Suh et Han (2003)



Source : SUH, B. et HAN, I. (2003). « The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce », *International Journal of Electronic Commerce*, vol. 7, no. 3, pp.135-161.

Par ailleurs, l'un des mécanismes de sécurité les plus répandu chez les marchands électroniques est la notification d'une politique sur la vie privée (Meinert et al., 2006). Des politiques qui varient selon l'emplacement, la longueur et la lisibilité, mais surtout en fonction du niveau garanti de protection fournie (Liu et Arnett, 2002). Les recherches ont en effet démontré les effets positifs des politiques sur la confiance et le comportement effectif (Suh et Han, 2003), Cependant Meinert et al. (2006) affirment que l'efficacité d'une politique de confidentialité se base sur sa formulation et son assurance à fournir des garanties sur la protection de la vie privée.

Concernant les raisons subjectives de confiance dans le contrôle mentionnées auparavant par Tan et Thoen (2001), il nous semble important de devoir rapporter les recherches liées à la fameuse théorie du comportement planifié (TPB) ou bien encore au TAM (Technology Acceptance Model). Il est à noter toutefois que ces théories se sont attachées à décrire principalement le construit de la confiance. Cependant ces dernières se sont révélées porteuses en termes de résultats sur le contrôle comportemental perçu.

Dans le contexte du commerce électronique, Chen et Dhillon (2003), faisant suite aux travaux de Shim et al. (2001), mentionnent l'importance de la commodité perçue dans la prédiction de l'attitude par rapport au magasinage en ligne. La commodité perçue est synonyme de comment un consommateur accepte l'Internet en tant que média pour magasiner ou bien par la perception de son utilité. Il a été prouvé que l'utilité perçue du média Internet pour magasiner en ligne augmente le sentiment de contrôle comportemental (Chen et Dhillon, 2003).

La notion d'utilité perçue est d'ailleurs largement étudiée en TAM (Chiravuri et Nazareth, 2001, Dahlberg et al., 2003, Davis et al., 1989, Gefen et Straub, 2000, Pavlou, 2003, Venkatesh et al., 1989). Aussi est prouvée la corrélation positive entre l'utilité perçue et l'attitude comportementale, c'est-à-dire l'attitude envers l'utilisation de la technologie. Une corrélation positive a été une fois de plus démontrée entre l'utilité perçue et l'intention comportementale. Enfin, l'utilité perçue dépend aussi de la qualité de l'information livrée par les technologies au consommateur (Chiravuri et Nazareth, 2001).

Concernant la théorie du comportement planifié, même si Fishbein et Ajzen (1980) n'ont pas inclus le comportement passé comme un prédicateur du comportement futur, beaucoup de chercheurs ont travaillé sur le sujet et ont prouvé la relation très étroite entre le comportement passé et le comportement futur (Shim et al., 2001). De fait, en accord avec Tan et Thoen (2001), on peut penser qu'en commerce électronique, l'expérience de l'Internet et du commerce électronique est un bon prédicateur de l'attitude comportementale et de l'intention comportementale.

1.2.3 Conclusion

Les chercheurs et spécialistes ont comme leitmotiv la fonction fondamentale de la confiance dans la mise en place de stratégies e-commerce. Cependant, tout est aussi question de contrôle. Et sans contrôle perçu, la confiance ainsi que les intentions comportementales et comportements effectifs sont nuls.

Dans notre recherche, nous nous attacherons à étudier le sentiment de contrôle comportemental sur les renseignements personnels censés être soutenus par l'ensemble des processus de régulation que nous avons pris le soin d'expliquer dans ce chapitre. Aussi, si nous avons choisi le contrôle comportemental, c'est qu'il semble le plus à même d'avoir des répercussions sur les intentions et attitudes comportementales selon la théorie du comportement planifié (Fishbein et Ajzen, 1980).

Oscar Wilde disait : « Le progrès ne fait peur que lorsqu'il n'est pas contrôlé ». Cette citation pourrait très bien s'appliquer à la notion de contrôle comportemental en commerce électronique. La notion de contrôle affecte de façon significative le cybercomportement de l'internaute magasinant sur l'Internet. Un facteur que les cybermarchands ne doivent en aucun cas sous-estimer car il est à l'origine du processus de magasinage sur Internet.

1.3 La confiance et le commerce électronique

Si l'on s'intéresse à la perception des consommateurs vis-à-vis du commerce électronique et du contrôle comportemental perçu sur les renseignements personnels, il semble nécessaire de devoir nous attarder sur la notion de confiance. En effet, dans le B2C appliqué au media Internet et impliquant une nouvelle façon de commercer, tout est aussi question de confiance. D'ailleurs, Ang et al. (2001) précisent que les sondages traitant des attitudes des internautes ont constamment révélé dans le passé que le principal obstacle à la divulgation des renseignements personnels sur Internet est lié au manque de confiance. Dans cette partie, nous tenterons de mieux comprendre le construit, ses antécédents ainsi que ses conséquences.

1.3.1 Le concept du sentiment de confiance

Cette notion de confiance, que tout le monde dit connaître, est un concept délicat à définir (Taylor, 1989). Aussi, les nombreuses recherches sur le construit attestent de

la difficulté à circonscrire la notion. Au cœur de ces recherches, les définitions varient selon les domaines de recherche. Parmi les disciplines qui s'intéressèrent au construit, nous noterons l'économie, la finance, le marketing, la philosophie, la sociologie, ou bien encore la psychologie sociale.

Autrement dit, beaucoup de définitions furent exposées ces dernières années, entraînant un semblant de désordre. Cependant un des premiers à s'y intéresser fut Rotter (1971,1980) dans le domaine des relations interpersonnelles, qui définit la confiance comme *« le degré général de vérité que nous accordons à un mot, une promesse ou une déclaration verbale ou écrite d'une autre personne »*. Rotter définit ce construit comme un trait de personnalité ou une prédisposition générale.

Aussi, concernant cette variable de la confiance, plusieurs courants de recherche l'appréhendent différemment. Le premier courant perçoit celle-ci comme une variable psychologique. Dans le cas présent, l'intention comportementale est le fruit de la conceptualisation du sentiment de confiance (Morgan et Hunt, 1994). La notion travaillée serait donc assimilée à un état psychologique influant l'intention d'exercer un comportement pouvant se manifester par l'attente (Rempel et al., 1985, Sirdeshmukh et al., 2002), la présomption (Gurviez et Korchia, 2002) ou bien encore la croyance interpersonnelle (Schlenker et al., 1973). Les chercheurs ayant assimilé le sentiment de confiance à un état psychologique expliquent celui-ci comme étant sous composé d'affectif et de cognitif.

Concernant le second courant de recherche, la notion de la confiance implique uniquement la dimension conative. Aussi l'intention comportementale serait la conséquence de se rendre vulnérable par les actions d'un autre (Mayer et al., 1995). Comme le soulignent Moorman et al. (1992), la confiance n'est en aucun cas nécessaire si il n'existe aucune vulnérabilité. De la même manière, la confiance appliquée au marketing relationnel est définie par l'acceptation d'une vulnérabilité face aux actions d'un autre, et ce dans le but de recevoir des bénéfices.

Cependant, pour Rousseau et al. (1998), la dichotomie faite par les auteurs précédemment cités est loin d'être évidente. C'est ainsi, que tout en se concentrant sur le principe de vulnérabilité, ils définissent ainsi la confiance: *« A psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another »*[2].

En commerce électronique, Gefen (2000) explique que la confiance agit comme un réducteur de l'incertitude comportementale et des risques liés à la relation entre un cybermarchand apte à profiter de la confiance du consommateur et ce dernier. De fait, il explique que lorsqu'un individu croit en une entité ou autre personne, l'individu allouant sa confiance assume le fait que de l'autre coté le comportement sera le même, réduisant par la même occasion la complexité de l'interaction. En conclusion, le cyberconsommateur accordant sa confiance au cybermarchand assume le fait que le cybermarchand n'abusera pas de cette confiance par le biais d'un comportement opportuniste et mal venu.

A propos de ce risque perçu, il a été largement étudié par Pavlou (2003) dans l'étude de l'intégration de la confiance et du risque perçu dans le TAM (Technology Acceptance Model). Il a été démontré que la confiance institutionnelle, que nous étudierons par la suite, réduit la perception du risque lors la relation. Ainsi, la compétence perçue, la bienveillance perçue et l'intégrité perçue réduisent de façon significative les risques perçus. De plus, il est démontré que cette confiance réduit les risques perçus par rapport à l'environnement et donc à l'Internet. Cette confiance, par conséquent, augmente les croyances envers le cybermarchand et réduit le risque perçu par rapport à une transaction.

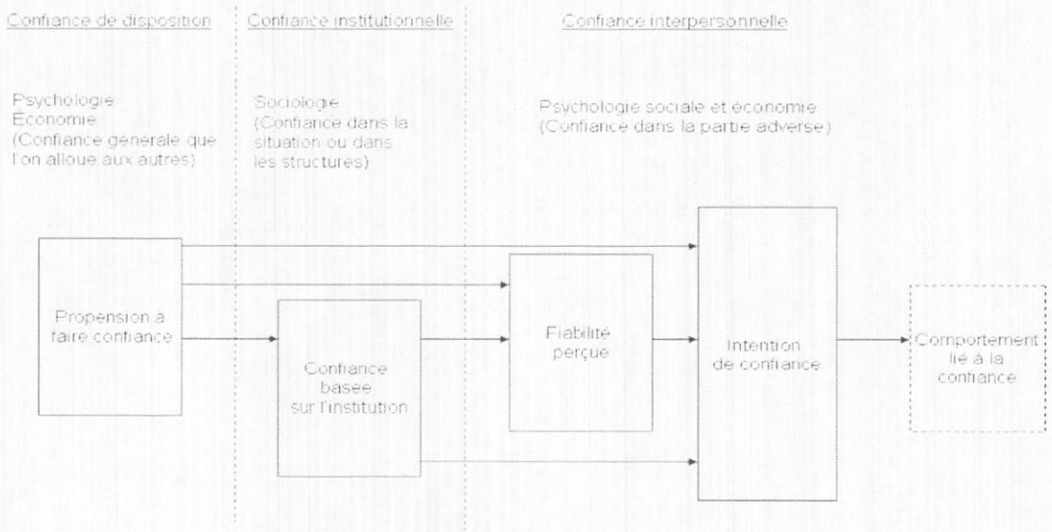
Quant à McKnight et Chervany (2002), ils ont dressé une typologie liée à la notion de confiance en commerce électronique qui s'applique très naturellement aux domaines du B2B et B2C. Cette typologie se base sur trois formes de confiance (figure 4) :

---

[2] Notre traduction : Un état psychologique comprenant l'intention d'accepter une vulnérabilité fondée sur des attentes positives d'intentions ou de comportements d'autrui

- La confiance de disposition qui se fonde sur la prédisposition générale à faire confiance à une personne ou une entité. Ce type de confiance fut précédemment étudié en économie et psychologie.
- La confiance institutionnelle largement étudiée en sociologie et qui se base par rapport à la confiance envers un situation ou une structure
- La confiance interpersonnelle étudiée en psychologie sociale et économie qui comprend la fiabilité perçue ainsi que ses conséquences comme l'intention comportementale et le comportement.

Figure 4 : Modèle de Mcknight et Chervany (2002)



Source : McKNIGHT, D.H. et CHERVANY, N.L. (2002). « What Trust Means in E-Commerce Customer Relationship », *International Journal of Electronic Commerce*, vol. 6, no. 2 (winter 2001-2002), p.35-53.

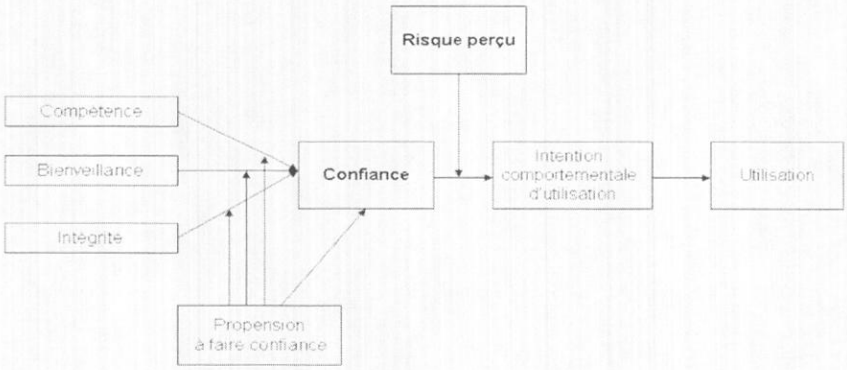
1.3.2 La notion de confiance interpersonnelle

Après les travaux de Mayer et al. (1995), beaucoup s'accordent à dire que la notion de confiance se base sur une tridimensionnalité certaine (Cheung et Lee, 2001, Gefen, 2002, Lee et Turban, 2001). En effet les travaux de Mayer et al. ont identifié que les recherches passées n'avaient pas permis de comprendre clairement les relations entre

la confiance et le risque. Mayer et al. (1995) ont mis le doigt sur le fait qu'il avait toujours existé une confusion entre antécédents de la confiance et conséquences.

De fait, ces mêmes auteurs ont défini la confiance, comme une volonté de se rendre vulnérable induisant une prise de risque de la part du consommateur. Aussi, la capacité, l'intégrité et la bienveillance sont vues comme des antécédents de la notion de confiance perçue globale; Mayer et al. (1995), avec leur modèle (Figure 5), avancent que ces trois déterminants caractérisent la fiabilité perçue du consommateur envers un marchand ou bien encore, la dimensionnalité de la confiance interpersonnelle ou confiance dyadique. Tan et Sutherland (2004) précisent que cette confiance interpersonnelle se focalise uniquement sur la confiance que l'on peut accorder à un cybermarchand.

Figure 5 : Modèle de Mayer et al. (1995)



Source : MAYER, R.C., DAVIS, J.H., SCHOORMAN, F.D. (1995). « An Integrative Model of Organizational Trust », *Academy of Management Review*, vol. 20, no. 3, p.709-734.

Concernant l'intégrité perçue du consommateur, nous la définirons dans les mêmes termes que Mayer et al. (1995): *« The relationship between integrity and trust involves the trustor's perception that the trustee adheres to a set of principles that the*

trustor finds acceptable »[3]. En d'autres termes, l'intégrité touche à la perception du consommateur à propos de l'honnêteté d'un marchand. Un construit étudié par Gefen (2002), et démontrant l'existence d'un impact positif significatif sur la confiance, alors que les deux construits de la capacité et de la bienveillance n'en avaient pas.

Deuxièmement, l'intégrité n'est pas le seul construit susceptible d'avoir un impact sur la confiance perçue. Mayer et al. (1995) voient dans la bienveillance une cause dont la conséquence est la variation de la confiance perçue. Voici la définition donnée: *« Benevolence is the extent to which a trustee is believed to want to do good to the trustor aside from an egocentric profit motive. Benevolence suggests that the trustee has some specific attachment to the trustor »*[4]. Il est certain que lorsque le consommateur s'intéresse à la bienveillance d'un cybermarchand, le cyberconsommateur juge si ce dernier est intéressé par le seul profit ou au contraire par les intérêts du client (Tan et Sutberland, 2004).

Enfin, la dimension de la capacité perçue, ou compétence perçue, semble avoir une influence certaine sur le construit de la confiance. Mayer et al. (1995) la définissent ainsi: *« Ability is that group of skills, competencies and characteristics that enable a party to have influence within some specific domain »*[5]. La capacité perçue est donc une évaluation subjective du consommateur envers l'expertise et la compétence d'un vendeur (Tan et Sutberland, 2004).

Selon Jarvenpaa et al. (2000), la confiance envers une boutique électronique dépendrait aussi de la réputation perçue de cette dernière, mais aussi de sa taille perçue (figure 6). De fait, il a été prouvé que la taille ainsi que la réputation perçue d'un cybermarchand sont corrélées positivement avec la confiance interpersonnelle

---

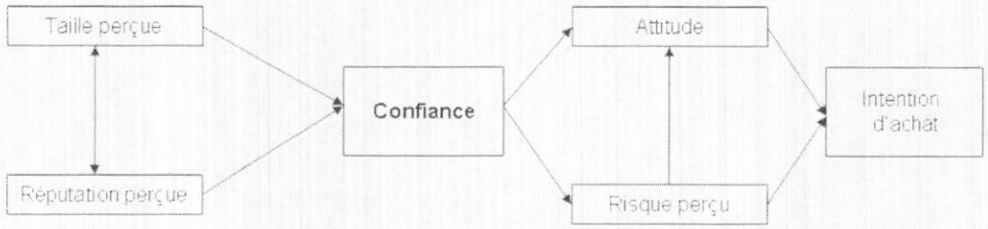
[3] Notre traduction : La relation entre l'intégrité et la confiance implique que la perception de celui qui fait confiance à la personne ou entité confidente adhère à l'ensemble des principes que ce dernier trouve acceptables.

[4] Notre traduction : La bienveillance est la mesure dans laquelle une entité ou un individu se rend crédible par une attitude à vouloir faire du bien autour de lui plutôt que d'être motivé par son seul profit. La bienveillance suggère qu'un confident a un certain attachement avec la personne ou l'entité qu'elle croit.

[5] Notre traduction : La compétence est un ensemble d'habilités, d'aptitudes et de caractéristiques qui permettent à un partie d'avoir une influence dans un domaine spécifique.

perçue. Pavlou (2003) arrive à la même conclusion concernant le seul antécédent de la réputation par une corrélation positive avec la confiance interpersonnelle. Il est, par conséquent admis que la réputation joue un rôle dans l'intention comportementale d'aboutir à une transaction ou à une divulgation de renseignements personnels.

Figure 6 : Modèle de Jarvenpaa et al. (2000)



Source : JARVENPAA, S.L., TRACTINSKY, N., VITALE, M. (2000). « Consumer trust in an Internet store », *Information Technology and Management*, vol. 1, no. 1-2, p.45-71.

1.3.3 La notion de confiance institutionnelle

Comme nous l'avons précisé auparavant, la notion de confiance s'inscrit dans une tridimensionnalité, à savoir la dimension de la confiance interpersonnelle largement étudiée par Mayer et al. (1995), mais aussi le sentiment de confiance institutionnelle ainsi que le sentiment de la confiance de disposition.

Concernant la confiance institutionnelle, elle part d'un point de vue sociologique puisque la confiance est une structure sociale construite autour d'une situation (Tan et Sutberland, 2004). Dans le domaine de l'Internet, cette dimension concerne la croyance générale qu'on a du media d'un point de vue technologique. McKnight et al. (2002) perçoivent la confiance institutionnelle comme une croyance de l'individu fondée sur des conditions structurelles présentes, et ce dans le but d'augmenter la probabilité d'aboutir à un résultat positif .

De plus, McKnight et Chervany (2002) ont adapté un modèle permettant d'étudier les antécédents de la notion d'intention de confiance. Outre l'intégration en tant qu'antécédents de processus cognitifs, de la propension à la confiance et de la confiance interpersonnelle dans leur modèle, ils ont aussi étudié la notion de confiance institutionnelle. Une confiance institutionnelle qui s'avéra par la suite avoir une corrélation positive avec l'intention de faire confiance.

De fait, dans un premier temps, cette dimension confère aux sous-dimensions de l'assurance structurelle donc au domaine de la régulation, de la protection légale ou bien encore de la protection technique faisant varier la confiance interpersonnelle (Tan et Sutberland, 2004). Shapiro (voir McKnight et al., 1998) réfère l'assurance structurelle à de la protection indépendante du cybermarchand en terme institutionnel. On parle là aussi de régulation, de garanties et de recours légaux mettant les cybermarchands face aux mêmes réalités auxquelles ils ne peuvent se soustraire. Quant à Ratnasingam (2005), elle conçoit cette confiance institutionnelle autour de standards techniques, de procédures de sécurité et de mécanismes de protection qui permettent d'apporter des solutions techniques aux inquiétudes.

Enfin, il parait important de souligner comme l'ont fait McKnight et al. (2002), la distinction entre cette confiance institutionnelle basée sur l'assurance structurelle et la confiance interpersonnelle :

"The distinction between trusting beliefs about a specific vendor and institution-based trust is important. Third-party icons that address general security may enhance perceptions about the Internet, but not beliefs about a specific vendor. On the other hand, an icon from an entity such as BBB may influence a customer's trusting beliefs in a specific vendor, but may do nothing to appease the consumer's uneasiness about the general security of the Web"[6].

---

[6] Notre traduction : La distinction entre les croyances liées à la confiance envers un vendeur spécifique et la confiance liée à une institution est importante. Les icônes des tiers partis qui s'adressent à la sécurité en général peuvent augmenter les croyances vis-à-vis de l'Internet, et non les croyances envers un vendeur spécifique. D'un autre coté, l'icône d'une entité comme BBB peut influer sur la confiance envers un vendeur spécifique, et ne pas apaiser les inquiétudes envers la sécurité en général sur l'Internet.

Dans un second temps, il existe la sous-dimension de la normalité situationnelle qui touche aux croyances environnementales perçues comme normales et favorables. Cette sous dimension prend bien évidemment en compte l'expérience individuelle sur Internet comme un facteur des plus influant de la confiance institutionnelle perçue (McKnight et al., 1998, Tan et Sutberland, 2004). En outre, le sentiment de confiance du consommateur envers le media, s'est révélé avoir un effet positif sur le sentiment de confiance interpersonnelle (McKnight et al., 2002).

En ce qui concerne Gefen (2000), l'auteur semble confirmer les recherches touchant à la normalité situationnelle. Après avoir travaillé sur la familiarité et ses conséquences en commerce électronique, il a démontré qu'il existe une corrélation positive entre la confiance et la familiarité. De plus, l'auteur a prouvé une même corrélation positive entre cette familiarité et l'intention comportementale d'acheter. Nous pensons aussi que cette familiarité peut s'appliquer dans le domaine de l'institution, à savoir l'expérience passée avec le commerce électronique et l'expérience d'Internet.

1.3.4 La notion de confiance de disposition

La notion de confiance de disposition a surtout été étudiée dans le domaine de la psychologie. Cette notion caractérise l'habilité et la volonté à former une croyance en général; cette dimension se définit comme un trait de personnalité qui évolue en fonction du temps et de l'individu (Tan et Sutberland, 2004). D'après Lee et Turban (2001), il apparaît clairement que la propension d'un individu à faire confiance agit comme variable modératrice entre la confiance interpersonnelle et le sentiment de confiance en lui-même. Enfin Gefen (2000) atteste que cette disposition à la confiance influence la confiance envers un vendeur. Il est à noter que la théorie de l'action raisonnée (Theory of Reasoned Action) confirme que les croyances prédisent très fortement les intentions et les comportements (Venkatesh et Davis, 2000)

Cette dimension fut particulièrement étudiée par McKnight et al. (2002) qui l'ont analysé par rapport à deux sous construits : la foi en l'humanité et la position de confiance. La foi en l'humanité est une extension de la confiance interpersonnelle qui

assume le fait que les autres sont généralement intègres, bien intentionnés et dignes de confiance. La position de confiance est une approche personnelle qui ne se base que par rapport à la post-relation, donc à l'expérience ; en d'autres termes, on a tendance à croire un cybermarchand, que celui-ci soit digne ou pas de cette confiance et ce jusqu'à ce qu'il nous prouve notre erreur par une attitude contraire.

Par ailleurs, cette disposition à faire confiance est fortement dépendante de plusieurs caractéristiques telles que la religion, la classe sociale ou bien encore l'importance de l'individu au sein de la famille (Rotter, 1971). Plus spécifiquement, les gens, tout au long de leur vie, intègrent des valeurs dans leurs propres systèmes de valeurs et les priorisent en fonction de leurs principes (Rokeash, 1971, voir Chen et Dhillon, 2003). Nous pouvons donc affirmer que les valeurs particulières d'un consommateur ont un impact sur la confiance et le comportement de ce dernier. Mayer et al. (1995) rajoutent que ces valeurs créeraient une prédisposition à la confiance.

1.3.5 Les multiples conséquences du sentiment de confiance

Comme nous avons pu le constater auparavant avec les travaux de Jarvenpaa et al. (2000) ou ceux de Pavlou (2003), la taille et la réputation perçue d'un cybermarchand ont une corrélation positive avec la confiance interpersonnelle. Cependant, ces travaux, concernant les antécédents de la notion de confiance, se sont révélés primordiaux dans l'étude des conséquences du sentiment de la confiance perçue du cybermarchand. En effet, il fut démontré l'influence positive du sentiment de confiance envers le cybermarchand sur l'attitude envers ce dernier. Il s'avère que cette confiance une fois instaurée diminue de façon significative le risque perçu pour, dans un dernier temps, se répercuter de façon positive sur l'intention d'achat. Toujours selon ces auteurs, le sentiment de confiance augmente de façon significative l'intention comportementale d'achat.

Quant à Grazioli et Jarvenpaa (2000), ils ont démontré que l'attitude d'un consommateur vis-à-vis d'un cybermarchand dépend fortement de la confiance interpersonnelle perçue. En fait, ce résultat rejoint les travaux de McKintosh et

Lockshin (1997) qui ont prouvé l'existence d'une corrélation positive entre la confiance et l'attitude à l'égard d'un magasin. Ils en concluent que pour être fidèle, ce qui constitue une intention comportementale en soi, l'attitude par rapport au magasin est une des composantes majeures dans la construction de l'intention.

Suh et Han (2003), qui ont largement étudié les antécédents de la confiance, arrivent à la même conclusion dans le milieu du commerce électronique. L'attitude à l'égard du commerce électronique est positivement corrélée avec l'intention d'utiliser le commerce électronique pour passer des transactions. Une relation positive entre l'intention et le comportement effectif est, elle aussi, déterminée.

1.4 Conclusion

Pour conclure et d'après la revue de littérature examinée, il semblerait que la variation du contrôle comportemental sur les renseignements personnels est une conséquence logique de la perception de l'individu vis-à-vis de la sécurité et de la vie privée assurée par des mécanismes de transaction, de régulation et de protection légale. Aussi, il existerait une interdépendance entre les construits du contrôle et de la confiance. Le sentiment de contrôle signifierait, alors, le sentiment de maîtrise personnelle du consommateur sur l'ensemble de ses renseignements personnels.

Concernant la confiance, il semblerait qu'elle puisse s'appliquer uniquement de façon tridimensionnelle. La divulgation d'informations privées chez un cybermarchand ainsi que la formation d'une attitude et d'une intention à utiliser ce dernier seraient influencées par une tridimensionnalité de la confiance, à savoir la confiance de disposition, la confiance institutionnelle et la confiance interpersonnelle.

Chapitre 2 : Cadre conceptuel et hypothèses

La revue de littérature exposée précédemment sert de support au chapitre que nous allons présenter maintenant, celui du cadre conceptuel de notre étude.

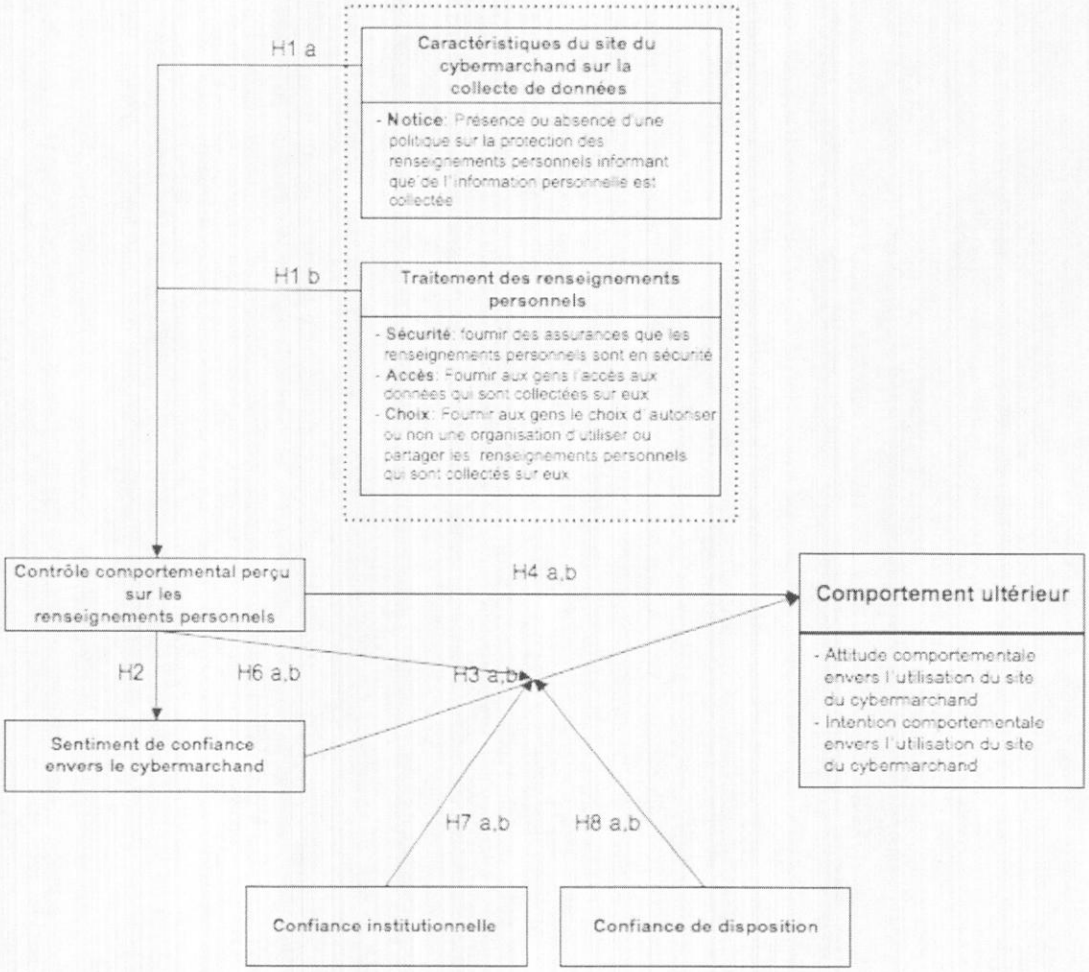
Cette partie sera l'occasion, tout en rappelant nos objectifs de recherche, d'introduire et d'expliquer de façon approfondie notre modèle conceptuel ainsi que les hypothèses qui s'y rattachent. Nous nous attarderons sur les variables manipulées, les variables dépendantes et co-variables. Enfin, nous décrirons l'opérationnalisation de cette recherche.

2.1 Cadre conceptuel

Suite à cette revue de littérature, le cadre conceptuel nous permet d'exposer une représentation schématique des liens entre les variables étudiées, leurs conséquences et les déterminants pertinents connexes au sujet d'étude. Il est important de noter que ce schéma (figure 7) est le fondement du présent mémoire.

Tout au long de la revue de littérature, nous avons tenté de démontrer l'effet néfaste des craintes des consommateurs sur la divulgation de l'information personnelle en se concentrant sur deux variables : le contrôle comportemental et la confiance. D'après plusieurs théories telles que le TAM (Technology Acceptance Model), le TPB (Theory of Planned Behavior) ou le TRA (Theory of Reasoned Action), ces deux variables ont un impact significatif sur le comportement du consommateur. C'est donc sur ces bases théoriques que nous avons souhaité développer notre problématique de recherche.

Figure 7 : Modèle conceptuel



Notre modèle s'inspire donc des modèles de Mcknight et Chervany (2002) dans l'étude de la confiance et de ses conséquences sur le comportement. Le modèle de ces auteurs intègre trois types de confiance :

- la confiance interpersonnelle
- la confiance de disposition
- la confiance institutionnelle

Nous reprenons aussi le modèle TPB (Ajzen, 1991) dans l'étude du contrôle comportemental. A noter que Ajzen (1991), a permis, par l'inclusion de la mesure du contrôle comportemental perçu, d'accroître de 11% la valeur prédictive du comportement. L'intention et l'attitude sont donc également étudiées puisque, toujours d'après le TPB, le contrôle comportemental permettrait de prévoir la valeur de l'intention à 13% (Ajzen, 1991), et d'après le TRA il serait prédit par l'attitude (Fishbein et Ajzen, 1975). L'intention, lors d'un comportement volontaire s'avère être le meilleur annonciateur de l'acte (Smetana et Adler, 1980).

Grâce à ce modèle, et en se focalisant sur la sécurité et la vie privée, nous serons alors à même de comprendre l'impact sur le comportement qu'ont la confiance et le contrôle ressenti par le consommateur lorsqu'il doit fournir des renseignements personnels à un cybermarchand.

2.1.1 Variables manipulées et formulation des hypothèses

Buchholz et Rosenthal (2002) expliquent que la vie privée inclut le concept du contrôle sur l'information personnelle divulguée. D'ailleurs la vie privée fut pendant longtemps définie comme le droit d'être « laissé tranquille » et de pouvoir contrôler son information personnelle (Warren et Brandeis, 1890). Aussi, lors de notre recherche, et dans le but de faire évoluer notre variable du contrôle comportemental perçu, nous nous appuierons sur quatre dimensions de la vie privée.

Ces dimensions sont prônées par le FTC (The Federal Trade Commission) et incluent :

- la sécurité
- l'accès
- le choix
- la notification.

Cette commission établit les bonnes pratiques vis-à-vis du traitement des renseignements personnels sur les dimensions citées précédemment (FTC Congress Report, 2000).

La sécurité :

Selon le FTC (FTC Congress Report, 2000), la sécurité doit être mentionnée dans les politiques sur la protection des renseignements personnels afin d'assurer au consommateur que les données recueillies sont bien gardées en sûreté. Il apparaît clairement que le comportement des individus dans l'environnement de l'Internet se base sur la perception de la sécurité ou de l'insécurité (Adams et Sasse, 1999). La perception de la sécurité joue donc un rôle majeur dans la genèse de la confiance en réduisant les craintes des consommateurs liées aux renseignements personnels (Jarvenpaa et Todd, 1997). Dans le même ordre d'idée, Liu et al. (2004) démontrent la corrélation positive entre la confiance et les tentatives de maintenir une sécurité raisonnable autour des renseignements personnels. Enfin, il a été largement démontré que la mention de présence de services de sécurité a un effet positif sur le comportement du consommateur (Spinellis et al., 1999, Suh et Han, 2003, Tan et Thoen, 2001).

VERISIGN, entreprise leader dans le domaine apportant des solutions de commerce électronique sécurisé, met en place des services basés sur la technologie SSL (Secure Socket Layers) qui forment « la base d'une infrastructure Internet sécurisée, en permettant aux sites Web de proposer à leurs clients un système d'échange ». VERISIGN ajoute que la base d'une infrastructure sécurisée « répond au besoin de confidentialité, d'intégrité, d'authentification et de non répudiation ». De fait, il serait intéressant de comprendre comment le contrôle perçu varie, en fonction de la mention ou la non mention des mesures de protection et des normes de sécurité susceptibles de protéger efficacement les renseignements personnels. Le consommateur se sent-il alors davantage maître de ses renseignements personnels si il est clairement mentionné qu'un système de sécurité le protège des attaques actives qui consistent à s'introduire dans un réseau pour voler et modifier des données ?

L'accès :

D'après, le FTC (FTC Congress Report, 2000), la dimension de l'accès est basée sur le fait d'offrir aux gens la possibilité d'accéder à l'information collectée sur leur propre personne afin de la vérifier, la modifier ou encore la supprimer. Il est démontré que cette dimension est positivement corrélée avec le degré général de confiance que va ressentir le consommateur (Liu et al., 2004). De fait, nous sommes portés à croire que lorsque l'individu sait que l'information personnelle qu'il divulgue lui sera accessible à tout moment, il se sentira alors plus en contrôle par rapport aux renseignements fournis. Il sera donc intéressant, lors de la manipulation, de constater l'impact sur le contrôle comportemental, selon qu'il y a présence ou absence de la mention d'accessibilité des renseignements personnels.

Le choix:

Le choix concerne la décision du consommateur de voir ses renseignements personnels révélés, être utilisés ou bien partagés à des fins promotionnelles. Cela concerne donc l'utilisation en interne et en externe des renseignements personnels. Selon le FTC (FTC Congress Report, 2000), il est dans les bonnes pratiques d'informer et de donner la possibilité au consommateur d'accepter ou non l'utilisation et le partage des renseignements. Le département américain du commerce (Safe Harbour, U.S Department of Commerce, 2000) explique d'ailleurs que dans n'importe quel établissement, les individus doivent avoir la possibilité de ne pas autoriser que l'information personnelle soit utilisée en interne ou bien partagée en externe avec des partis tierces (opt-out). Pour de l'information dite sensible, les individus devraient donc avoir la possibilité d'autoriser ou non les marchands à procéder à l'utilisation et au partage de leurs renseignements personnels (opt-in). Conséquemment aux recommandations apportées par les organismes de régulation et autres commissions, nous allons, dans notre expérience, nous appliquer à faire varier la dimension du choix dans la politique de protection des renseignements personnels en fonction de trois énoncés formulés. Les deux premiers énoncés traiteront de l'utilisation secondaire (utilisation en interne et partage pour l'externe) des renseignements personnels soit en format opt-in, en demandant la permission au consommateur, soit en format opt-out en contraignant le consommateur à se

désengager si il ne souhaite pas donner son autorisation. Le troisième et dernier énoncé portera sur la possibilité de naviguer anonymement lors d'une session soit en format opt-in, en donnant le choix au consommateur de refuser que des cookies soient enregistrés sur son ordinateur, soit en format opt-out, en indiquant les URLs de sociétés extérieures fournissant des logiciels anti-cookies. Pour information, les cookies sont de petits fichiers textes s'installant sur les ordinateurs et qui permettent aux sites Internet de retracer facilement un internaute lors de sa navigation.

La notification :

La notification concerne le fait qu'il existe, ou qu'il n'existe pas, une politique sur les renseignements personnels prônant la transparence sur l'utilisation secondaire qu'il est faite des renseignements personnels collectés. Miyasaki et Fernandez (2000), dans une étude sur les politiques de confidentialité, estiment qu'il existe une influence positive sur l'intention d'achat lorsque celles-ci sont présentes. Il sera intéressant de comprendre comment le consommateur se comporte dépendamment de sa sensibilisation à la présence ou non d'une collecte de données. Concernant cette dernière dimension, il semble que, sans souci de notification de la part du marchand à informer de la récolte de données, il n'existe logiquement aucune mention des autres dimensions de sécurité, choix et accès. De fait, nous partirons du principe qu'il existe toujours la mention d'une collecte de données si présence de politique de confidentialité, et, que la notification dépendra donc uniquement de la présence ou non de cette politique sur la protection des renseignements personnels. Conséquemment à notre position, nous nous intéresserons à mesurer le contrôle comportemental en fonction de la présence ou de l'absence d'une politique de confidentialité.

Finalement, Arcand et Nantel (2005), dans une étude empirique, avaient constaté que le fait de lire une politique de confidentialité impactait de façon négative sur le contrôle perçu, la confiance (dimension de l'intégrité), et les intentions comportementales. En d'autres termes, les auteurs avaient conclu que lorsque la politique sur la protection des renseignements personnels était présente, les individus se sentaient moins en contrôle sur leur vie privée que lorsque celle-ci n'était pas

consultée. Néanmoins, les auteurs rajoutent que la littérature touchant à la vie privée semble démontrer le contraire, du moins en ce qui concerne l'impact de la lecture d'une politique de confidentialité sur:

- La confiance (Lee et Turban, 2001, Liu et al, 2005, Suh et Han, 2003)
- L'intention comportementale (Liu et al, 2005)

Ceci nous amène à poser la première hypothèse :

H1A : De façon opérationnelle, la présence d'une politique sur la protection des renseignements personnels a un impact positif sur le sentiment de contrôle comportemental

H1B : De façon opérationnelle, le fait de pouvoir influer sur le traitement des renseignements personnels a un impact positif sur le sentiment de contrôle comportemental

2.1.2 Impact des variables dépendantes et formulation des hypothèses

Langfred (2004) affirme que le contrôle comportemental et la confiance s'exercent réciproquement lorsque qu'il existe une interdépendance entre deux parties. Une interdépendance que Knights et al. (2001) jugent présente dans le domaine de l'Internet. Cependant Langfred (2004) explique que même si la confiance interpersonnelle est présente chez les deux parties négociantes, il subsiste le problème de la complexité du contrôle sur les actions lorsqu'il existe une importante autonomie individuelle. En conséquence, il peut, certes, y avoir de la confiance entre le cybermarchand et un consommateur, ainsi qu'une réciprocité entre contrôle comportemental et confiance interpersonnelle ; néanmoins il existe aussi une forte asymétrie de pouvoir qui traduit une relation entre les deux parties fondée sur le déséquilibre. En psychologie sociale, Verlhiac (NC) souligne le lien existant entre « contrôle comportemental » et « confiance » ; ce chercheur explique que lorsqu'un sujet n'a pas confiance en ses propres capacités de contrôle, il n'a alors qu'un faible sentiment de contrôle sur les éléments négatifs qu'il peut être amené vivre, et par conséquent, il en sera affecté. En utilisant le TPB, Pavlou (2003) a découvert que le contrôle comportemental perçu est corrélé positivement à la confiance à l'égard d'un

cybermarchand. De fait, nous pensons logiquement que le contrôle comportemental perçu sur les renseignements personnels a un effet positif sur la confiance allouée à un cybermarchand.

Ceci nous amène à poser la seconde hypothèse :

H2 : Le sentiment de contrôle comportemental sur les renseignements personnels est positivement corrélé au sentiment de confiance alloué au cybermarchand (confiance interpersonnelle)

Lors d'une méta analyse, Swan et al. (1999), ont montré que la confiance du consommateur envers un vendeur (confiance interpersonnelle) a une influence bénéfique dans le développement d'une attitude, d'une intention et d'un comportement positif. De nombreuses recherches ont démontré l'effet favorable de la confiance interpersonnelle sur l'attitude (Ang et al., 2001, Grazioli et Jarvenpaa, 2000, Jarvenpaa et al., 2000, McKintosh et Lockshin, 1997, Pavlou, 2003) et sur l'intention (Gefen, 2000, McKnight et Chervany, 2002, Pavlou, 2003, Rousseau et al., 1998). D'après une étude menée en 1999, 63% des consommateurs ayant refusé de fournir des renseignements personnels à des sites Internet indiquaient que leurs comportements étaient dus à un manque de confiance (Hoffman et al., 1999).

Ce qui nous amène à poser la troisième hypothèse :

H3 : Le sentiment de confiance alloué au cybermarchand (confiance interpersonnelle) est positivement corrélé à :

- A : l'attitude comportementale envers l'utilisation du site du cybermarchand

- B : l'intention comportementale envers l'utilisation du site du cybermarchand

Tout au long de notre revue de littérature et au début de ce second chapitre, nous avons mentionné l'importance du modèle TPB. Ajzen (1988) a révélé l'influence positive du contrôle sur le comportement ; il a également démontré (1991) l'influence directe du construit sur les intentions. Taylor et Todd (1995) ont prouvé par ailleurs que ces deux théories étaient appropriées à l'étude des déterminants du comportement liés à l'utilisation des technologies. Pavlou (2003) ou bien encore George (2004) ont

d'ailleurs noté la corrélation positive entre le contrôle comportemental perçu et le comportement. Subséquemment aux arguments exposés dans la construction des deux premières hypothèses et à la corrélation positive établie entre le contrôle perçu et le comportement ultérieur dans le TPB, nous posons nos deux prochaines hypothèses.

Voici présentée notre quatrième hypothèse :

H4 : Le sentiment de contrôle comportemental sur les renseignements personnels est positivement corrélé à:

- A : l'attitude comportementale envers l'utilisation du site du cybermarchand

- B : l'intention comportementale envers l'utilisation du site du cybermarchand

Voici présentée notre cinquième hypothèse faisant logiquement suite à H2 et H3A,B :

H5 : Le sentiment de confiance joue un rôle de médiation dans la relation qui unit le contrôle comportemental perçu et :

- A : l'attitude comportementale envers l'utilisation du site du cybermarchand

- B : l'intention comportementale envers l'utilisation du site du cybermarchand

Finalement, et de façon cohérente, il sera intéressant d'étudier l'impact du sentiment de contrôle comportemental sur les renseignements personnels dans la relation qui unit le sentiment de confiance envers le cybermarchand et le comportement ultérieur.

Voici présentée notre sixième hypothèse :

H6 : Le sentiment de contrôle comportemental sur les renseignements personnels a un effet modérateur sur la relation entre le sentiment de confiance envers le cybermarchand et:

- A : l'attitude comportementale envers l'utilisation du site du cybermarchand

- B : l'intention comportementale envers l'utilisation du site du cybermarchand

2.1.3 Effets des co-variables et formulation des hypothèses

Malgré le contrôle comportemental ressenti et la confiance allouée au cybermarchand, les comportements ultérieurs peuvent aussi êtres dépendants de deux autres formes de confiance (Mcknight et al., 1998).

Concernant la première forme de confiance, elle se base sur les croyances que peut avoir un individu vis à vis de la structure et de l'assurance structurelle (McKnight et al., 1998). En outre, nous pouvons nous référer aux travaux de Shim et al. (2001) qui ont démontré que le comportement futur dépend aussi fortement du comportement antérieur sur le media. L'expérience passée dans l'Internet dépendrait donc des précédentes expériences de magasinage en ligne puisque celles-ci apparaissent avoir un impact direct sur les intentions comportementales de magasiner (Eastlick et Lotz, 1999). Cependant, Mcknight et al. (2002) pensent que l'expérience de l'Internet est seulement un antécédent de la confiance que l'on alloue au média. Aussi, les auteurs conseillent fortement d'être spécifique par rapport à l'institution. Dans le même ordre d'idée, Lee et Turban (2001) déclarent que pour qu'il y ait un comportement, la seule présence de la confiance interpersonnelle ne suffit pas.

Ce qui nous amène à poser la septième hypothèse :

H7 : Le sentiment de confiance envers le commerce électronique (confiance institutionnelle) a un effet modérateur sur la relation entre le sentiment de confiance envers le cybermarchand et:

- A : l'attitude comportementale envers l'utilisation du site du cybermarchand

- B : l'intention comportementale envers l'utilisation du site du cybermarchand

La dernière forme de confiance mentionnée dans notre revue de littérature concerne la confiance de disposition. Mcknight et al., (1998) estiment que la confiance de disposition est composée de la propension à faire confiance (Trusting Stance), ainsi que de la foi en l'humanité (Faith in humanity) en fonction de l'intégrité, de la bienveillance et de la compétence. En effet, si nous nous intéressons à ce lien, c'est que les recherches précédentes ont démontré que les deux dimensions de la confiance

de disposition influencent la confiance que l'on peut avoir dans le vendeur et donc dans le comportement du consommateur (Gefen, 2000).

Ce qui nous amène à poser la huitème et dernière hypothèse :

H8 : Le sentiment de confiance de disposition a un effet modérateur sur la relation entre le sentiment de confiance envers le cybermarchand et:

- A : l'attitude comportementale envers l'utilisation du site du cybermarchand

- B : l'intention comportementale envers l'utilisation du site du cybermarchand

2.2 Opérationnalisation des concepts clefs

Cette partie va nous permettre de comprendre les conditions expérimentales touchant aux variables indépendantes. Tandis que dans un second temps, nous nous attarderons sur l'opérationnalisation des concepts clefs de notre recherche.

2.2.1 Conditions expérimentales

Dans cette section, nous allons traiter de la façon dont se déroulera la manipulation de nos deux variables indépendantes, c'est-à-dire :

- Les caractéristiques du site du cybermarchand sur la collecte des données
- Le traitement des renseignements personnels du site du cybermarchand

Les caractéristiques du site du cybermarchand sur la collecte des données

Comme nous l'avons mentionné précédemment, les caractéristiques du site du cybermarchand varient en fonction de la présence ou de l'absence d'une notification indiquant la récolte de données. Le premier niveau de l'expérimentation présente deux conditions :

- **1ère condition niveau 1 : Absence d'une politique détaillée sur la protection des renseignements personnels**
- **2nd condition niveau 1 : présence d'une politique détaillée sur la protection des renseignements personnels**

Le traitement des renseignements personnels du site du cybermarchand

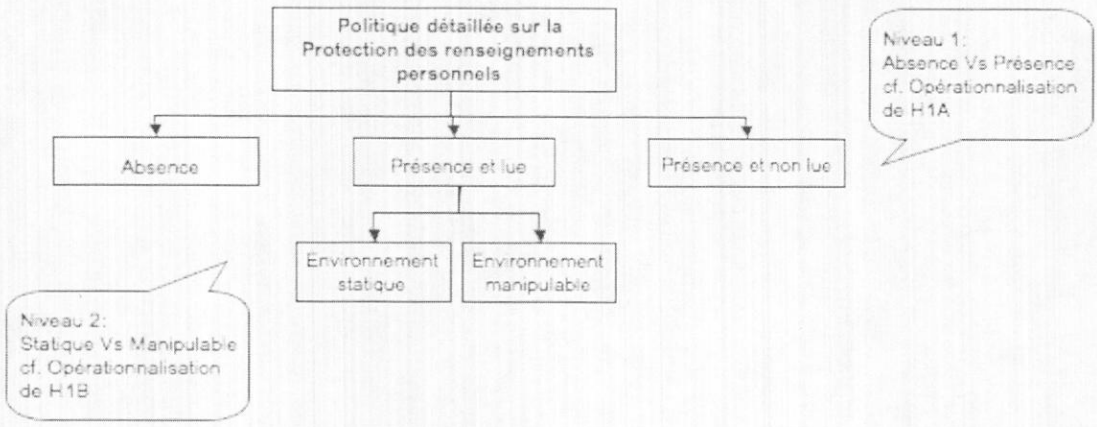
Cette partie est considérée comme le second niveau lors de l'expérimentation et implique obligatoirement la présence d'une politique détaillée sur la protection des renseignements personnels. Voici, ci-dessous, les deux conditions de notre second niveau :

- **1ère condition niveau 2 : présence d'une politique détaillée statique sur la protection des renseignements personnels consultée par l'internaute**
- **2nd condition niveau 2 : présence d'une politique détaillée dynamique sur la protection des renseignements personnels consultée par l'internaute**

Lorsque nous faisons état d'un environnement dynamique ou statique nous le voyons en fonction des critères de sécurité, accès et choix.

Voici présentée ci-dessous (figure 8) une description schématique de nos différents niveaux d'expérimentation :

Figure 8 : Description schématique des niveaux de l'expérimentation



Par conséquent, pour le traitement de notre hypothèse H1A, nous regardons s'il existe une variance du contrôle comportemental que perçoit l'individu sur ses renseignements personnels dépendamment de l'absence ou de la présence

(environnement statique et dynamique) d'une politique détaillée sur la protection des renseignements personnels. Dans un second temps, nous vérifions s'il existe une différence dans la perception du contrôle entre les personnes ayant lu la politique (environnement statique et dynamique) et les personnes ne l'ayant pas lu lorsque celle-ci était présente. Par la suite, pour le traitement de H1B, nous examinons si l'effet sur le contrôle perçu de l'individu varie en fonction de l'environnement (environnement statique versus environnement dynamique). Voici présenté ci-dessous (tableau 1) notre devis expérimental :

Tableau 1 : Devis expérimental

Niveaux	Conditions expérimentales	Contenu des conditions
1	**Absence** d'une politique détaillée sur la protection des renseignements personnels	Aucune notification présente sur le site Internet expérimental.
2A	**Présence** d'une politique détaillée statique sur la protection des renseignements personnels	Présence d'une notification sur le site Internet expérimental. *Sécurité* : Mention d'un système de contrôle basé sur la technologie SSL *Accès* : Absence de mention d'une possibilité d'accéder à tout moment à l'information divulguée *Choix* : *Format opt-out* - Utilisation en interne et externe des renseignements personnels. Format où l'utilisateur n'a aucun contrôle direct et choix de donner ou ne pas donner son accord à cette utilisation. L'entreprise ne demande aucune permission. L'utilisateur peut cependant se désengager plus tard par courriel. Concernant l'anonymat, le consommateur n'a aucun contrôle sur son anonymat lors de la navigation. Il peut cependant se diriger vers des liens en externes pour télécharger des logiciels pouvant assurer son anonymat.
2B	**Présence** d'une politique détaillée dynamique sur la protection des renseignements personnels.	Présence d'une notification sur le site Internet expérimental. *Sécurité* : Mention d'un système de contrôle basé sur la technologie SSL *Accès* : Mention d'une possibilité d'accéder à tout moment à l'information divulguée *Choix* : *Format opt-in* - Utilisation en interne et externe des renseignements personnels. Format où l'utilisateur a le contrôle direct et choix de donner ou ne pas donner son accord à cette utilisation. L'entreprise demande la permission. Concernant son anonymat, l'internaute a le contrôle direct et le choix de naviguer ou non de façon anonyme.

À noter que chaque niveau est représenté par un site expérimental variant seulement au niveau du contenu de la politique sur la protection des renseignements personnels. Nous nommons les trois sites expérimentaux :

- ***Site 1*** pour le niveau 1 (Absence de politique)
- ***Site 2A*** pour le niveau 2A (Présence d'une politique détaillée statique)
- ***Site 2B*** pour le niveau 2B (Présence d'une politique détaillée dynamique)

Voici présenté ci-dessous le contenu détaillé des politiques sur la protection des renseignements personnels pour nos deux sites expérimentaux 2A (tableau 2) et 2B (tableau 3). Nous n'intégrons pas le site expérimental 1 pour l'unique raison que le site ne possède aucun lien hypertexte vers une quelconque politique.

Tableau 2 : Contenu de la politique du site expérimental 2A

Détails du contenu de la politique sur la protection des renseignements personnels	
Sécurité	Divulguez vos renseignements personnels en toute sécurité grâce à la mise en place de la technologie d'encryptage la plus puissante qui soit actuellement disponible sur le marché. La technologie SSL 128 bits.
Accès	« Aucune mention »
Choix en opt-out	- Vous allez recevoir sous peu, nos infolettres et bien d'autres informations susceptibles de vous intéresser. Veuillez nous indiquer par courriel si vous ne désirez rien recevoir. - Vous allez recevoir sous peu des offres de nos partenaires commerciaux susceptibles de vous intéresser. Veuillez nous indiquer par courriel si vous ne désirez rien recevoir. - Dans le but de vous offrir une expérience personnalisée, nous recevons et nous enregistrons vos informations personnelles. Nous utilisons notamment des « cookies » qui seront intégrés automatiquement dans votre ordinateur. Si vous souhaitez naviguer anonymement, certaines sociétés développent des logiciels à cet effet. Voici les adresses de quelques-unes d'entre elles : http://www.anonymizer.com, http://www.idzap.com, http://www.somebody.net. Nous ne garantissons pas l'efficacité de ces produits.

Tableau 3 : Contenu de la politique du site expérimental 2B

Détails du contenu de la politique sur la protection des renseignements personnels	
Sécurité	Divulguez vos renseignements personnels en toute sécurité grâce à la mise en place de la technologie d'encryptage la plus puissante qui soit actuellement disponible sur le marché. La technologie SSL 128 bits.
Accès	À tout moment, vous pouvez accéder à l'information que vous nous avez transmise afin de la vérifier, la modifier ou encore la supprimer.
Choix en opt-in	☐ Informez nous, en cochant cette case, si vous souhaitez recevoir nos infolettres et bien d'autres informations susceptibles de vous intéresser. ☐ Informez nous, en cochant cette case, si vous souhaitez recevoir des offres de nos partenaires commerciaux susceptibles de vous intéresser. ☐ Informez nous en cochant cette case si vous souhaitez naviguer anonymement. Aucun cookie ne sera enregistré sur votre ordinateur.

2.2.2 Choix des échelles de mesures des variables dépendantes et co-variables

Voici présentée ci-dessous l'opérationnalisation des concepts clefs de notre recherche avec un récapitulatif des variables et des échelles de mesures employées (Tableau 4) pour le traitement des hypothèses H2 à H8.

Les variables du contrôle perçu et de la confiance interpersonnelle : Ces deux variables sont mesurées à partir d'échelle de Likert en 7 positions. Dans le cadre de la mesure du contrôle comportemental perçu sur les renseignements personnels, nous utilisons la même échelle de mesure que George (2004) dans un contexte de recherche très comparable au notre. Pour rappel, l'auteur a étudié – avec intégration du TPB - les relations entre les croyances à propos de la vie privée sur Internet et la confiance. Cette échelle de mesure contient trois items. Concernant le sentiment de confiance envers le cybermarchand, nous disposons d'une échelle de mesure à deux

items que Gefen (2002) a employé pour mesurer la confiance générale envers un vendeur dans l'étude de l'impact de la confiance sur le cyberconsommateur.

Les variables du comportement ultérieur :

Deux variables sont mesurées :

- l'attitude envers le cybermarchand
- l'intention comportementale.

Les deux échelles de mesure utilisées pour la mesure de « l'attitude comportementale d'utiliser le site du cybermarchand » et de « l'intention comportementale d'utiliser le site du cybermarchand » proviennent des recherches de Suh et Han (2003). À partir d'échelle de Likert en 7 positions, nous employons 5 items pour la première variable et 4 pour la seconde. Rappelons que le contexte de recherche de Suh et Han (2003) fut l'étude de l'impact de la confiance et de la perception de la sécurité dans le TAM .

Les co-variables : « la confiance de disposition» et « la confiance institutionnelle » sont mesurées d'après les échelles de mesures utilisées par Mcknight et al. (2002). La confiance de disposition est mesurée sur une échelle à 6 items intégrant la propension à faire confiance et la foi en l'intégrité des hommes. Concernant la confiance dans le commerce électronique, sur les 15 items utilisés par Mcknight et al. (2002), nous en utilisons seulement 9. Aussi il nous semble plus logique dans le cadre de notre recherche de nous attarder sur les items traitant de la normalité situationnelle en général, de la normalité situationnelle en rapport avec l'intégrité, et finalement de l'assurance structurelle perçue. Si nous avons souhaité faire un tri dans nos échelles de mesure en supprimant les items connexes à la bienveillance et à la compétence, c'est qu'il nous semble que notre recherche touche plus particulièrement à la dimension de l'intégrité puisqu'il est question de mesurer la réaction des consommateurs en fonction des politiques de protection des renseignements personnels. La séparation de l'intégrité des deux autres dimensions au sein de la confiance interpersonnelle n'apparaît pas offenser Mayer et al. (1995), puisque ceux-ci ajoutent dans leurs recherches que les trois dimensions peuvent être traitées indépendamment les unes des autres.

Tableau 4 : Variables déclarées et opérationnalisation

Variables	Fiabilité α original	Items	Auteurs	Contexte d'étude
Contrôle comportemental perçu *	0.88	3 items	George (2004)	Étude intégrant le TPB et investiguant les relations entre les croyances à propos de la vie privée sur Internet et la confiance.
Confiance envers le cybermarchand	0.91	2 items	Gefen (2002)	Impact de la confiance et de ses multiples dimensions sur les cyberconsommateurs.
Attitude comportementale	0.95	5 items	Suh et Han (2003)	Étude de l'impact de la confiance et de la perception de la sécurité dans le TAM.
Intention comportementale	0,90	4 items	Suh et Han (2003)	
Confiance de disposition	0,82 à 0,90 selon dimension	6 items	Mcknight et al. (2002)	Étude de la formation de la confiance dans l'organisation.
Confiance institutionnelle	0,85 à 0,96 selon dimension	9 items	Mcknight et al. (2002)	

* L'échelle sera adaptée au contexte de l'étude

Le profil socio démographique : il est intégré au questionnaire dans le but de mieux connaître les participants à l'étude. Les questions sont les mêmes que celles utilisées par Phelps et al. (2000) dans une étude sur les craintes liées à la confidentialité des renseignements personnels. Nous posons donc les questions de l'age, du sexe, du statut marital, de l'éducation, du statut d'emploi et du revenu.

2.2.3 Déroulement du questionnaire

Voici présentés ci-dessous le déroulement et l'ordre des questions posées dans le questionnaire :

- Questions de vérification portant sur la lecture de la politique sur la protection des renseignements personnels (6 items)
- Questions au sujet du sentiment de contrôle comportemental sur les renseignements personnels (3 items)

- Questions concernant le sentiment de confiance du consommateur vis-à-vis du cybermarchand (2 items)
- Questions concernant l'attitude comportementale quant à utiliser le site du cybermarchand (5 items)
- Questions concernant l'intention comportementale quant à utiliser le site du cybermarchand (4items)
- Questions se rapportant à la confiance du consommateur dans l'institution (9 items)
- Questions concernant la confiance de disposition du consommateur (6 items)
- Questions concernant le profil sociodémographique de l'individu

Comme nous le faisions remarquer auparavant, il n'existe pas d'item dans le questionnaire tentant de mesurer le comportement de divulgation des renseignements. De fait, un outil informatique permettant l'analyse de la navigation des internautes est mis en place afin d'étudier l'acception des internautes à ce que leurs informations privées divulguées soient utilisées et diffusées dans un but promotionnel en interne comme en externe lors de la lecture de la politique.

Chapitre 3 : Méthodologie de recherche

Dans le but d'atteindre nos objectifs de recherche, nous exposerons dans ce chapitre la méthodologie employée. La particularité de notre modèle conceptuel et les objectifs de la recherche impliquent le recours à une méthodologie expérimentale. Cette façon de procéder permet l'obtention d'une variation par la manipulation du degré de contrôle comportemental perçu sur les renseignements personnels, variable centrale dans notre recherche.

En ce qui nous concerne, la méthode expérimentale offre au consommateur la possibilité de maîtriser la politique d'un cybermarchand relative à la protection de ses renseignements personnels. Cette façon d'opérer semble la plus appropriée dans le traitement de H1A, H1B. Par la suite, la variation obtenue dans le contrôle comportemental perçu sur les renseignements personnels permettra de vérifier les hypothèses H2 à H8.

3.1 L'expérimentation

L'expérience, dans le cadre de cette recherche, consistait à diriger les consommateurs vers trois sites expérimentaux. Chaque individu était assigné de façon totalement aléatoire à l'un des trois sites; il lui était demandé de s'inscrire à un programme de recherche sur la musique en ligne, naviguer puis d'évaluer le site visité par l'entremise d'un questionnaire. Cette partie de chapitre examine les sites Internet marchands construits ainsi que les différentes étapes liées à l'expérience.

3.1.1 Description approfondie des conditions expérimentales

Comme mentionné dans le chapitre précédent, nous avons mis à disposition de la recherche trois sites Internet expérimentaux dont la seule variation se situait au niveau de la politique quant à la protection des renseignements personnels. Dans le cas du premier site Internet (site 1), il n'existait pas de politique détaillée visant à informer les consommateurs d'une récolte de données, ni de la protection mise en

place pour protéger ces dernières. À l'inverse, les sites 2A et 2B portaient la mention d'une politique. Cependant ces deux sites variaient en fonction de l'environnement. La politique relative à la protection des renseignements personnels était donc statique dans le site 2A, tandis qu'elle était sous le contrôle de l'usagé dans le site 2B.

Nous exposons les contenus des conditions expérimentales dépendamment des cinq dimensions exposées auparavant et en fonction du devis expérimental réalisé lors de notre second chapitre (tableau 1) :

- *Les caractéristiques du site du cybermarchand sur la collecte des données :*

  - Absence totale de lien hypertexte sur le site expérimental conduisant vers une politique détaillée sur la protection des renseignements personnels. Cette condition expérimentale s'applique uniquement au site 1.

  - Présence, par lien hypertexte, d'une politique détaillée quant à la protection des renseignements personnels. Ce lien (dont l'ouverture se fait en pop up) se situe dans la page html qui intègre le formulaire d'inscription. Cette condition expérimentale s'applique pour les sites 2A et 2B.

- *La dimension de la sécurité au sein de la politique :*

  - Mention à l'intérieur de la fenêtre pop up – exposant la politique relative à la protection des renseignements personnels - d'un système de contrôle basé sur la technologie SSL. La présence d'une notification de sécurité est effective pour le site 2A comme pour le site 2B du fait même de l'incapacité à donner un quelconque contrôle réaliste sur cette dimension.

- *La dimension de l'accès au sein de la politique :*

  - Absence totale de mention à l'intérieur de la fenêtre pop up qui aurait informé le consommateur de la possibilité d'accéder à tout moment à ses informations personnelles et bancaires divulguées. Cette condition expérimentale s'applique seulement dans le cas du site 2A.

  - Mention à l'intérieur de la fenêtre pop up qui informe le consommateur de la possibilité d'accéder à tout moment à ses informations personnelles et

bancaires divulguées. Cette condition expérimentale s'applique seulement dans le cas du site 2B.

- *La dimension du choix au sein de la politique :*

  - Présence en format opt-out de la dimension du choix à l'intérieur de la fenêtre pop up. Le consommateur a le choix, en envoyant un courriel, de se soustraire aux activités marketing du site Internet marchand et de ses partenaires commerciaux. Cette condition expérimentale s'applique dans le cas du site 2A.

  - Présence en format opt-out de la dimension de l'anonymat à l'intérieur de la fenêtre pop up. Le consommateur a le choix, en se rendant sur des sites spécialisés, d'installer un logiciel empêchant au cybermarchand d'enregistrer les informations personnelles via les « cookies ». Cette condition expérimentale s'applique dans le cas du site 2A.

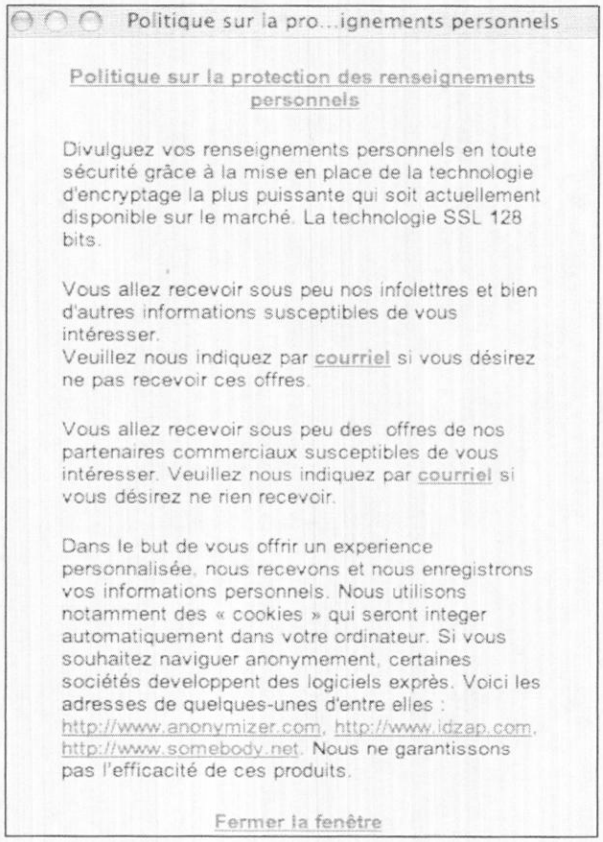
  - Présence en format opt-in de la dimension du choix à l'intérieur de la fenêtre pop up. Le consommateur a le choix d'accepter ou refuser le fait que les informations qu'il divulgue soient partagées en interne et/ou en externe. Cette condition expérimentale s'applique dans le cas du site 2B.

  - Présence en format opt-in de la dimension de l'anonymat à l'intérieur de la fenêtre pop up. Le consommateur a le choix d'accepter ou refuser le fait que ses informations personnelles soient enregistrées via les « cookies ». Cette condition expérimentale s'applique dans le cas du site 2B.

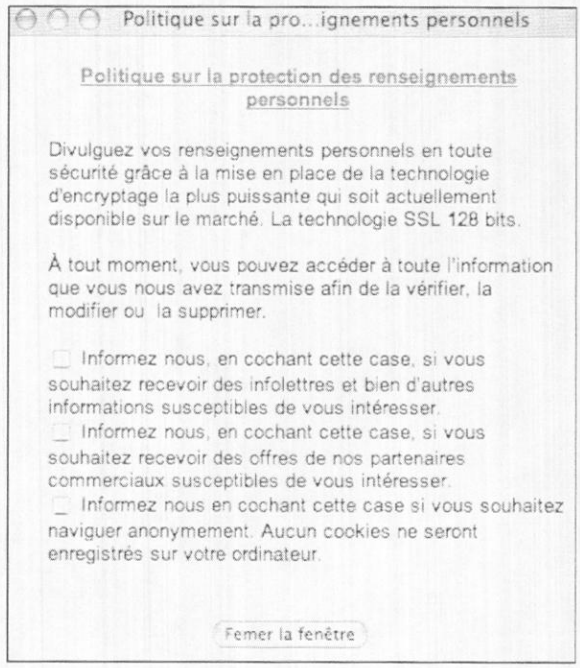
Par conséquent, d'après les contenus des politiques relatives à la protection des renseignements personnels expliqués dans le second chapitre (tableau 2 et tableau 3) pour les sites 2A et 2B, et d'après l'information énoncée ci-dessus révélant l'endroit où est située l'intégration concrète des politiques sur les sites Internet expérimentaux, nous sommes en mesure de présenter ci-dessous les fenêtres pop up des politiques et leur contenu exact.

Figure 9 : Les pop-ups de politique sur la protection des renseignements personnels

Pop up de politique sur la protection des renseignements personnels pour le site **2A**



Pop up de politique sur la protection des renseignements personnels pour le site **2B**



3.1.2 Description des sites Internet expérimentaux

3.1.2.1 Annonce de l'expérience

L'expérience démarrait par l'envoi d'une annonce courriel (figure 10) à 840 personnes du panel de la Chaire de Commerce Électronique RBC Groupe Financier.

Figure 10 : Annonce courriel

Bonjour,

La Chaire RBC en commerce électronique <http://hec.ca/chairerbc> vous invite à participer à une étude portant sur les habitudes d'écoute et d'acquisition de la musique sur le Web.
Nous sommes donc à la recherche de participants, pour naviguer sur le site de l'étude et répondre à quelques questions en ligne. En acceptant de participer, vous courrez la chance de gagner **un prix en argent d'une valeur de 400 Dollars ou un iPod nano de 4Giga !**

Pour obtenir plus de détails et pour participer à l'étude, cliquer sur le lien suivant : http://www.net-question.com/etude96
Vous pouvez également copier ce lien et le coller dans le champ de de votre navigateur réservé à la saisie des adresses de navigation.

Merci infiniment pour votre participation et pour votre précieuse collaboration!
Chaire RBC en Commerce électronique

N.B : Vous avez reçu ce message parce que vous vous êtes inscrit(e) à notre panel. Toutefois, si vous souhaitez vous désinscrire vous pouvez le faire en nous retournant ce message en précisant en objet « DESINSCRIPTION ».

L'adresse URL présentée dans l'annonce était un lien hypertexte renvoyant de façon aléatoire à l'un des trois sites expérimentaux. Le consommateur α avait donc autant de chance de naviguer sur le site 1 que sur le site 2A ou 2B. Chaque participant avait la possibilité de gagner un prix en argent de 400$CAN ou un iPod nano 4Giga.

3.1.2.2 Architecture commune à tous les sites Internet expérimentaux

Lors de cette recherche, nous avons décidé de faire naviguer les consommateurs sur un site Internet de la Chaire de Commerce Électronique RBC Groupe Financier comportant en son sein un site réel de la grande toile. En d'autres termes, les 3 sites expérimentaux dont l'architecture et le contenu étaient identiques - mis à part la politique relative à la protection des renseignements personnels - comportaient :

- Une première page présentant les directives quant aux principes éthiques (figure 11). Cette page permettait à l'internaute de bien comprendre la portée de l'expérience, sa durée, la politique de confidentialité de la Chaire de

Commerce Électronique RBC Groupe Financier ainsi que le contact du chercheur principal. Il est important de mentionner que lorsque les individus sondés ne faisaient pas partie du panel de la Chaire de Commerce Électronique RBC Groupe Financier (cf. Pré-test), l'internaute devait alors accepter de s'inscrire au panel de la chaire pour participer à la recherche.

- La seconde page était une page expliquant les taches à réaliser (figure 12).
- La troisième page était celle au centre de l'expérience. Elle contenait un site Internet marchand réel entouré d'un cadre fixe de la chaire de commerce électronique RBC Groupe Financier (figure 13).

Figure 11 : Page Index à tous les sites expérimentaux

HEC Montréal – Recherche sur les attitudes des consommat...e aux pratiques commerciales des marchands électroniques

eBay canada Informations (171) Mac Sports (91) Voyages Musique Mon actu aide statistique logement download

HEC Montréal – Recherche ...

HEC MONTRÉAL

Bonjour Madame, bonjour Monsieur,

Je suis étudiant en maîtrise de marketing à l'école des Hautes Études Commerciales (HEC Montréal). Dans le cadre de ma formation, j'effectue une recherche sur les attitudes des consommateurs face aux pratiques commerciales des marchands électroniques. Vous allez donc être soumis à une expérimentation sur les attitudes des consommateurs face aux pratiques commerciales des marchands électroniques.

Vous avez donc choisi de prendre part à cette étude et donc de participer à cette expérience se déroulant en trois étapes :

- S'inscrire à notre programme de recherche RBC Groupe Financier sur les habitudes d'écoute et d'acquisition de la musique en ligne en répondant à une première courte enquête. Ne vous inquiétez pas, aucune compétence n'est requise.
- Naviguer sur le site Internet Sirius et s'informer sur ce que propose ce marchand en termes de service
- Répondre au questionnaire de la recherche

Vous devez vous inscrire et répondre au questionnaire pour courir la chance de gagner au tirage au sort le iPod nano 4 Gigas

Lors de cette étude, ayez à l'esprit que vous êtes sur un site expérimental de la chaire de recherche RBC Groupe Financier (HEC Montréal). Votre identité en tant que participant ne pourra être retracée à partir des résultats que nous diffuserons. Tous les renseignements personnels collectés seront gardés en sécurité et en toute confidentialité par la chaire de recherche RBC Groupe Financier (HEC Montréal) malgré tout ce que vous pourrez lire lors de votre expérience dans les scénarios ou les politiques sur les renseignements personnels proposés. Notez que l'expérience commence dès que vous avez cliqué sur « Participer et commencer l'expérience ».

Répondez sans hésitation aux questions incluses dans les questionnaires, car ce sont vos premières impressions qui reflètent généralement le mieux votre pensée. Il n'y a pas de limite de temps pour répondre aux questionnaires, bien que nous avons estimé que cela devrait vous prendre environ 20 minutes.

Compte tenu des mesures de confidentialité qui seront prises, votre participation ne devrait vous causer aucun préjudice pas plus qu'elle ne vous profitera directement. Vos réponses devraient nous permettre de contribuer au développement des connaissances en marketing. Les informations recueillies resteront strictement confidentielles, et ne seront utilisées que pour l'avancement des connaissances et la diffusion des résultats globaux dans des forums savants ou professionnels.

Vous êtes complètement libre de refuser de participer à ce projet, et vous pouvez décider en tout temps d'arrêter de répondre aux questions. Le fait de remplir ce questionnaire sera considéré comme votre consentement à participer à notre recherche. Si vous avez des questions concernant cette recherche, vous pouvez contacter le chercheur principal, Monsieur Mathieu Arles-Dufour au numéro de téléphone et/ou à l'adresse de courriel indiqués ci-dessous.

Merci de votre précieuse collaboration!

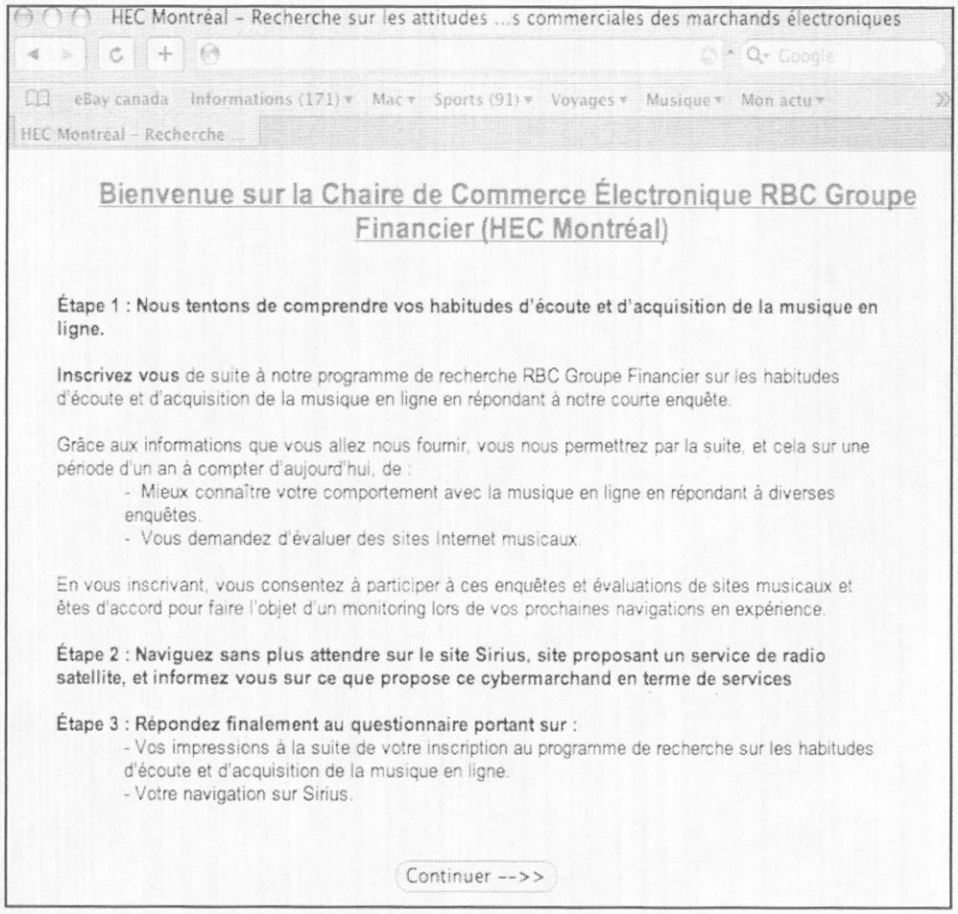
Mathieu Arles-Dufour
mathieu.arles-dufour@hec.ca

☐ ***J'affirme que j'ai pris connaissance des renseignements sur la présente recherche***
☐ ***Je comprends que le fait de répondre au questionnaire (en étape 3) correspond à donner mon consentement à participer à la recherche***

Le comité d'éthique de la recherche de HEC Montréal a statué que la collecte d'information liée à la présente étude satisfait aux normes éthiques en recherche auprès des êtres humains. Pour toute question en matière d'éthique, vous pouvez contacter le secrétariat de ce comité au (514) 340-6257.

Participer et commencer l'expérience -->>

Figure 12 : Seconde page informant des taches à réaliser



L'intérêt d'utiliser un cybermarchand authentique sur notre troisième page était de donner le sentiment à l'individu sondé qu'il naviguait sur un site marchand réel alors qu'il se trouvait sur un site expérimental de la Chaire de Commerce Electronique RBC Groupe Financier. Le second intérêt, dans l'utilisation d'un site Internet réel, était d'impliquer le consommateur lors de sa navigation afin qu'il soit apte à mieux traiter l'information à laquelle il était exposé.

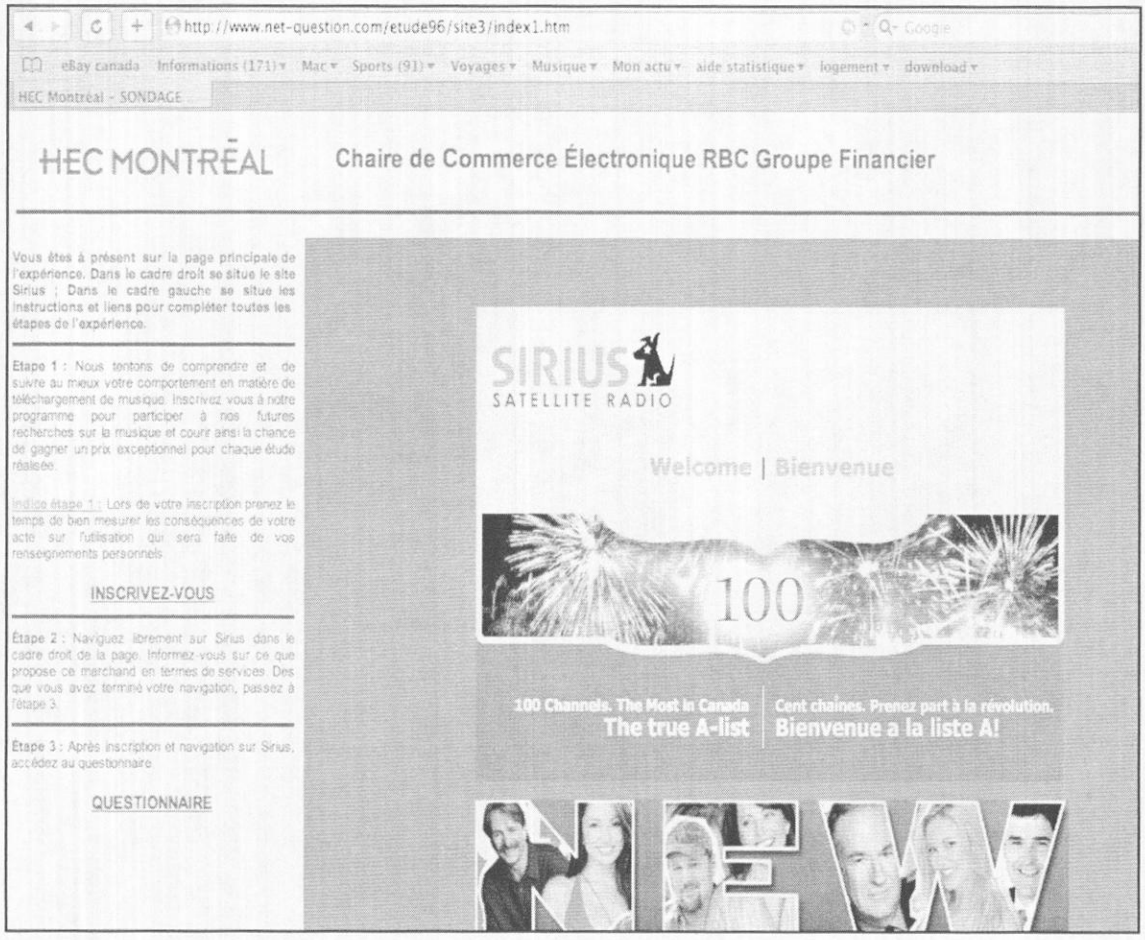
Il nous semble logique de penser que l'internaute qui se promène sur un site réel a plus de chance de s'impliquer dans l'expérience qu'un internaute visitant un site fictif dont l'existence dans le monde « World Wide Web » est nulle. Lorsque nous parlons d'implication, nous acceptons l'idée de l'importance du cognitif dans la prise de décision du consommateur. Nous admettons que cet état d'implication possède des

valeurs motivationnelles qui entraînent et influencent des processus cognitifs comme l'attention, les processus de compréhension et de décision (Celsi et Olson, 1989). Lors du processus décisionnel, les consommateurs recherchent et utilisent l'information dans le but de résoudre un problème de façon rationnelle (Foxall et Goldsmith, 1994). En effet, un consommateur plus impliqué est plus à même de traiter l'information subséquente qu'un consommateur moins impliqué (Celsi et Olson, 1989). L'attitude d'un consommateur impliqué tend donc vers des processus mentaux plus profonds et complexes dans ce qui touche au processus décisionnel du consommateur (Gardner, Mitchell et Russo, 1978, Bettman, 1982, voir Nantel et Robillard, 1990).

Par conséquent, le site Internet marchand choisi se nomme SIRIUS, disponible depuis peu sur SIRIUSCANADA.CA. Société américaine, Sirius propose un service payant de bouquet radio satellite inédit, ainsi qu'une multitude de lecteurs radios satellites. Le choix de sélectionner le site de ce marchand comme objet de notre expérience s'explique par le caractère innovant des services musicaux et des produits offerts. Son originalité pouvait susciter chez le consommateur un intérêt tel, que la probabilité de son implication sur le plan cognitif et affectif était renforcée (Solomon et al., 2005). Il faut savoir que la radio satellite, ainsi que ses lecteurs radios spécifiques n'étaient, encore très récemment, disponibles qu'aux Etats-Unis.

Le site Internet original de SIRIUSCANADA.CA était présenté à l'intérieur des sites Internet expérimentaux sur la troisième page. Lors de la navigation de SIRIUS, l'internaute pouvait facilement accéder aux informations relatives aux services et produits proposés. Il pouvait se renseigner sur la programmation offerte, sur les lecteurs radios satellites ou bien encore activer sa ligne.

Figure 13 : Troisième page informant des taches et contenant le site SIRIUS



Cette troisième page indiquait dans le cadre gauche les trois étapes à effectuer par les consommateurs lors de l'expérience. Le lien hypertexte « Inscrivez-vous » renvoyait vers une page d'inscription au programme de recherche fictif sur les habitudes d'écoute et d'acquisition de la musique en ligne où chaque individu devait, par la même occasion, répondre à une première courte étude portant sur la musique. Cette page d'inscription était au centre de l'expérience puisqu'elle contenait les politiques fictives relatives à la protection des renseignements personnels. Finalement, un lien hypertexte en bas de page permettait à l'internaute de se rendre facilement au questionnaire final de la recherche.

3.1.2.3 L'inscription au centre de l'expérience.

Comme nous l'avons vu précédemment, chacun des sites expérimentaux contenait un cadre SIRIUS, entouré par un cadre de la Chaire de Commerce Electronique RBC Groupe Financier comportant toutes les informations relatives à l'expérience. Ce dernier cadre comprenait en milieu de page un lien hypertexte menant à une inscription (cf. « INSCRIVEZ VOUS », figure 13).

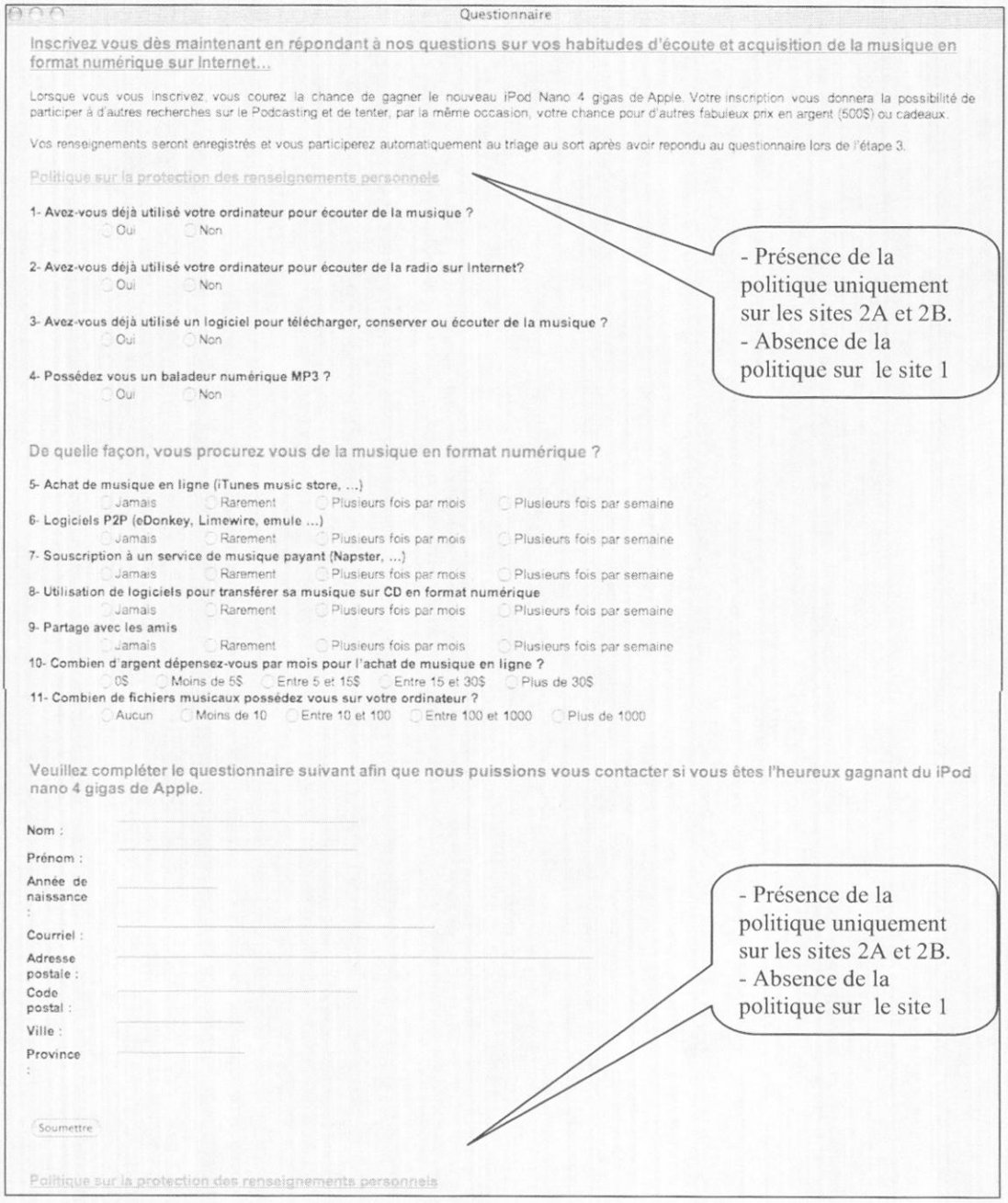
L'intitulé qui incitait les consommateurs à s'inscrire se présentait sous la forme suivante : *« Nous tentons de comprendre et de suivre au mieux votre comportement en matière de téléchargement de musique. Inscrivez vous à notre programme pour participer à nos futures recherches sur la musique et courir ainsi la chance de gagner un prix exceptionnel pour chaque étude réalisée..»*

Après que l'internaute ait cliqué sur le lien « INSCRIVEZ VOUS», une fenêtre pop up s'ouvrait (Figure 14) et présentait :

- Un texte d'introduction à l'inscription
- Des questions sur les habitudes en matière de musique
- Une demande de renseignements personnels tel que : Nom ; Prénom ; Année de naissance ; Adresse de courriel ; Adresse postale ; Code postal ; Ville ; Province.
- Deux liens hypertexte dirigeant vers la même politique relative à la protection des renseignements personnels.

Lorsque le consommateur avait complété son inscription, il devait cliquer sur « soumettre ». Il recevait alors un mot de remerciement l'invitant à continuer l'expérience en naviguant sur le site de SIRIUS (cadre navigable sur la troisième page des sites expérimentaux (figure 13)). En d'autres termes, nous incitions les consommateurs à passer à la seconde étape de l'expérience.

Figure 14 : Page d'inscription



Finalement, dans le but de mesurer l'audience de la politique relative à la protection des renseignements personnels, nous avons utilisé la méthode des logs, et ce afin de récolter les données de navigation. Cette méthode nous a renseigné sur le comportement de navigation des consommateurs et nous a permis de comparer les résultats obtenus aux réponses apportées dans le questionnaire. Parallèlement, cette

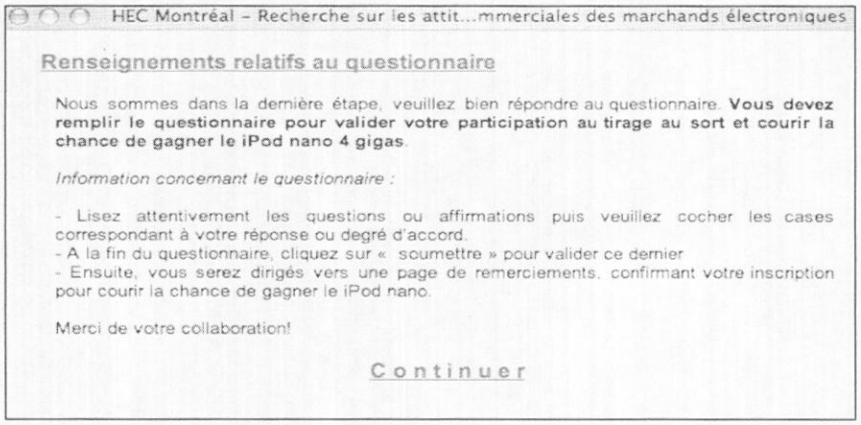
méthode a permis de connaître le comportement susceptible de résulter de la lecture de la politique relative à la protection des renseignements personnels.

3.1.2.4 Renseignements relatifs au questionnaire post navigation

Lorsque les individus avaient fini de naviguer sur SIRIUS, l'étape post navigation débutait (en cliquant sur « QUESTIONNAIRE » - cf. figure 13-) par une introduction au questionnaire (figure 15). La page html présentée a été mise en place afin d'informer le consommateur quant au déroulement du questionnaire.

Concernant le questionnaire lui-même, il était composé de 41 questions divisées en 10 parties. Pour rappel, le questionnaire a été construit à partir d'échelles de mesures originales et traduites de l'anglais en français. Le questionnaire en ligne uniquement en version française était identique pour chacun des individus sondés.

Figure 15 : Introduction au questionnaire d'évaluation



À la fin du questionnaire, et après avoir validé ce dernier, le consommateur recevait un mot de remerciement de la Chaire de Commerce Electronique RBC Groupe Financier pour le temps qu'il avait bien voulu accorder à la recherche.

3.1.3 Récapitulatifs des étapes de l'expérience

Dans un souci de précision, nous avons souhaité récapituler les principales étapes de l'expérience :

1 : Envoi du courriel à 840 personnes incitant ces dernières à participer à l'expérience.

2 : Les consommateurs intéressés, après avoir cliqué sur le lien hypertexte, se retrouvaient sur la page d'accueil du site de l'expérience. Ils étaient alors dirigés vers un des trois sites expérimentaux assignés de façon aléatoire. Ces consommateurs avaient donc autant de probabilité de naviguer sur le site 1, que sur les sites 2A ou 2B.

3 : Les consommateurs consentant à participer à l'étude suivaient les 3 étapes de l'expérience :

- S'inscrire à un programme de recherche sur les habitudes d'écoute et d'acquisition de la musique en ligne mené par la Chaire de Commerce Électronique RBC Groupe Financier en répondant à une première courte étude.
- Naviguer sur le site SIRIUSCANADA.CA.
- Répondre au questionnaire de la recherche évaluant le site SIRIUS.

4 : Après avoir validé les réponses du questionnaire, l'individu sondé recevait un mot de remerciement.

3.2 Tests préliminaires

Lors de cette recherche, deux tests préliminaires furent réalisés :

- Le premier intervenait par l'intermédiaire d'entrevues personnelles par méthode protocolaire.

- Le second pré test était l'expérience elle-même, mais avec un échantillon moindre que l'échantillon final.

Les pré tests réalisés permettaient de s'assurer de la bonne compréhension des sites expérimentaux et des échelles de mesures. On s'assurait, par la même occasion, de la fidélité de nos mesures et de la validité des manipulations.

3.2.1 Pré test 1

Le pré test 1 permettait de s'assurer de la bonne compréhension du site Internet et des items utilisés dans le questionnaire. Comme le confirment Hunt et al. (1982): « *Pretesting, the final stage, is the use of a questionnaire in a small pilot study to ascertain how well the questionnaire works. Pretesting an instrument is necessary because, as Backstrom and Hursch (1963) have pointed out, « no amount of intellectual exercise can substitute for testing an instrument designed to communicate with ordinary people* » »[7]

La méthode d'entrevue personnelle par analyse de protocole était utilisée. Cette méthode nous permettait de se rendre compte directement des hésitations, réactions et commentaires du répondant.

Lorsque l'individu lisait le scénario, qu'il naviguait sur le site, qu'il accomplissait la tâche puis qu'il répondait au questionnaire, il lui était demandé de penser tout haut. Cette méthode permettait donc d'optimiser de façon conséquente :

- La tâche à accomplir
- Le site Internet expérimental
- Le questionnaire

À noter que les 3 sites étaient à l'étude lors de ce pré test.

6 étudiants de la M.Sc, 2 par site, ont permis de pointer les erreurs connexes à la navigation, d'optimiser l'étape de l'inscription au sondage en ne mettant que les items compréhensibles par le grand public. Ce pré test a permis de produire un

[7] Le pré-test, étape finale, est l'utilisation d'un questionnaire dans une petite étude pilote pour s'assurer du bon fonctionnement de ce dernier. Le pré test est un instrument nécessaire parce que, comme l' ont fait remarquer Backstrom et Hursh (1963), « Aucun exercice intellectuel ne peut remplacer un instrument dessiné à communiquer avec des gens ordinaires » »

questionnaire (cf : étape 3) plus parcimonieux et compréhensible ; certaines questions ont été reformulées, d'autres supprimées.

3.2.2 Pré-test 2

Le pré test 2 nous a permis de contrôler la fiabilité de nos échelles de mesure ; en d'autres termes, nous en avons vérifié la stabilité et la consistance. Nous nous sommes donc assurés de la bonne compréhension de nos échelles de mesures, de leur validité interne et externe par l'intermédiaire des alpha de Cronbach et de l'analyse factorielle. De plus, ce pré test nous a également permis de tester le fait que selon que les consommateurs soient exposés au site 1, 2A, ou 2B, l'expérience sur ces derniers créait une variation dans le degré de perception du contrôle. Finalement, grâce aux questions de vérifications, nous avons pu nous assurer que les manipulations réalisées fonctionnaient efficacement.

Le pré-test a été effectué entre le 7 février 2006 et le 6 mars 2006. Dans un premier temps, nous avons diffusé les sites expérimentaux via courriel, via annonces journal, annonces babillard. Dans un second temps, l'url des sites expérimentaux a été envoyé à 250 personnes du panel de la chaire de commerce électronique RBC Groupe Financier. Au total, 104 répondants ont accepté de participer.

Tout d'abord les échelles de mesure sélectionnées dans le cadre de cette recherche apparaissent stables et consistantes (tableau 5). Nous avons trouvé les alpha de Cronbach grâce à l'analyse de fiabilité et les facteurs grâce à l'analyse en composante principale.

Tableau 5: Fiabilité des échelles de mesure

Variables	Items	Fiabilité α pour pré test 2
Contrôle comportemental perçu	3	**.84 (1 facteur)**
Confiance envers le cybermarchand	2	**.87 (1 facteur)**
Attitude comportementale	5	**.90 (1 facteur)**
Intention comportementale	4	**.94 (1 facteur)**
Confiance de disposition	6	**.80 (2 facteurs à .71 pour 3 items et .76 pour 3 autres items)**
Confiance institutionnelle	9	**.94 (1 facteur)**

Le fait de trouver 2 facteurs pour la confiance de disposition est tout a fait logique puisque lors de la construction de l'échelle à 6 items, 3 items sont pris pour mesurer la propension à faire confiance, 3 autres pour mesurer la foi en l'intégrité des hommes. En conclusion, les échelles de mesure ne demandent aucune modification supplémentaire.

Deuxièmement, il semble qu'une variance soit obtenue dans le sentiment de contrôle perçu sur les renseignements personnels dépendamment de la politique lue (tableau 6). En effet, les personnes ayant lu la politique du second site expérimental (site 2A) comportant une politique statique en opt-out sur la protection des renseignements personnels se sentaient moins en contrôle que les personnes ayant lu la politique du troisième site expérimental (site 2B) comportant une politique dynamique en opt-in (p=.008).

Tableau 6 : Comparaison des moyennes pour le sentiment de contrôle perçu sur les renseignements personnels

	Site visité	N	Moyenne	t	P
Sujets ayant lu la politique	Site avec politique en opt-out (site 2A)	20	2,7833	-1,7038	**,008**
	Site avec politique en opt-in (site 2B)	13	4,4872		

Troisièmement enfin, l'analyse des moyennes des questions de vérification nous a permis de vérifier les manipulations. Nous avons lancé 3 analyses :

- Comparaison des moyennes des personnes ayant visité le site sans politique (site1) versus un site avec politique (site 2A + 2B). On ne considérait que QVE1 dans ce cas, les autres items n'étaient pas concernés (tableau 7).
- Comparaison des moyennes des personnes ayant lu la politique en opt-out (site2A) versus des personnes ayant lu la politique en opt-in (site 2B). On ne considérait pas QVE1 dans ce cas, cela n'étant pas pertinent. Les autres items étaient tous concernés (tableau 8).
- Comparaison des moyennes des personnes ayant lu la politique (site 2A et site 2B) versus des personnes n'ayant pas lu la politique (tous sites). On ne considérait pas QVE1 dans ce cas, cela n'étant pas pertinent. Les autres items étaient tous concernés (tableau 9).

Dans le cadre de ces 3 analyses, nous avons dû recoder QVE3, QVE4, QVE5 car les items étaient inversés (recodification de QVE4 pour les visiteurs du site 2B, recodifications de QVE3 et QVE5 pour les visiteurs du site 2A). La recodification s'est faite par rapport aux bonnes réponses, 7 étant une réponse valide et 1 une réponse incorrecte.

Pour rappel, voici les 5 questions de vérifications (échelle de Likert à 7 point « pas du tout d'accord » à « entièrement d'accord » et un huitième point pour « je ne sais pas »):

QVE1 - La page d'inscription (que vous avez remplie lors de l'étape 1) possède un lien hypertexte dirigeant vers la politique sur la protection des renseignements personnels :

QVE2 - Lors de mon inscription (cf. étape 1), on m'assure qu'une technologie d'encryptage très puissante protège mes renseignements personnels:

QVE3 - Lors de mon inscription (cf. étape 1), on m'assure qu'il est possible d'accéder à tout moment à l'information divulguée afin de la vérifier, la modifier ou la supprimer:

QVE4 - Lors de mon inscription (cf. étape 1), on m'inclut automatiquement aux listes de distribution:

QVE5 - Lors de mon inscription (cf. étape 1), on me donne la possibilité (en cochant des cases) d'être inclut dans les listes de distribution:

Tableau 7 : Comparaison des moyennes pour QVE 1 des personnes ayant visité le site 1 (sans politique) versus un site avec politique (site 2A +2B)

	Site visité	N	Moyenne	p
QVE 1	Site avec politique (site 2A et 2B)	62	6,60	**,000**
	Site sans politique (site 1)	23	3,61	

Les personnes ayant visité le site 1 n'ont pas répondu correctement, contrairement à celles ayant visité le site 2A et 2B (p= .000).

Tableau 8 : Comparaison des moyennes pour QVE2, QVE3, QVE4 et QVE5 des personnes ayant lu la politique du site 2A versus le site 2 B

	Site visité	N	Moyenne	p
QVE 2	Site avec politique en opt-out (site 2A)	19	6,05	**,271**
	Site avec politique en opt-out (site 2B)	11	5,00	
	Site visité	N	Moyenne	p
QVE 3 (en recodé)	Site avec politique en opt-out (site 2A)	14	6,64	**,435**
	Site avec politique en opt-out (site 2B)	8	6,00	
	Site visité	N	Moyenne	p
QVE 4 (en recodé)	Site avec politique en opt-out (site 2A)	20	5,95	**,321**
	Site avec politique en opt-out (site 2B)	11	6,55	
	Site visité	N	Moyenne	p
QVE 5 (en recodé)	Site avec politique en opt-out (site 2A)	20	6,55	**,491**
	Site avec politique en opt-out (site 2B)	9	6,00	

Les résultats s'avèrent probants puisque les internautes ayant lu les politiques sur la protection des renseignements personnels ont répondu correctement sans aucune différence quelque soit le site visité (site 2A et 2B uniquement)..... Le test fut non significatif pour QVE2 (p=.271), QVE3 (p=.435), QVE4 (p=.321), QVE5 (p=.491).

Tableau 9 : Comparaison des moyennes pour QVE2, QVE3, QVE4 et QVE5 des personnes ayant lu la politique des site 2A ou 2B versus les personnes n'ayant pas lu de politique (site 1)

	Site visité	N	Moyenne	p
QVE 2	Site avec politique en opt-out (site 2A)	30	5,67	**,000**
	Site avec politique en opt-out (site 2B)	50	3,06	
	Site visité	N	Moyenne	p
QVE 3 (en recodé)	Site avec politique en opt-out (site 2A)	22	6,41	**,000**
	Site avec politique en opt-out (site 2B)	49	3,00	
	Site visité	N	Moyenne	p
QVE 4 (en recodé)	Site avec politique en opt-out (site 2A)	31	6,16	**,000**
	Site avec politique en opt-out (site 2B)	54	3,28	
	Site visité	N	Moyenne	p
QVE 5 (en recodé)	Site avec politique en opt-out (site 2A)	29	6,38	**,000**
	Site avec politique en opt-out (site 2B)	52	3,71	

Les résultats sont là encore probants puisque les internautes ayant lu les politiques sur la protection des renseignements personnels ont répondu correctement contrairement aux personnes n'ayant pas lu les politiques. Le test est significatif pour QVE2 (p=.000), QVE3 (p=.000), QVE4 (p=.000), QVE5 (p=.000).

En conclusion des 3 analyses, les individus ont compris convenablement les politiques sur la protection des renseignements personnels. Les échelles de mesures sont fiables et valides. Finalement, une variance dans le contrôle apparaît dépendamment de la politique sur la protection des renseignements personnels qui a

été lue. En somme, aucune modification n'a donc été apportée lors de la collecte de donnée finale aux sites expérimentaux 1, 2A et 2B.

3.3 Échantillonnage et collecte de données

3.3.1 Environnement lors de la collecte de données finale

L'environnement de l'expérience était non contrôlé. L'internaute pouvait, de n'importe quel endroit et à n'importe quel moment, se connecter au site expérimental qui lui était assigné de façon probabiliste. Cependant, il ne pouvait y accéder qu'une seule fois. La seule condition pour pouvoir naviguer sur le site et répondre au questionnaire était de posséder un ordinateur connecté sur l'Internet.

3.3.2 Population à l'étude pour la collecte de données finale

Dans le cadre de cette recherche, il a été décidé de ne pas contrôler les variables socio démographiques susceptibles d'impacter sur le comportement du consommateur et sur les variables de la confiance.

De plus, n'ayant fait aucune modification sur les sites expérimentaux entre la seconde phase de pré test et le test final, il a été logiquement décidé d'agréger les données du pré test 2 et de la collecte de donnée finale. De fait, nous avons récolté 209 questionnaires analysables. 65 pour le site 1, 76 pour le site 2A, 68 pour le site 2B.

Chapitre 4 : Résultats

Ce chapitre présente les résultats obtenus grâce à la collecte de données réalisée. Rappelons que 209 individus au total ont participé au sondage. Parmi les sondés, 65 internautes (soit 31,1%) ont visité le site 1 qui ne contenait aucune politique, 76 autres (soit 36,4%) se sont rendu sur le site 2A contenant une politique statique sur la protection des renseignements personnels en opt-out, enfin les 68 derniers (soit 32,5%) sont allés sur le site 2B dont la politique était dynamique en opt-in.

Sur un total de 144 personnes ayant eu accès à un lien dirigeant vers une politique contenant des renseignements liés à la sécurité et à la vie privée, 58 (soit 40,28%) se sont attardés sur le contenu de celle-ci. Ce fort pourcentage s'explique sans doute par le fait d'avoir conseillé aux individus sondés de bien mesurer les conséquences sur l'utilisation qui allait être faite de leurs renseignements personnels lors de leur inscription sur le site 1, 2A ou 2B (voir figure 12). La seconde raison susceptible de justifier ce nombre important de clics sur les politiques s'explique aussi par le scénario proposé. Pour rappel les Internautes devaient s'inscrire à un programme de recherche sur les habitudes d'écoute et d'acquisition de la musique en ligne. Ce programme de recherche, outre les enquêtes et évaluations de sites musicaux, informait l'individu, qu'en s'inscrivant, il consentait de fait à être monitoré sur une période d'un an lors de ses prochaines navigations en expérience.

Par ailleurs, parmi les gens ayant visité les politiques, une minorité ont précisé la façon dont ils souhaitaient que leurs renseignements personnels soient traités. C'est le cas des internautes ayant consulté la politique statique en opt-out sur la protection des renseignements personnels (site 2B) pour laquelle seulement 6 internautes sur 34 (soit 17,65%) ont envoyé un courriel les désengageant des infolettres proposées et des offres des partenaires. Autrement dit, 28 internautes sur 34 (soit 82,35%) ayant cliqué sur le lien de la politique puis assuré en avoir pris connaissance, ont consenti à recevoir des infolettres et des promotions de partenaires. À l'inverse, la politique dynamique en opt-in du site 2B n'a enregistré l'accord que d'une seule personne sur 24 pour les infolettres et de deux personnes pour les promotions des partenaires. De

plus, il est intéressant de constater que 41,66% des 24 personnes concernées par la politique dynamique en opt-in ont spécifié vouloir naviguer de façon totalement anonyme contre aucune lorsque la politique était statique en opt-out. De fait, il apparaît clairement que l'option du statique en opt-out dans un but de promotion s'avère plus intéressante que le format dynamique en opt-in puisque l'opt-out retient le consentement des internautes à la promotion, à hauteur de 82,35% dans notre expérience au lieu de 4,16% à 8,33% dans le cas de l'opt-in. Ce fait précis rappelle les travaux de Arcand et Nantel (2005) qui ont comparé les politiques sur la vie privée à des « armes à double tranchant ». Les auteurs ont démontré que la lecture d'une politique impacte négativement sur le contrôle, la confiance et l'intention comportementale mais est positivement reliée à la divulgation des renseignements personnels.

Retenons également que sur un total de 209 personnes, 151 (soit 72,2%) n'ont pas consulté le contenu des politiques sur la protection des renseignements personnels, bien qu'elles aient divulgué : noms, prénoms, courriels et adresses postales. Enfin, l'autre chiffre intéressant, et troublant, est le nombre très important d'internautes n'ayant jamais pris connaissance des politiques et, lors des questions de vérification, assurant l'avoir fait; c'est ainsi que 76 personnes sur 151 (soit 50,33%) au final, n'ont pas répondu correctement.

En ce qui concerne notre population à l'étude, l'âge moyen des répondants est de 30 ans avec une grande majorité se situant dans la fourchette 19-26 ans (60,6%). La majorité des sondés sont des hommes (57,6%), les femmes représentant 42,4%. Pour rappel, la totalité des individus sondés sont des habitants du Québec. Les répondants sont majoritairement des célibataires (79,5%) dont le dernier niveau de scolarité gradué est le 1er cycle en université (53,4%); 44% d'entre eux sont étudiants à temps plein tandis que la proportion des travailleurs à temps plein s'élève à 28%. Enfin, la dernière donnée sociodémographique concerne le revenu; ils sont ainsi 51,5 % à percevoir un salaire en dessous de 15000 $, 14% un salaire entre 15000 $ et 25000 $, 24% un salaire entre 25000 $ et 50000 $, et seulement 10,5% à toucher un revenu au-dessus de 50000 $.

De fait, si nous devions faire un portrait type de cet échantillon, nous pourrions alors définir celui d'un jeune homme habitant dans la zone urbaine de Montréal, gagnant un salaire de niveau moyen et titulaire d'un diplôme universitaire significatif d'un certain degré de culture. Il est très intéressant de constater enfin que le profil de notre répondant moyen est proche de l'internaute moyen au Québec, à savoir : âge se situant entre 18 et 24 ans, résidant dans un centre urbain (Montréal ou Québec), ayant complété des études postsecondaires mais dont les revenus excèdent 60 000 $ (NETendances, Cefrio, 2001, voir Communautique, 2002).

4.1 Validité et fidélité de la recherche

Dans un premier temps, afin de tester la fiabilité des échelles de mesure sur notre échantillon total de 209 individus, nous utilisons les alpha de Cronbach. Voici présenté ci-dessous le résultat de chaque alpha par variables étudiée :

Tableau 10: Fiabilité des échelles de mesure

Variables	Items	Fiabilité α pour test final
Contrôle comportemental perçu	3	.89
Confiance envers le cybermarchand	2	.84
Attitude comportementale	5	.92
Intention comportementale	4	.94
Confiance de disposition	6	.84
Confiance institutionnelle	9	.94

L'analyse des alpha de Cronbach démontre clairement une cohérence interne puisque les 6 variables à l'étude possèdent des alpha supérieurs à .80.

Finalement, en ce qui concerne la validité des échelles de mesure, une analyse factorielle en composante principale (par rotation varimax) est conduite afin de s'assurer que chaque item lors du test final a bien mesuré les mêmes dimensions.

Tableau 11: Validité des échelles de mesure

Variables	Items	Analyse factorielle
Contrôle comportemental perçu	3	**1 composant expliquant à 81,819% la variabilité totale**
Confiance envers le cybermarchand	2	**1 composant expliquant à 86,894% la variabilité totale**
Attitude comportementale	5	**1 composant expliquant à 76,593% la variabilité totale**
Intention comportementale	4	**1 composant expliquant à 85,557% la variabilité totale**
Confiance de disposition	6	**1 composant expliquant à 56,199% la variabilité totale**
Confiance institutionnelle	9	**1 composant expliquant à 72,513% la variabilité totale**

Nous constatons une validité satisfaisante des échelles de mesure.

4.2 Effets des politiques sur la protection des renseignements personnels sur le sentiment de contrôle comportemental

Cette section vise à analyser les résultats liés à l'impact qu'ont eu, dans notre expérience, les politiques sur la protection des renseignements personnels sur le contrôle perçu. Nous comparons donc, de façon exploratoire, chacun des groupes d'individus dépendamment de la présence ou absence de la politique, de sa lecture ou non, et de son format (dynamique en opt-in versus statique en opt-out). Cette partie traite aussi en simultanée H1A et H1B.

Tout d'abord, cette partie exploratoire prend en compte 4 groupes indépendants :

- Le groupe « Contrôle » constitué d'individus n'ayant jamais eu accès à la politique sur la protection des renseignements personnels.
- Le groupe « Pas lu » constitué d'individus ayant eu accès à la politique sur la protection des renseignements personnels mais n'ayant pas cliqué dessus.

- Le groupe « Lu statique opt-out » constitué d'individus ayant cliqué sur le lien dirigeant à la politique statique en opt-out sur la protection des renseignements personnels.
- Le groupe « Lu dynamique opt-in » constitué d'individus ayant cliqué sur le lien dirigeant à la politique dynamique en opt-in sur la protection des renseignements personnels.

Voici résumé ci-dessous un tableau descriptif des différents groupes :

Tableau 12: Tableau descriptif des groupes en rapport avec l'effet des politiques sur la protection des renseignements personnels

Groupe	n	Moyenne du contrôle perçu
Contrôle	65	3,5410
Pas lu	86	4,1142
Lu statique opt-out	34	3,0625
Lu dynamique opt-in	24	4,8842
Lu (total)*	58	3,8163

* Fusion des groupes « Lu statique opt-out » et « Lu dynamique opt-in »

Comparaison des moyennes du sentiment de contrôle entre les individus n'ayant pas lu la politique qui se présentait et ceux l'ayant lu :

Le premier test réalisé afin d'explorer en profondeur les conséquences des caractéristiques des sites des cybermarchands sur la collecte de donnée ainsi que sur la dimension du traitement des renseignements personnels est de comparer le contrôle perçu des internautes n'ayant pas lu la politique versus ceux l'ayant lu. Par conséquent, un test t est conduit et confronte le groupe « pas lu » aux personnes ayant lu la politique, c'est-à-dire les groupes « Lu dynamique opt-out » et « Lu dynamique opt-in ». Il est important de noter que cette analyse cache la nature du contenu des politiques et donc des caractéristiques du site du cybermarchand sur la collecte de données.

Voici les résultats du test t :

Tableau 13: Test t sur le sentiment de contrôle comportemental par lecture ou non de la politique sur la protection des renseignements personnels

	Groupe	N	Moyenne	t	p
Sentiment de contrôle	Pas lu	86	4,1142	.984	.328
	lu	58	3,8163		

Les résultats démontrent qu'il n'existe pas de différence significative dans la perception du contrôle entre les internautes ayant cliqué sur la politique et ceux l'ayant ignoré (t=.984 ; p=.328). Ce résultat est non significatif car il cache sans doute la vrai nature de ce qui est lu dans les politiques d'où l'importance de l'analyse qui suit.

Comparaison des moyennes du sentiment de contrôle entre les différents groupes d'individus ayant eu accès à une politique :

Dans le souci de rentrer plus en détail, nous opérons un premier test F afin de constater s'il existe des différences dans le contrôle perçu à travers nos différents groupes d'individus lorsque la politique est présente. Les groupes concernés par le test F sont :

- Le groupe « Pas lu » (n=86)
- Le groupe « Lu statique opt-out » (n=34)
- Le groupe « Lu dynamique opt-in » (n=24)

Voici les résultats du test F :

Tableau 14: Test F sur l'effet des politiques sur le sentiment de contrôle comportemental lorsque la politique est présente

	Groupe	N	Moyenne	f	p
Sentiment de contrôle	Pas lu	86	4,1142	9.669	**.000**
	Lu statique opt-out	34	3,0625		
	Lu dynamique opt-in	24	4,8842		

Il existe donc au moins une différence significative entre deux groupes (F=9.669; p=.000) lorsque nous réalisons le test F sans prendre en compte le groupe « contrôle ». Afin de faire une analyse plus fine des résultats, on effectue toutes les comparaisons deux à deux. Voici les résultats :

Tableau 15: Comparaisons des moyennes 2 à 2 de l'effet des politiques sur le sentiment de contrôle comportemental lorsque la politique est présente

		Différence des moyennes (I-J)	**Erreur standard**	**p**
Groupe (i)	Groupe (j)			
Lu statique opt-out	Lu dynamique opt-in	-1,822	,428	**,000**
	Pas lu	-1,052	,325	**,002**
Lu dynamique opt-in	Lu statique opt-out	1,822	,428	,000
	Pas lu	,770	,370	**,039**

Premièrement, nous constatons qu'il existe une différence significative dans le contrôle perçu entre les personnes ayant lu la politique statique en opt-out et ceux l'ayant lu en dynamique opt-in (p=.000). D'après les moyennes (cf. Tableau 12), les personnes ayant lu la politique dynamique en opt-in (moyenne = 4,8842) se sentent significativement plus en contrôle sur leurs renseignements personnels que les individus ayant parcouru une politique statique fondée sur le désengagement (moyenne = 3,0625). En d'autres termes ce résultat confirme H1B.

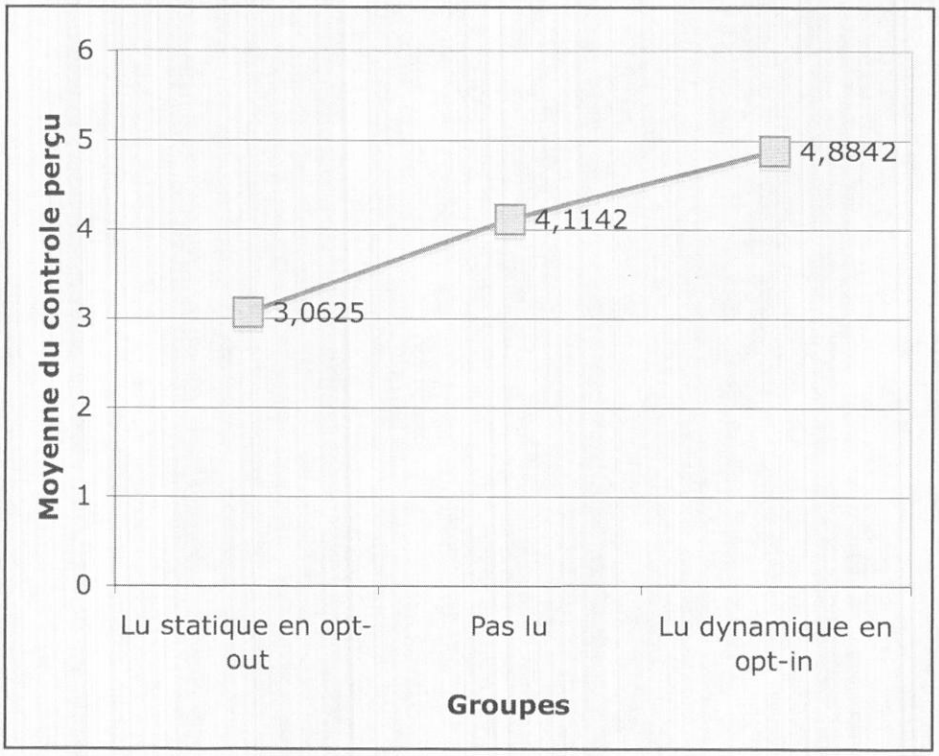
Deuxièmement, il existe aussi une différence significative entre les personnes n'ayant pas lu la politique lorsque celle-ci est présente et les personnes s'étant rendu sur la politique statique en opt-out (p=.002). Par conséquent, nous en concluons que les internautes ne s'étant pas renseignés sur la politique sur les renseignements personnels pourtant présente (moyenne = 4,1142) se sentent plus en contrôle sur leurs renseignements personnels que les personnes ayant lu la politique statique en opt-out (moyenne = 3,0625).

Troisièmement, nous remarquons une dernière différence significative entre les gens ayant lu la politique dynamique en opt-in et les autres n'ayant pas cliqué sur le lien de la politique qui se présentait à eux (p=.039). Autrement dit, les individus ayant cliqué

sur une politique dynamique fondée sur le consentement préalable (moyenne = 4,8842) se sentent significativement plus en contrôle sur leurs renseignements personnels que les personnes ayant lu la politique statique fondée sur le consentement implicite (moyenne = 3,0625).

Voici présenté ci-dessous un graphique résumant les résultats décrits auparavant :

Figure 16: Comparaisons des moyennes de l'effet des politiques sur le sentiment de contrôle comportemental lorsque la politique est présente



Comparaison des moyennes du sentiment de contrôle entre les individus ayant eu accès à une politique et le groupe n'ayant pas eu accès à une politique quelconque:

Dans la continuation de notre exploration des données, nous réalisons un second test F en prenant cette fois-ci les quatre groupes afin de comparer les trois groupes étudiés précédemment dans le premier test F à notre groupe « contrôle »
Les 4 groupes concernés par le test F sont donc :

- Le groupe « Contrôle » (n=65)
- Le groupe « Pas lu » (n=86)
- Le groupe « Lu statique opt-out » (n=34)
- Le groupe « Lu dynamique opt-in » (n=24)

Tableau 16: Test F sur l'effet des politiques sur le sentiment de contrôle comportemental

	Groupe	**N**	**Moyenne**	**F**	**p**
Sentiment de contrôle	Contrôle	65	3,5410	7.131	**.000**
	Pas lu	86	4,1142		
	Lu statique opt-out	34	3,0625		
	Lu dynamique opt-in	24	4,8842		

Lorsque le test F est réalisé sur les 4 groupes incluant donc le groupe « contrôle » qui ne pouvait cliquer sur la politique absente, le test s'avère significatif (F=7.131; p=.000). Afin de rendre l'analyse des résultats plus fine, nous utilisons la méthode de Dunnett pour comparer tous les groupes au groupe contrôle. Voici les résultats :

Tableau 17: Comparaisons des moyennes par rapport au groupe « contrôle » de l'effet des politiques sur le sentiment de contrôle comportemental

		Différence des moyennes (I-J)	**Erreur standard**	**p**
(I) Groupe	(J) Groupe			
Lu statique opt-out	Contrôle	-,4784	,35137	,992
Lu dynamique opt-in	Contrôle	1,3432	,39653	**,001**
Pas lu	Contrôle	,5732	,27285	**,050**

Tout d'abord, il n'existe aucune différence significative entre les personnes ayant lu la politique statique en opt-out et ceux n'ayant jamais eu accès à une quelconque politique (p=.992). Néanmoins, nous constatons que cette différence est présente (p=.001) lorsque nous comparons le groupe « contrôle » (Moyenne = 3,5410) avec ceux ayant lu la politique dynamique en opt-in (Moyenne = 4,8842). En d'autres termes, les personnes ayant lu une politique dynamique fondée sur le consentement préalable se sentent largement plus en contrôle sur leurs renseignements personnels que les individus n'ayant jamais eu accès à une politique.

Finalement, nous remarquons, et ceci de façon significative, que la seule présence d'une politique sur la protection des renseignements personnels a un impact sur le sentiment de contrôle comportemental (p=.050). La comparaison des moyennes démontre que le contrôle ressenti est plus grand chez les individus ayant visité les sites avec politique sans en lire le moindre contenu (moyenne = 4,1142) que les internautes ayant visité les sites sans aucune mention de la politique sur la protection des renseignements personnels (moyenne = 3,5410). Ce résultat permet par ailleurs de soutenir l'hypothèse H1A.

4.3 *Effets du sentiment de contrôle comportemental sur le sentiment de confiance alloué au cybermarchand*

Cette section traite de notre seconde hypothèse, soit H2

Dans le cadre de cette analyse, nous prendrons uniquement en compte les 58 personnes ayant lu les politiques sur la protection des renseignements personnels. Voici présentée ci-dessous l'analyse corrélationnelle:

Tableau 18 : Matrice de corrélation entre les variables du contrôle perçu sur le renseignements personnels et la confiance interpersonnelle

		Contrôle comportemental
Confiance interpersonnelle	r	,365**
	p	,000
	N	58

** La corrélation est significative à un niveau de 0.01

De fait, nous pouvons en conclure qu'il existe une corrélation positive entre les variables du sentiment de contrôle sur les renseignements personnels et la confiance allouée à un cybermarchand lorsque nous prenons uniquement en compte les deux groupes ayant visité la politique sur la protection des renseignements personnels (dynamique en opt-in et statique en opt-out). Nous pouvons donc confirmer H2.

Ainsi, plus un individu est renseigné sur la politique de protection des renseignements personnels plus il se sent en contrôle sur ses renseignements personnels, et plus il se sent en confiance vis-à-vis du cybermarchand qui collecte ses données (r=.365 ; p=.000). Dans le cas où nous aurions pris l'échantillon total, H2 aurait aussi était validé (r=.275 ; p=.000).

4.4 Effets de la confiance allouée au cybermarchand sur le comportement ultérieur

Cette section traite de notre troisième hypothèse, soit H3A et H3B.

Dans le même esprit que le traitement de H2, une analyse de la corrélation est présentée. Les variables à l'étude sont la confiance envers le cybermarchand (confiance interpersonnelle) ainsi que l'attitude et l'intention comportementale à utiliser le cybermarchand.

Tableau 19 : Matrice de corrélation entre les variables « confiance interpersonnelle, attitude comportementale et intention comportementale »

		Attitude comportementale	Intention comportementale
Confiance interpersonnelle	r	,562**	,470**
	p	,000	,000
	N	209	209

** La corrélation est significative à un niveau de 0.01

Le sentiment de confiance interpersonnelle est corrélé positivement à l'attitude comportementale (r=.562 ; p=.000) et à l'intention comportementale (r=.470; p=.000). Les corrélations sont moyennement fortes. Les hypothèses H3A et H3B sont donc confirmées. Autrement dit, plus l'internaute se sent en confiance avec le cybermarchand et plus il aura une intention et une attitude positives envers l'utilisation du site.

4.5 Effets du sentiment de contrôle comportemental sur le comportement ultérieur

Cette section traite de nos quatrième et cinquième hypothèses, soit H4A, H4B, H5A et H5B.

Une nouvelle matrice de corrélation permet d'étudier la relation entre les différentes variables en jeu.

Tableau 20 : Matrice de corrélation entre les variables « confiance interpersonnelle, attitude comportementale et intention comportementale »

		Attitude comportementale	Intention comportementale
Contrôle comportemental	r	,130	,220**
	p	,061	,001
	N	209	209

** La corrélation est significative à un niveau de 0.01

Les valeurs des p-values nous amènent à conclure que le contrôle comportemental ne connaît une corrélation positive que lorsque la variable dépendante est l'intention comportementale (r=.220 ; p=.001) confirmant ainsi H4B. Dès lors, nous ne pouvons que réfuter H4A. Le contrôle comportemental sur les renseignements personnels n'a donc pas d'effet significatif sur l'attitude comportementale envers l'utilisation d'un site Internet marchand.

Précédemment, nous avons constaté la validation de H2 et H3B. Nous en concluons donc que les conditions sont remplies pour vérifier H5B. Le sentiment de confiance alloué au cybermarchand joue un rôle de médiation dans la relation qui unit le contrôle comportemental et l'intention comportementale. La nature de cette médiation est d'ailleurs totale, puisque lorsque nous incluons, grâce à une régression linéaire multiple, le sentiment de confiance alloué au cybermarchand, la relation entre le contrôle comportemental et l'intention comportementale devient non significative (r=.097 ; p=.127).

À l'inverse, H5A est réfutée, puisqu'il n'existe en aucun cas une relation significative lors du traitement de H4A. Le sentiment de confiance alloué au cybermarchand ne joue donc aucun rôle de médiation dans la relation qui unit le contrôle comportemental et l'attitude comportementale.

4.6 *Effets de modération sur le comportement ultérieur*

Cette section traite simultanément de nos sixième, septième et huitième hypothèses ; soit H6A, H6B, H7A, H7B, H8A et H8B

Nous testons ici, l'effet des trois variables du contrôle, de la confiance institutionnelle et de la confiance de disposition dans la relation qui unit la confiance envers le site Internet marchand et l'attitude envers l'utilisation de ce dernier.

De fait, nous testons simultanément H6A, H7A, H8A par l'intermédiaire d'une analyse de covariance (ANCOVA). Cependant, nous prenons en compte uniquement les effets d'interaction entre les co-variables et la confiance dans le site marchand, puisque nous cherchons seulement à tester les relations précédemment citées. L'analyse des effets de modérateurs est supportée par les travaux de Baron et Kenny (1986) qui démontrèrent qu'une « variable modératrice affecte la direction ou la force de la relation entre une variable indépendante ou prédicatrice et une variable dépendante ou critère. » (p.1174)

Dans le cadre de cette analyse, nous recodons les 3 co-variables et la variable « confiance dans le site marchand » en variables binaires (faible (si moyenne<3,5) vs forte (si moyenne>4,5)). Les valeurs comprises entre 3,51 et 4,49 ne sont pas prises en compte. Cette façon de faire nous permettra, par la suite, d'analyser plus facilement s'il y a présence d'une ou plusieurs interactions.[8]

En voici le tableau descriptif :

[8] Dans le cadre de l'Ancova, les analyses ont aussi été conduites sur les variables continues. Néanmoins les résultats ont été marginalement significatifs ou non significatifs.

Tableau 21 : Tableau descriptif des co-variables et de la variable confiance dans le site après recodification

	n	
	Niveau faible	**Niveau fort**
Variables		
Contrôle comportemental	35	43
Confiance institutionnelle	15	63
Confiance de disposition	12	66
Confiance envers le site Internet marchand	14	64

Le tableau ci-dessous présente les résultats de l'analyse.

Tableau 22 : Analyse de covariance du contrôle, de la confiance envers le commerce électronique et de la confiance de disposition sur l'attitude envers l'utilisation d'un site Internet marchand

Source de variation	Type III Somme des carrés	Degré de liberté	Carré moyen	F	P
Modèle corrigé	74,489	7	10,641	8,361	,000
Intercept	331,087	1	331,087	260,148	,000
Confiance dans le site	43,720	1	43,720	34,353	**,000**
Confiance dans le commerce électronique	,153	1	,153	,120	,730
Confiance de disposition	,491	1	,491	,386	,536
Contrôle comportemental	2,417	1	2,417	1,899	,173
Confiance dans le site * Confiance dans le commerce électronique	,954	1	,954	,749	,390
Confiance dans le site * Confiance de disposition	7,955	1	7,955	6,251	**,015**
Confiance dans le site * Contrôle comportemental	6,882	1	6,882	5,408	**,023**
Erreur	89,088	70	1,273		
Total	1936,644	78			
Total corrigé	163,578	77			

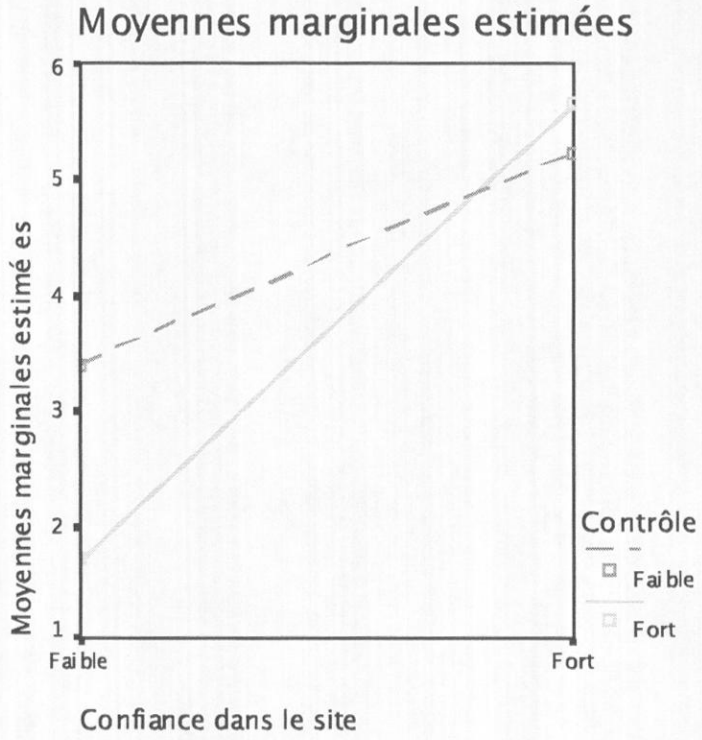
a R Squared = ,455 (Adjusted R Squared = ,401)

Le tableau de l'analyse de la co-variance fait mention d'effets significatifs. En effet, ajouté à l'impact significatif de la confiance dans le site sur l'attitude comme nous avions pu le constater auparavant dans nos analyses, il existe aussi une interaction entre le sentiment de confiance alloué à un cybermarchand et le contrôle perçu sur les

renseignements personnels. Autrement dit, il existe une modération du contrôle comportemental dans la relation qui unit la confiance à l'égard d'un cybermarchand et l'attitude envers l'utilisation du site de ce dernier. De plus, il existe une modération de la confiance de disposition entre la confiance dans le site Internet marchand et l'attitude. De fait, nous confirmons donc H6A et H8A et infirmons H7A.

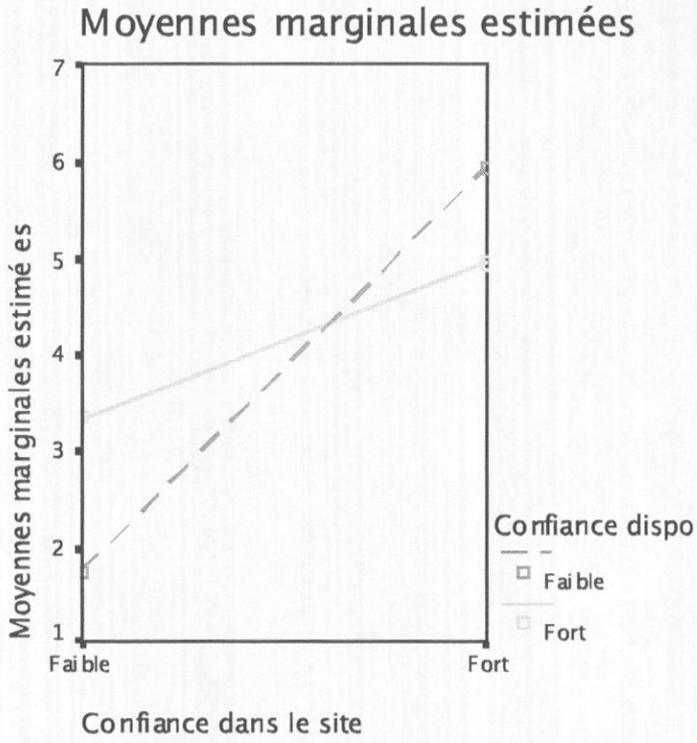
Regardons à l'aide de représentations graphiques les effets du contrôle comportemental (figure 16) et de la confiance de disposition (figure 17) dans la relation qui unit la confiance à l'égard d'un cybermarchand et l'attitude envers l'utilisation du site de ce dernier :

Figure 17: Représentation graphique de l'effet du contrôle comportementale en tant que co-variable dans la relation qui unit la confiance à l'égard d'un cybermarchand et l'attitude envers l'utilisation du site de ce dernier



Autrement dit, les effets du contrôle sur l'attitude envers l'utilisation du site marchand sont significativement meilleurs lorsque le sujet est fortement en confiance que lorsqu'il l'est faiblement (F=5,408).

Figure 18: Représentation graphique de l'effet de la confiance de disposition en tant que co-variable dans la relation qui unit la confiance à l'égard d'un cybermarchand et l'attitude envers l'utilisation du site de ce dernier



Autrement dit, les effets de la confiance de disposition sur l'attitude envers l'utilisation du site marchand sont significativement meilleurs lorsque le sujet est faiblement en confiance que lorsqu'il l'est fortement (F=6,251).

Par la suite, nous testons l'effet des trois mêmes variables étudiées dans l'analyse de co-variance ci-dessus lorsque la variable d'intérêt est définie par l'intention comportementale. Voici l'analyse de la co-variance présentée ci-dessous :

Tableau 23 : Analyse de covariance du contrôle, de la confiance envers le commerce électronique et de la confiance de disposition sur l'intention envers l'utilisation d'un site Internet marchand

Source de variation	Type III Somme des carrés	Degré de liberté	Carré moyen	F	P
Modèle corrigé	59,260	7	8,466	3,976	,001
Intercept	115,663	1	115,663	54,320	,000
Confiance dans le site	15,674	1	15,674	7,361	**,008**
Confiance dans le commerce électronique	1,952	1	1,952	,917	,342
Confiance de disposition	,115	1	,115	,054	,817
Contrôle comportemental	1	,158	,074	,786	1
Confiance dans le site * Confiance dans le commerce électronique	2,944	1	2,944	1,383	,244
Confiance dans le site * Confiance de disposition	1,574	1	1,574	,739	,393
Confiance dans le site * Contrôle comportemental	1,397	1	1,397	,656	,421
Erreur	149,051	70	2,129		
Total	981,070	78			
Total corrigé	208,312	77			

a R Squared = ,284 (Adjusted R Squared = ,213)

Nous observons une seule interaction. Elle concerne le sentiment de confiance alloué au site Internet marchand sur l'intention d'utiliser ce dernier. Aussi, l'ANCOVA démontre que ni le contrôle, ni la confiance de disposition, ni la confiance dans le commerce électronique modère la relation qui unit la confiance dans le site et l'intention d'utiliser ce dernier. Nous infirmons donc H6B, H7B et H8B

Conclusions

Nous allons synthétiser, dans ce chapitre, l'ensemble des résultats obtenus et expliquer en quoi notre recherche répond à la problématique et aux hypothèses émises. Il s'agit là d'une problématique fondée sur la compréhension de l'impact de la confiance et du contrôle en commerce électronique dans un contexte de marketing relationnel toujours plus perfectionné où sécurité et vie privée des internautes sont mis à rude épreuve.

Après un examen approfondi des résultats obtenus dans le chapitre précédent, nous discuterons des implications marketing que la présente étude a mises en évidence, et qui, nous l'espérons, seront d'un grand intérêt pour les gestionnaires et les chercheurs du domaine concerné. Par la suite, nous serons amenés à exposer les principales limites et avenues de la recherche pour les futures études.

Néanmoins, afin de mieux comprendre l'épilogue de ce mémoire, il semble nécessaire de récapituler les grandes phases de l'étude :

L'examen complet de la revue de littérature, nous a permis de comprendre les internautes et les raisons de leurs inquiétudes par rapport à la sécurité et à la vie privée dans le contexte de la protection des renseignements personnels. Des craintes qui semblent limiter le potentiel énorme du commerce électronique tellement l'économie de la trace sur le nouveau média est source d'appréhension. Enfin, après avoir fait le lien entre le sentiment de contrôle sur les renseignements personnels et les services de sécurité et de confidentialité, l'importance du construit de la confiance a été traitée de façon tridimensionnelle.

Par conséquent, la compréhension des phénomènes liés à la sécurité et à la vie privée en commerce électronique, ainsi que l'importance du contrôle comportemental sur les renseignements personnels et de la confiance envers un cybermarchand dans la construction d'un comportement ultérieur nous a permis de schématiser le tout dans un cadre conceptuel.

Suivant ce cadre conceptuel et les objectifs de la recherche, nous avons émis des hypothèses, confirmées ou infirmées par la suite, grâce à une expérimentation en ligne proposant 3 sites Internet créés par la chaire de commerce électronique RBC Groupe Financier. Des sites, qui pour rappel, ne variaient qu'en fonction du contenu et de la présence, ou absence, d'une politique sur la protection des renseignements personnels.

Après deux pré tests très satisfaisants, dont le dernier n'a subi aucune modification pour le test final, 105 répondants ont accepté de participer à l'expérience à laquelle nous avons agrége les 104 répondants ayant pris part au second pré test.

5.1 Synthèse des résultats et conclusion

Tout d'abord, nous débutons la discussion par un récapitulatif des résultats obtenus grâce aux différentes analyses statistiques menées (Analyse de la variance ; Analyse de corrélation ; Analyse de la co-variance). Chaque hypothèse émise est, de fait, reprise dans le tableau suivant :

Tableau 24 : Synthèse des résultats

Hypothèses	C*	I**	Variables en cause	Nature de la relation
H1A	X		Absence ou présence d'une politique sur la protection des renseignements personnels ↦ Contrôle comportemental perçu	Contrôle plus important lors de la présence d'une politique
H1B	X		Traitement des renseignements personnels ↦ Contrôle comportemental perçu	Contrôle plus important lorsque la politique est dynamique en opt-in
H2	X		Contrôle comportemental perçu ↦ Sentiment de confiance alloué au cybermarchand	Plus le contrôle est élevé, plus la confiance dans le cybermarchand est grande
H3A	X		Sentiment de confiance alloué au cybermarchand ↦ Attitude envers l'utilisation du site du cybermarchand	Plus la confiance dans le cybermarchand est grande, plus l'attitude à utiliser le site de ce dernier est positive

H3B	X		Sentiment de confiance alloué au cybermarchand ↦ Intention envers l'utilisation du site du cybermarchand	Plus la confiance dans le cybermarchand est grande, plus l'intention à utiliser le site de ce dernier est positive
H4A		X	Contrôle comportemental perçu ↦ Attitude envers l'utilisation du site du cybermarchand	
H4B	X		Contrôle comportemental perçu ↦ Intention envers l'utilisation du site du cybermarchand	Plus le contrôle est élevé, plus l'intention à utiliser le site du cybermarchand est positive
H5A		X	Médiation du Sentiment de confiance alloué au cybermarchand entre contrôle comportemental perçu et Attitude comportementale	
H5B	X		Médiation du Sentiment de confiance alloué au cybermarchand entre contrôle comportemental perçu et Attitude comportementale	Médiation totale de la confiance allouée au cybermarchand
H6A	X		Contrôle comportemental perçu * Sentiment de confiance alloué au cybermarchand↦ Attitude envers l'utilisation du site du cybermarchand	Modération du contrôle comportemental perçu
H6B		X	Contrôle comportemental perçu * Sentiment de confiance alloué au cybermarchand↦ Intention envers l'utilisation du site du cybermarchand	
H7A		X	Confiance dans le commerce électronique * Sentiment de confiance alloué au cybermarchand↦ Attitude envers l'utilisation du site du cybermarchand	
H7B		X	Confiance dans le commerce électronique * Sentiment de confiance alloué au cybermarchand↦ Intention envers l'utilisation du site du cybermarchand	
H8A	X		Confiance de disposition * Sentiment de confiance alloué au	Modération de la confiance de disposition

			cybermarchand↦ Attitude envers l'utilisation du site du cybermarchand	
H8B		X	Confiance de disposition * Sentiment de confiance alloué au cybermarchand↦ Intention envers l'utilisation du site du cybermarchand	

* Hypothèse confirmée
** Hypothèse infirmée

Le tableau présenté ci-dessus indique des résultats très satisfaisants par rapport au cadre conceptuel proposé et aux hypothèses avancées. En effet, la majorité des hypothèses posées sont ici confirmées.

Premièrement, dans le cadre de l'étude, les politiques sur la protection des renseignements personnels sont bien, pour l'internaute, la source d'un gain de contrôle comportemental sur les renseignements personnels. Il est ainsi démontré qu'un site Internet proposant un lien vers une politique sur la protection des renseignements personnels augmente sensiblement le sentiment de contrôle contrairement à un site n'en faisant pas mention.

Ensuite, basée sur les dimensions de la sécurité, de l'accès et du choix, nous constatons la force d'une politique dynamique fondée sur le consentement préalable (opt-in) par rapport à une politique statique établie sur le consentement implicite de l'internaute (opt-out). En effet, il existe un contrôle perçu des individus sur leurs renseignements personnels significativement plus grand lorsque la politique sollicite l'accord de l'internaute. Néanmoins les résultats démontrent également la faiblesse de l'opt-in par rapport à l'opt-out quant à l'acception des internautes à ce que leurs informations privées divulguées soient utilisées et diffusées dans un but promotionnel en interne comme en externe. Précisons, pour rappel, que 82,35% des internautes ayant consulté la politique statique en opt-out avaient consenti à recevoir des infolettres et des promotions de partenaires contre 4,16% à 8,33% dans le cas de la politique dynamique en opt-in.

Il a aussi été démontré que lorsqu'une politique sur la protection des renseignements personnels (indépendamment du format statique en opt-out et dynamique en opt-in) est présente, il n'existe aucune différence dans le contrôle perçu entre les personnes ayant consulté cette dernière et les autres ne l'ayant pas lu. Néanmoins ce résultat est à prendre avec des pincettes puisque notre recherche révèle également une différence significative entre les personnes ayant lu une politique en format statique en opt-out et les personnes n'ayant pas consulté la politique qui se présentait à eux. Cette différence de perception du contrôle est aussi notable entre les personnes ayant lu une politique en format dynamique en opt-in et les personnes n'ayant pas consulté la politique qui se présentait à eux. Autrement dit, le contrôle perçu est moindre lorsque l'internaute lit un format statique en opt-out que lorsqu'il ne consulte pas la politique pourtant présente. Dans le cas d'une politique dynamique en format opt-in, c'est le contraire, puisque le sentiment de contrôle est plus grand lorsque ce format est consulté que lorsqu'il ne l'est pas.

Par ailleurs, les analyses révèlent que ce même construit du contrôle est corrélé, certes faiblement, mais de façon positive avec le sentiment de confiance à l'égard du cybermarchand, ainsi qu'avec l'intention comportementale d'utiliser ce dernier. Un résultat qui met au jour une médiation partielle de cette confiance dans la relation qui unit contrôle et intention. Les analyses ont en effet prouvé l'existence d'une forte corrélation positive entre la confiance envers le cybermarchand et les comportements ultérieurs (cf. Attitude et Intention envers l'utilisation d'un site Internet marchand). Finalement, la confiance à l'égard du cybermarchand « médit » totalement l'impact du contrôle sur l'attitude comportementale puisque aucune corrélation n'a été établie entre ces deux dernières variables.

Enfin, il est intéressant de constater la modération du sentiment de contrôle comportemental entre la confiance à l'égard du cybermarchand et l'attitude envers ce dernier. Dans le cas présent, la confiance de disposition et la confiance institutionnelle ne font acte d'aucune interaction avec la confiance allouée au cybermarchand lorsque la variable d'intérêt est l'intention d'utiliser ce dernier.

Néanmoins, la confiance de disposition modère la relation entre la confiance dans le site et l'attitude envers l'utilisation de celui-ci.

5.2 *Implications marketing*

Cette recherche tend donc à démontrer l'importance des pratiques liées à la collecte de données privées dans la construction d'un marketing relationnel fondé sur le contrôle et la confiance de l'internaute. En ce sens, si le marketing relationnel ne se préoccupe pas des craintes des internautes, cette économie de la trace ne pourra que difficilement aboutir à des attitudes ainsi qu'à des intentions positives et freineront alors fortement le développement du potentiel du commerce électronique.

Se préoccuper des craintes des consommateurs est donc un devoir éthique mais aussi commercial. Les résultats le démontrent d'eux-mêmes, puisque informer les internautes d'une collecte de données et leur donner le pouvoir (du moins sur les dimensions de l'accès et du choix) impactent positivement sur le contrôle, la confiance ainsi que sur l'attitude et l'intention d'utiliser un site Internet marchand. De fait, il est conseillé aux gestionnaires une transparence et une allocation du pouvoir en informant les cyberconsommateurs des quatre dimensions travaillées à savoir la notification, la sécurité, l'accès et le choix.

Bien évidemment, d'un point de vue éthique et moral, et concernant le traitement des renseignements personnels, nous optons pour des politiques fondées sur le consentement préalable donnant la possibilité aux internautes de se désengager ou bien encore de naviguer anonymement. De plus, la dimension de la sécurité se doit d'être communiquée dans le seul but de démontrer que des mécanismes de régulation sont bien là pour rassurer l'internaute. Enfin, un autre point important est d'inciter les internautes à se renseigner sur ces politiques, qui, nous l'avons vu, augmentent le sentiment de contrôle, de confiance, d'attitude et d'intention.

Néanmoins beaucoup de gestionnaires, en lisant ces lignes, se poseront la question de l'efficacité de l'opt-in contre l'opt-out en ce qui concerne l'acception des internautes

à ce que leurs informations privées divulguées soient utilisées et diffusées dans un but promotionnel en interne comme en externe. Cette recherche a en effet démontré que malgré les avantages que peuvent apporter le consentement préalable, l'opt-out reste cependant le meilleur moyen de récolter des données personnels utilisables pour la promotion et la personnalisation. Sur ce point précis, le conflit reste grand et le gestionnaire doit faire le choix entre un format dynamique en opt-in, dont la force est de générer contrôle et confiance, contre un autre format statique en opt-out moins performant.

Sur ce point précis, Arcand et Nantel (2005) insistent sur le fait que publier une politique sur la protection des renseignements personnels est comme une « arme à double tranchant », d'un côté cela produit un sentiment de contrôle plus faible et impacte donc négativement sur la confiance mais d'un autre coté cela impacte positivement sur la divulgation des renseignements personnels. Dans le cas de notre recherche, « l'arme à double tranchant » opposerait d'un côté une politique dynamique fondée sur le consentement préalable récoltant peu de renseignements personnels utilisables à la promotion mais apportant contrôle et confiance et d'un autre côté une politique statique fondée sur le consentement implicite récoltant en plus grand nombre des informations privées utilisables à la promotion mais apportant moins de contrôle et de confiance.

La solution à ce conflit pourrait être de reconsidérer l'emplacement des politiques dans l'architecture des sites Internet marchands ; des politiques dont l'emplacement ne se situerait pas non plus à la périphérie, mais bien au centre et en amont du processus de navigation. Cette pratique éthique donnerait alors le sentiment de pouvoir et de confiance au consommateur, et commercialement elle renforcerait l'attitude et l'intention d'utiliser le cybermarchand.... Dans ce dessein, une politique dynamique deviendrait donc une porte d'entrée à la navigation, à la fois configurable et personnalisable, dont le consommateur serait le seul à posséder les clefs. Des clefs susceptibles, par la suite, d'être confiées au cybermarchand digne de confiance et en mesure de placer des offensives de commercialisation bien perçues accompagnées d'une plus grande personnalisation de l'offre.

Le marketing de la confiance fondée sur l'allocation du pouvoir deviendrait–il alors une garantie indispensable à l'avenir du commerce électronique ? Ce type de marketing ne pourrait-il pas se situer en amont d'une économie de la trace, afin de résoudre la problématique de son acceptation par les internautes ?

En tout cas, un fait s'avère évident dans la mise en place de stratégie en commerce électronique, le gestionnaire se doit de considérer les notions de contrôle et de confiance ; deux construits reposant sur les dimensions de la notification, de la sécurité, de l'accès et du choix.

5.3 *Limites et avenues de recherche*

Tout d'abord, nous souhaitons informer le lecteur qu'il est difficile d'affirmer que les résultats de cette recherche sont représentatifs des Québécois car l'échantillonnage n'est pas probabiliste. Aussi, nous pensons, que le nombre de répondants constitue une limite à la généralisation des résultats.

Par ailleurs, nous constatons quelques limitations d'un point de vue méthodologique. Premièrement, les politiques sur la protection des renseignements personnels construits ont été volontairement abrégées afin de rendre leur lecture aisée et d'optimiser le nombre d'individus les ayant réellement lues. Néanmoins la réalité est tout autre. De plus, il semble que le fait d'avoir explicitement incité les participants à prendre connaissance des politiques constitue une limite à la validité externe de l'étude.

Deuxièmement, le choix du cybermarchand peut s'avérer être en soi une certaine limite dans le sens où ce dernier (cf. siriuscanada.ca) propose un nouveau service méconnu du grand public susceptible de faire concurrence au monde de la gratuité, à savoir, la radio en ligne, le podcasting[9], ou bien encore le téléchargement de musique

[9] Le podcasting : Moyen de diffusion de fichiers sonores sur Internet. Il permet aux utilisateurs de s'inscrire à un flux (feed en anglais) et ainsi de récupérer de nouveaux fichiers audio automatiquement.

sur les réseaux P2P[10]. Ce dernier point peut sensiblement impacter sur les attitudes et intentions envers l'utilisation d'un cybermarchand proposant un service de musique payant. En ce sens, il aurait sans doute été pertinent de choisir un cybermarchand vendant des produits ou services que l'on ne trouve pas gratuitement sur l'Internet, afin de ne pas biaiser les comportements ultérieurs.

Troisièmement, nous pensons qu'un environnement contrôlé pourrait, contrairement à notre expérimentation, mettre en évidence des phénomènes et des variables non décelées dans un environnement non contrôlé. En effet, comme diraient Kerlinger et Lee (2000) : *« The ideal of science is the controlled experiment »*[11]*(P.467).* Dans ce raisonnement, la méthode connue sous le terme d'analyse par protocole (Sénecal et al., 2002) aurait sans doute permis d'étudier de nouveaux comportements et de nouvelles perceptions grâce à la verbalisation lors de la navigation. Simultanément, chaque internaute sondé aurait alors pu analyser sa propre navigation grâce à un enregistrement vidéo qui, par la suite aurait été approfondi grâce aux logs, entrevues et autres questionnaires.

Pour ce qui a trait au cadre conceptuel, le contrôle a été travaillé de façon unidimensionnelle. En outre, il serait intéressant de considérer, dans un nouveau modèle, les trois dimensions que la revue de littérature a su déceler, à savoir, le contrôle comportemental, décisionnel et cognitif. De plus, la confiance, uniquement concentrée sur la dimension de l'intégrité, pourrait englober les autres dimensions que Mayer et al. (1995) ont su remarquer, c'est-à-dire la bienveillance et la compétence.

Finalement, nous pensons que certaines variables auraient pu apporter une grande contribution à la recherche. De la même manière, nous pensons à la taille perçue et la réputation perçue d'un marchand précédemment étudiées par Jarvenpaa et al. (2000)

---

[10] P2P : Peer to peer ou poste à poste : Technologie de mise en connexion directe de micros à distance où chaque ordinateur est interconnecté et peut s'échanger n'importe quel type de fichiers (exemple : Limewire, Edonkey, Kazaa, Morpheus, etc...)

[11] Notre traduction : La science idéale est l'expérimentation contrôlée.

susceptibles d'affecter le sentiment de confiance, le risque perçu (Mayer et al., 1995) et de modifier l'intention.

Bibliographie

ADAMS, A. et SASSE, M.A. (1999), « Privacy issues in ubiquitous multimedia environments: wake sleeping dogs, or let them lie? », *In Proceedings of Interact '99, IFIP TC.13 International Conference on Human-Computer Interaction*, pp. 214-221.

ALAIN, M. (2000). La Psychologie du Contrôle», [réf. du 10 septembre 2005]. <http://www.uqtr.ca/cours/pls-1009/Psychologie_du_controle/grandes_lignes.htm>.

AJZEN, I. et MADDEN, T.J. (1986). « Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control », *Journal of Experimental Social Psychology*, vol. 22, pp. 453-474.

AJZEN, I. (1988). *Attitudes, personality, and behavior*, Open University press, Milton-Keynes, 188 p.

AJZEN, I. (1991). « The theory of planned behavior », *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211.

ANG, L., DUBELAAR, C. et LEE, B. (2001). « To trust or not to trust ? A model of Internet trust from the customer's point of view », *14th Bled Electronic Commerce Conference, Bled, Slovenia* [réf. du 5 fevrier 2005]. <http://www.uow.edu.au/~boon/Bled2001.pdf>.

ARCAND, M. et NANTEL, J. (2005). « A website's privacy policy: a double-edged sword. Risks and benefits when consumers read your privacy statement », *12th Annual International Conference Promoting Business Ethics, New York, US* [réf. du 24 Avril 2006]. <http://www.net-question.com/chairerbc/fichiers/51002.pdf >.

AVERILL, J.R. (1973). « Personal control over aversive stimuli and its relationship to stress », *Psychological Bulletin.* vol. 80, no. 4, pp. 286-303.

BANDURA, A. (1982). « Self-efficacy mechanism in human agency », *American Psychologist*, vol. 37, no. 2, pp. 122-147.

BARON, R. M. et KENNY, D. A. (1986). « The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations », *Journal of Personality and Social Psychology*, vol. 51, pp. 1173-1182.

BARWISE, P., HAMMOND, K. et ELBERSE, A. (2002) « Marketing and the Internet: A research review », *Future Media Working Paper*, [réf. du 8 Novembre 2005]. <http://www.marketingandtheinternet.com>.

BATESON, J.E.G. et HUI, M.K. (1991). « Perceived control and the effects of crowding and consumer choice on the service experience », *Journal of Consumer Research*, vol. 18, no. 2, pp. 174-184.

BÉLANGER, F., HILLER, J.S. et SMITH, W.J. (2002). « Trustworthiness in electronic commerce: The role of privacy, security, and site attributes », *Journal of Strategic Information Systems*, vol. 11, no. 3-4, pp. 245-270.

BETTER BUSINESS BUREAU (2001). « Third-party assurance boosts online purchasing », [réf. du 14 Juin 2006]. < www.bbbonline.org/ about/press/2001/101701.asp>.

BUCHHOLZ, R.A. et ROSENTHAL, S.B. (2002). « Internet privacy: Individual rights and the common good », *S.A.M. Advanced Management Journal*, vol. 67, no. 1, pp. 34-41.

BHIMANI, A. (1996). « Securing the commercial Internet », *Communications of the ACM*, vol. 39, no. 6, pp. 29-35.

CELSI, R.L. et OLSON, J. (1989), « The effects of felt involvement on consumers' attention and comprehension processes », *Journal of Consumer Research*, vol. 15, no. 2, pp. 210-224.

CHANG, M.K. (1998). « Predicting unethical behavior: A comparison of the theory of reasoned action on the theory of planned behavior », *Journal of Business Ethics*, vol. 17, no. 16, pp. 1825-1835.

CHEN, S.C. et DHILLON, G.S. (2003). « Interpreting Dimensions of Consumer Trust in E-Commerce », *Information Technology and Management*, vol. 4, no. 2-3, pp. 303-318.

CHEUNG, C.M.K et LEE, M.K.O. (2001). « Trust in Internet shopping: Instrument development and validation through classical and modern approaches », *Journal of global Information Management*, vol. 9, no. 3, pp. 23-35.

CHIRAVURI, A. et NAZARETH, D. (2001). « Consumer trust in electronic commerce: An alternative framework using technology acceptance », *Proceedings of the Seventh Americas Conference on Information Systems*, pp. 781-784.

COMMUNAUTIQUE (2002). « La lutte contre la pauvreté et l'exclusion : le moteur du développement de l'Internet citoyen », [réf. du 25 mars 2006]
< http://www.communautique.qc.ca/docomtiq/moteur.html >.

DAHLBERG, T., MALLAT, N. et OORNI, A. (2003). « Consumer acceptance of mobile payment solutions », *Proceedings of the CIC Roundtable*, [réf. du 11 septembre 2005]. <http://web.hhs.se/cic/roundtable2003/papers/D31_Dahlberg_et_al.pdf >.

DAVIS, F.D., BAGOZZI, R.P. et WARSHAW, P.R. (1989). « User acceptance of computer technology: a comparison of two theoretical models », *Management Science*, vol. 35, no. 8, pp. 982-1003.

DECI, E.L. et RYAN, R.M. (1991). *Intrinsic Motivation and Self-Determination in Human Behavior*, In Steers, Motivation and Work Behavior, 5° édition, pp. 44-58.

DECONCHY, J-P (2004) « Lorsqu'on veut expliquer l'inexplicable… », *Cerveau et Psycho*, Décembre, no. 8 [réf. du 8 avril 2005].
< http://auriol.free.fr/psychiatrie/inexplicable.htm >.

EASTLICK, M.A. et LOOTZ, S.L. (1999). « Profiling potential adopters of an interactive shopping medium », *International Journal of Retail and Distribution Management*, Vol. 27, no. 6-7, pp. 209-223.

FARANDA, W.T. (2001). « A scale to measure the cognitive control form of perceived control: Construction and preliminary assessment », *Psychology & Marketing*, Vol. 18, no. 12, pp.1259-1281.

FISHBEIN, M. et AJZEN, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley, 578 p.

FISHBEIN, M. et AJZEN, I. (1980). *Understanding attitudes and predicting social behavior*, Prentice-Hall Inc, NJ, Englewood Cliffs. 278 p.

FOXALL , G.R. et GOLDSMITH, R.E .(1994), *Consumer psychology for marketing*, Routledge, 1ère édition, 243 p.

FRIEDMAN, M.I. et LACKEY, G.H. (1991). *Psychology of Human Control: A General Theory of Purposeful Behavior*, New York, NY: Praeger Publishers, 264 p.

FRIEDMAN, B., KAHN, P.H. et HOWE, D.C. (2000). « Trust online », *Association for Computing Machinery. Communications of the ACM*, vol. 43, no. 12, pp. 34-40.

FTC REPORT TO CONGRESS (2000). « Privacy Online: Fair Information Practices In The Electronic Marketplace », [réf. du 18 octobre 2005]. < http://www.ftc.gov/reports/privacy2000/privacy2000.pdf >.

GEFEN, D. et STRAUB, D.W. (2000) « The relative importance of perceived ease-of-use in IS adoption: A study of e-commerce adoption », *Journal of the Association for Information Systems*, vol. 1, no. 8, pp. 1-28.

GEFEN, D. (2000). « E-commerce: The role of familiarity and trust », *Omega – International Journal of Management Science*, vol. 28, no. 6 (décembre), pp. 725-737.

GEFEN, D. (2002). « Reflections on the dimensions of trust and trustworthiness among online consumers », *Database for Advances in Information Systems*, vol. 33, no. 3, pp. 38-53.

GEORGE, J.F. (2004). « The theory of planned behaviour and Internet purchasing », *Internet Research*, Vol. 14, no. 3, pp. 198-212.

GURVIEZ P. et KORCHIA M. (2002). « Proposition d'une échelle multidimensionnelle de la confiance dans la marque », *Recherche et Applications en Marketing*, vol. 17, no. 3, pp. 41-58.

GUSEMAN, Denis S. (1981). *Risk Perception and Risk Reduction in Consumer Services*, American Marketing Association, pp. 200-204.

GRAZIOLI, S. et JARVENPAA, S.L. (2000). « Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers », *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, Vol. 39, no. 4; pp. 395-410.

HOFFMAN, D.L. et NOVAK, T.L. (1996). « Marketing in hypermedia computer-mediated environments: Conceptual foundations », *Journal of Marketing*, Vol. 60, no. 3; pp. 50-69.

HOFFMAN, D.L., NOVAK, T.L. et PERALTA, M. (1999). « Building consumer trust in online environment: the case for information privacy »,
Project 2000 working paper [réf. du 20 septembre 2005].
<http://elab.vanderbilt.edu/Research/papers/Building%20Consumer%20Trust%20in%20Online%20Environments%20%20The%20Case%20for%20Information%20Privacy%20%5BHoffman,%20Novak,%20Marcos%20Peralta%20-%201998%5D.pdf>.

HUNT, S.D., SPARKMAN, R.D. et WILCOX, J.B. (1982), « The pretest in survey research: issues and preliminary findings », *Journal of Marketing Research*, Vol. 19, no. 2, pp. 269-73.

INDUSTRIE CANADA (2005). « Statistiques sur le commerce électronique », (Juin 2005), Tableaux [réf. du 6 septembre 2005]
<http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/gv00163f.html>.

INFOWORLD (2005). « Security concerns to stunt e-commerce growth », (Juin 2005), [réf. du 7 septembre 2005]
< http://www.infoworld.com/article/05/06/24/HNsecurityconcerns_1.html >.

INTERNET WORLD STATS (2005). « Internet usage statistics - The Big Picture World Internet Users and Population Stats », (Juillet 2005), Tableau, [réf. du 6 septembre 2005] < http://www.internetworldstats.com/stats.htm >.

JARVENPAA, S.L. et TODD, P.A. (1997). « Consumer reactions to electronic shopping on the World Wide Web », *International Journal of Electronic Commerce*, vol. 1, no. 2, pp. 59-88.

JARVENPAA, S.L., TRACTINSKY, N. et VITALE, M. (2000). « Consumer trust in an Internet store », *Information Technology and Management*, vol. 1, no. 1-2, p. 45-71.

JUANG, W-S., LEI, C-L. et LIAW, H-T. (2003). « Privacy and anonymity Protection with blind threshold signatures », *International Journal of Electronic Commerce*, vol. 7, no. 2, pp. 143-157.

KARASEK, R.A. (1979). « Job demands, job decision latitude, and mental strain: implications for job redesign », *Administrative Science Quarterly*, vol. 24, pp. 285–308.

KERLINGER, F.N. et LEE, H.B. (2000). Foundations of Behavioral Research, Thomson Learning, 4e édition, 890 p.

KNIGHTS, D., NOBLE, F., VURDUBAKIS, T. et WILLMOTT, H. (2001). « Chasing shadows: control, virtuality and the production of trust », *Organization Studies*, vol. 22, no. 2, pp. 310-336.

LACEY, H.M. (1979). « Control, perceived control, and the methodological role of cognitive constructs », *Choice and Perceived Control*, Lawrence C. Perlmuter, and Richard A. Monty editions, pp. 5-16.

LANGER, E., JANIS, I. et WOLFER, J. (1975). « Reduction of psychological stress in surgical patients », *Journal of Experimental Social Psychology*, vol. 11, pp. 155-165.

LANGFRED, C.W. (2004). « Too much of a good thing? Negative effects of high trust and individual autonomy in self-managing teams », *Academy of Management Journal*, vol. 47, no. 3, pp. 385-399.

LAWRENCE, D.H. (1922). *The Letters of D.H. Lawrence*, vol. 4.

LEE, M. et TURBAN, E. (2001). « A trust model for consumer internet shopping », *International Journal of Electronic Commerce*, vol. 6, no. 1, pp. 75-91.

LEIFER, R. et MILLS, P.K. (1996) « An information processing approach for deciding upon control strategies and reducing control loss in emerging organizations », *Journal of Management*, vol. 6, pp. 113-137.

LIU, C. et ARNETT, K. (2002). « An examination of privacy policies in Fortune 500 Web sites», Mid-American Journal of Business, vol. 17, no. 1, pp. 13-22.

LIU, C., MARCHEWKA, J.T. et KU, C. (2004). « American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce », *Journal of Global Information Management*, vol. 12, no. 1, pp. 18-40.

LIU, C., MARCHEWKA, J.T., LU, J. et YU, C-S. (2005). « Beyond concern - a privacy-trust-behavioral intention model of electronic commerce », *Information & Management*, vol. 42, no. 2, pp. 289-304.

MACINTOSH, G. et LOCKSHIN, L. (1997) « Retail relationships and store loyalty: A multi-level perspective », *International Journal of Research in Marketing*, vol. 14, no. 5, pp. 487-497.

MAYER, R.C., DAVIS, J.H. et SCHOORMAN, F. (1995). « An Integrative Model of Organizational Trust », *Academy of Management Review*, vol. 20, no. 3, pp. 709-734.

MCKNIGHT, D. H., CUMMINGS, L.L. et CHERVANY, N.L. (1998). « Initial trust formation in new organizational relationships », *Academy of Management. The Academy of Management Review*, vol. 23, no. 3, pp. 473-490.

MCKNIGHT, D.H. et CHERVANY, N.L (2002). « What Trust Means in E-Commerce Customer Relationship », *International Journal of Electronic Commerce*, vol. 6, no. 2, pp. 35-53.

MCKNIGHT, D.H., CHOUDHURY, V. et KACMAR, C. (2002). « Developing and validating trust measures for e-commerce: An integrative typology », *Information Systems Research*, Vol. 13, no. 3, pp. 334-359.

MEINERT D.B., PETERSON D.K., CRISWELL J.R. et CROSSLAND, M.D. (2006). « Privacy Policy Statements and Consumer Willingness to Provide Personal Information », *Journal of Electronic Commerce in Organizations*, Vol. 4, no. 1; pp. 1-18.

MILNE, G. et ROHM, A. (2000). « Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives », *Journal of Public Policy & Marketing*, vol. 19, no. 2, pp. 238-249.

MIYASAKI, A.D. et FERNANDEZ, A. (2000). « Internet Privacy and Security: An Examination of Online. Retailer Disclosures », *Journal of Public Policy & Marketing*, vol. 19, no. 1, pp. 54-61.

MOORES, T. (2005). « Do consumers understand the role of privacy seals in e-commerce? », *Communications of the ACM*, Vol. 48, no. 3; pp. 86-91.

MOORMAN, C., DESHPANDE, R. et ZALTMAN, G. (1992). « Relationship between providers and users in market research: the dynamics of trust within and between organizations », *Journal of Marketing Research,* vol. 29, August, pp. 314-328.

MORGAN, R. et HUNT, S.D. (1994). « The commitment-trust theory of relationship marketing? », *Journal of Marketing*, Vol. 58, no. 3; pp. 20-38.

MORRIS, S.A. et MARSHALL, T.E. (2004). « Perceived control in information systems », *Journal of Organizational and End User Computing*, vol. 16, no. 2, pp. 38-52.

NANTEL, J. et ROBILLARD, R. (1990). *Le concept de l'implication dans l'étude des comportements des consommateurs : une revue de littérature*, Ecole des hautes études commerciales, 90-01, 59 p.

NANTEL, J. (2006). « Vers une économie de la trace », *Consortium Marketing 2006*, HEC Montréal.

NATARAAJAN, R. et ANGUR, M.G. (1997). « Perceived control in consumer choice: A closed look. », *Proceedings of the European Conference for the association for Consumer Research*, pp. 288-292.

NEUMAN, P.G. (1991). « Inside RISKS: Computers, Ethics, and Values », *Communications of the ACM*, vol. 34, no. 7, pp. 106-109.

OFFICE QUEBECOIS DE LA LANGUE FRANCAISE (2005). « Vocabulaire d'Internet - Banque de terminologie du Québec », [réf. du 9 septembre 2005] <http://www.infoworld.com/article/05/06/24/HNsecurityconcerns_1.html>.

PARKER, L.E. et PRICE, R.H. (1994). « Empowered managers and empowered workers: The effects of managerial support and managerial perceived control on workers' sense of control over decision making », *Human Relations*, vol. 47, no. 8, pp. 911-928.

PAVLOU, P.A. (2003). « Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model », *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101-134.

PHELPS, J., NOWAK, G. et FERRELL, E. (2000). « Privacy concerns and consumer willingness to provide personal information », *Journal of Public Policy and Marketing*, vol. 19, no. 1, pp. 27-41.

RATNASINGAM, P. et PAVLOU, P.A. (2003). « Technology trust in internet-based interorganizational electronic commerce », *Journal of Electronic Commerce in Organizations*, vol. 1, no. 1, pp. 17-41.

RATNASINGAM, P. (2005) « Trust in inter-organizational exchanges: a case study in business to business electronic commerce », *Decision Support Systems*, vol. 39, no. 3, pp. 525-544.

RATNASINGAM, P., GEFEN, D. et PAVLOU, P.A. (2005). « The Role of Facilitating Conditions and Institutional Trust in Electronic Marketplaces », *Journal of Electronic Commerce in Organizations*, vol. 3, no. 3, pp. 69-83.

REMPEL, J.K., HOLMES, J.G. et ZANNA, M.P. (1985). « Trust in close relationships », *Journal of Personality and Social Psychology*, vol. 49, pp. 95-112.

ROTTER, J.B. (1966). « Generalized expectancies for internal versus external control of reinforcement », *Psychological Monographs*, vol. 80, no. 609.

ROTTER, J.B. (1971). « A new scale for the Measurement of Interpersonal Trust », *Journal of Personality and Social Psychology*, vol. 35, pp. 351-365.

ROTTER, J.B. (1980). « Interpersonal Trust, Trustworthiness and Gullibility », *American Psychologist*, vol. 35, no. 1, pp.1-7.

ROUSSEAU, D., SITKIN, S., BURT, R.S. et Camerer, C. (1998). « Not so different after all: A Cross-discipline view of trust », *Academy of Management Review*, vol. 23, no. 3, pp. 393-404.

SAFE HARBOUR UNITED STATES DEPARTMENT OF COMMERCE (2000), « Safe Harbour Privacy principles », [réf. du 18 octobre 2005] <http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm>.

SARGENT, L.D. et TERRY, D.J. (1998). « The effects of work control and job demands on employee adjustment and work performance », *Journal of Occupational and Organizational Psychology*, vol. 71, pp. 219 -236.

SCHLENKER, B.R., HELM, B. et TEDESCHI, J.T. (1973). « The effects of personality and situational variables on behavioural trust », *Journal of Personality and Social Psychology*, vol. 25, pp. 419-427.

SÉNÉCAL, S., GHARBI, J. et NANTEL, J. (2002), « The Influence of the Flow on Hedonic and Utilitarian Shopping Values », dans S. Broniarczyk et K. Nakamoto (Eds.), Advances in Consumer Research, Vol. 29.

SHIM, S., EASTLICK, M.A., LOTZ, S.L. et WARRINGTON, P. (2001). « An online prepurchase intentions model: The role of intention to search », *Journal of Retailing*, vol. 77, pp. 397-416.

SIRDESHMUKH, D., SINGH, J. et SABOL, B. (2002) « Consumer trust, value, and loyalty in relational exchanges», *Journal of marketing*, vol. 66, no. 1, pp. 15-37.

SKINNER, E.A. (1995). *Perceived Control, Motivation, & Coping.* Individual Differences and Development Series, Thousand Oaks, CA: Sage Publications, vol. 8, 232 p.

SKINNER, D. et SPIRA, L.F. (2003). « Trust and control - a symbiotic relationship ? », *Corporate Governance*, vol. 3, no. 4, pp. 28-35.

SMETANA, J.G. et ADLER, N.E. (1980). « Fishbein's value x expectancy model: An examination of some assumptions », *Personality and Social Psychology Bulletin*, vol. 6, no. 1, pp. 89-96.

SMITH, C.S., TISAK, J., HAHN, S.E. et SCHMIEDER, R.A. (1997). « The measurement of job control », *Journal of Organizational Behavior*, vol. 18, no. 3, pp. 225-237.

SOLOMON, M.R., ZAICHKOWSKY, J.L. et POLEGATO R. (2005), *Consumer Behaviour: Buying, Having, and Being,* Pearson. Prentice Hall, 3ième édition, 640 p.

SPINELLIS, D., KOKOLAKIS, S. et GRITZALIS, S. (1999). « Security requirements, risks and recommendations for small enterprise and home-office environments », *Information Management & Computer Security*, vol. 7, no. 3, pp. 121-128.

STATISTIQUE CANADA (2005). « Préoccupations concernant la confidentialité et la sécurité sur Internet, selon le type d'acheteur en ligne, accès de n'importe quel endroit », [réf. du 6 septembre 2005]

< http://www40.statcan.ca/l02/cst01/comm11a_f.htm?sdi=achats%20ligne >.

SUH, B. et HAN, I. (2003). « The impact of customer trust and perception of security control on the acceptance of electronic commerce », *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 135-161.

TAN, Y-H et THOEN, W. (2001). « Toward a Generic Model for Electronic Commerce», *International Journal of Electronic Commerce*, vol. 5, no. 2, pp. 61-74.

TAN, F. et SUTHERLAND, P. (2004). « Online consumer trust: A multi-dimensional model », *Journal of Electronic Commerce in Organization*, vol. 2, no. 3, pp. 40-53.

TAYLOR, R. (1989). « The Role of Trust in Labor-Management Relations», *Organizational Development Journal*, vol. 7, pp. 85-89.

TAYLOR, S. et TODD, P.A. (1995) « Understanding Information Technology Usage: A Test of Competing Models », I*nformation Systems Research*, vol. 6, no. 2, pp. 144-176.

TSIAKIS, T. et STEPHANIDES, G. (2005). « The concept of security and trust in electronic payments », *Computer and Security*, vol. 24, no. 1, pp. 10-15.

VENKATESH, V. et DAVIS, F.D. (2000). « A theoretical extension of the technology acceptance model: Four longitudinal field studies », *Management Science*, vol. 46, no. 2, pp. 186-204.

VIJAYASARATHY, L.R. et JONES, J.M. (1998). « Internet consumer catalog shopping: findings from an exploratory study and directions for future research », *Internet Research*, vol. 8, no.4, pp. 322-330.

VINCENT, A. (2004). *Les réactions des consommateurs quant aux politiques de confidentialité des cybermarchands*, Montréal, Quebec Amérique, coll. Presses HEC, 186 p.

WANG, Y-S., WANG, Y-M., LIN, H-H. et TANG, T-I. (2003) « Determinants of user acceptance of Internet banking: an empirical study », International Journal of Service Industry, vol. 14, no. 5, pp. 501-519.

WARREN, S.D. et BRANDEIS, L.D. (1980). « The Right To Privacy », *Harvard Law Review*, vol. 5 no. 4, pp. 193-220.

WARRINGTON, T.B., ABGRAB, N.J. et CALDWELL, H.M. (2000), « Building trust to develop competitive advantage in e-business relationships», Competitiveness Review, vol. 10, no. 2, pp. 160-168.

WHITE, R.W. (1959). « Motivation reconsidered: The concept of competence », *Psychological Review*, vol. 66, no. 5, pp. 297-333.

Annexes

Annexe 1 : Questionnaire de la collecte de données finale

0/ Avez-vous pris connaissance de la politique sur la protection des renseignements personnels lors de votre inscription en étape 1?
Oui
Non

Qve/ Question de vérification. veuillez nous indiquer - sur une échelle de 1 à 7 – votre degré d'accord avec les affirmations suivantes. Si vous n'en avez aucune idée, cochez la case 8 intitulée « je ne sais pas ».

1 : La page d'inscription (que vous avez remplie lors de l'étape 1) possède un lien hypertexte dirigeant vers la politique sur la protection des renseignements personnels.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : Lors de mon inscription (cf. étape 1), on m'assure qu'une technologie d'encryptage très puissante protège mes renseignements personnels.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : Lors de mon inscription (cf. étape 1), on m'assure qu'il est possible d'accéder à tout moment à l'information divulguée afin de la vérifier, la modifier ou la supprimer.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

4 : Lors de mon inscription (cf. étape 1), on m'inclut automatiquement aux listes de distribution.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

5 : Lors de mon inscription (cf. étape 1), on me donne la possibilité (en cochant des cases) d'être inclut dans les listes de distribution.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Qa/ Suite aux différentes informations que vous avez pu lire lors de votre inscription en étape 1, veuillez nous indiquer votre sentiment par rapport au contrôle que vous sentez avoir sur vos renseignements personnels? Veuillez, pour répondre à ces questions nous indiquer - sur une échelle de 1 à 7 - le chiffre qui correspond le mieux à votre sentiment.

1 : Lors de mon inscription en étape 1, j'étais capable de m'assurer de la protection de mes renseignements personnels :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : Lors de mon inscription en étape 1, m'assurer de la protection de mes renseignements personnels était totalement sous mon contrôle lors de mon inscription au panel en étape 1 :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : Lors de mon inscription en étape 1, j'avais les ressources, les connaissances et les compétences pour m'assurer de la protection de mes renseignements personnels:
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Qb/ Les questions suivantes traiteront de la perception que vous avez de Sirius après avoir visité ce dernier lors de l'étape 2. Veuillez, pour répondre à ces questions nous indiquer - sur une échelle de 1 à 7 – votre sentiment :

1: Je me fie à Sirius pour bien faire son travail :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2: J'ai confiance dans Sirius:
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Qc/ Dans cette section, Veuillez nous indiquer votre attitude envers l'utilisation de Sirius après avoir visité ce dernier lors de l'étape 2. Veuillez nous indiquer - sur une échelle de 1 à 7 – votre degré d'accord avec les affirmations suivantes :

1 : Utiliser Sirius serait une bonne idée :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : Utiliser Sirius serait une idée sage :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : Utiliser Sirius serait une idée plaisante :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

4 : Utiliser Sirius serait une idée positive :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

5 : Utiliser Sirius serait une idée attractive :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Qd/ Les questions suivantes vous demandent d'indiquer quelle intention vous avez d'utiliser Sirius suite à ce vous avez pu voir ou lire lors votre visite sur Sirius. Même énoncé que pour les questions précédentes, veuillez nous indiquer - sur une échelle de 1 à 7 – votre degré d'accord avec les affirmations suivantes :

1 : J'ai l'intention d'utiliser Sirius dans le futur :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : J'espère utiliser Sirius dans le futur :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : J'utiliserai fréquemment Sirius dans le futur :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

4 : Je recommanderai fortement aux autres Sirius:
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Les questions suivantes nous permettront de mieux vous connaître. De fait, nous vous poserons trois séries de questions sur votre disposition à croire votre prochain, sur la confiance que vous avez dans le commerce électronique, et, votre perception de la sécurité sur Internet.

Qe/ Veuillez nous indiquer, de façon général, votre prédisposition à croire votre prochain. Veuillez choisir - sur une échelle de 1 à 7 – votre accord ou désaccord avec les affirmations suivantes :

1 : En général, la plupart des gens gardent leurs promesses :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : Je pense que les gens essayent généralement de protéger leurs promesses par l'action :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : La plupart des gens sont honnêtes quand ils font affaires avec les autres :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

4 : Je fais habituellement confiance aux gens jusqu'à ce qu'ils me donnent une raison de ne plus croire en eux
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

5 : Je donne généralement le bénéfice du doute aux gens quand je les rencontre pour la première fois :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

6 : Mon approche typique est de faire confiance à mes nouvelles connaissances jusqu'à ce que celles-ci me prouvent le contraire :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Qf/ Dépendamment de ce que vous avez pu vivre sur la grande toile, veuillez nous décrire votre perception générale du commerce électronique. Pensez bien à tous ce que vous avez vu, entendu et vécu en relation avec le commerce électronique, puis indiquez - sur une échelle de 1 à 7 – votre degré d'accord avec les affirmations suivantes :

1 : Je me sens à l'aise quant au déroulement des choses lorsque je fais un achat ou d'autres activités sur l'Internet :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : Je me sens à l'aise avec le fait de passer un achat sur L'Internet :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : Je me sens à l'aise à devoir me fier à un cybermarchand sachant qu'ils s'acquitteront de leurs obligations :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

4 : Depuis que les cybermarchands s'acquittent généralement de leurs obligations, je me sens à l'aise à faire des affaires sur Internet
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

5 : Lors de la visite chez un cybermarchand, Je suis toujours dans le sentiment de pouvoir me fier à lui :
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Qg/ Dépendamment de ce que vous avez pu vivre sur la grande toile, veuillez nous décrire votre perception générale de la sécurité sur Internet. Pensez bien à tous ce que vous ressentez par rapport à la sécurité sur l'Internet censée protéger vos informations personnelles des attaques. Indiquez - sur une échelle de 1 à 7 – votre degré d'accord avec les affirmations suivantes.

1 : L'Internet possède assez de protection pour me rendre serein lorsque je dois l'utiliser pour traiter de mes affaires personnelles
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

2 : Je suis certain que l'environnement technologique et légal de l'Internet me protège des problèmes liés à l'utilisation du média
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

3 : Je pense que l'encryptage et les autres mécanismes de sécurité présents sur l'Internet fait de cet endroit, un endroit sûr pour faire des affaires.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

4 : De façon générale, L'Internet est devenu un environnement sûr et robuste pour faire des affaires.
Pas du tout d'accord 1 2 3 4 5 6 7 Entièrement d'accord

Les questions suivantes nous permettront de mieux savoir qui vous êtes ?

Qh/ Veuillez nous indiquez votre profil sociodémographique ?

1 : Quel age avez-vous ? ____ ans

2 : Etes vous un homme [ ] ou une femme [ ] ?

3 : Quel est votre statut marital ?
[ ] Célibataire [ ] Marié(e) [ ] Divorcé/séparé [ ] Veuf/veuve

4 : Quel est le dernier niveau de scolarité que vous avez gradué :
[ ] Primaire [ ] Secondaire [ ] Collégial [ ] universitaire, 1er cycle
[ ] universitaire, 1er cycle [ ] universitaire, 2nd cycle [ ] universitaire, 3ième cycle

5 : Quel est le votre statut d'emploi :
[ ] Temps plein [ ] Mi-temps [ ] retraité [ ] A la maison [ ] Etudiant à temps plein [ ] Sans emploi

6 : Quel est votre revenu ?
[ ] $15,000 ou moins [ ] $15,001-$24,999 [ ] $25,000-$50,0000 [ ] Plus de $50,0000

Annexe 2 : Sites internet expérimentaux

Introduction à la recherche pour Pré Test

Sites Internet : 1, 2A, 2B
Étape : Pré Test
Population concernée : Personnes hors panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Page d'introduction à la recherche mentionnant les renseignements liés à la recherche et le recrutement en parallèle pour le panel de la Chaire de Commerce Électronique RBC Groupe Financier

HEC MONTRÉAL

Bonjour Madame, bonjour Monsieur,

Je suis étudiant en maîtrise de marketing à l'école des Hautes Études Commerciales (HEC Montréal). Dans le cadre de ma formation, j'effectue une recherche sur les attitudes des consommateurs face aux pratiques commerciales des marchands électroniques. Vous allez donc être soumis à une expérimentation sur les attitudes des consommateurs face aux pratiques commerciales des marchands électroniques.

Vous avez donc choisi de prendre part à cette étude et donc de participer à cette expérience se déroulant en trois étapes :

- S'inscrire à un panel de la chaire de recherche RBC Groupe Financier (HEC Montreal) en répondant à notre étude sur les habitudes d'écoute et d'acquisition de la musique en ligne.
- Naviguer sur le site Internet Sirius et s'informer sur ce que propose ce marchand en termes de service
- Répondre au questionnaire de la recherche

Vous devez vous inscrire et répondre au questionnaire pour courir la chance de gagner au tirage au sort le iPod nano 4 Gigas

Lors de cette étude, ayez à l'esprit que vous êtes sur un site expérimental de la chaire de recherche RBC Groupe Financier (HEC Montréal). Votre identité en tant que participant ne pourra être retracée à partir des résultats que nous diffuserons. Tous les renseignements personnels collectés seront gardés en sécurité et en toute confidentialité par la chaire de recherche RBC Groupe Financier (HEC Montréal) malgré tout ce que vous pourrez lire lors de votre expérience dans les scénarios ou les politiques sur les renseignements personnels proposés. Notez que l'expérience commence dès que vous avez cliqué sur « Participer et commencer l'expérience ».

Soyez informé qu'en vous inscrivant (Étape 1) à la chaire de Commerce Electronique RBC Groupe Financier, Vous rentrez automatiquement dans un échantillon de personnes que l'on constitue en vue d'effectuer diverses recherches scientifiques.

Répondez sans hésitation aux questions incluses dans les questionnaires, car ce sont vos premières impressions qui reflètent généralement le mieux votre pensée. Il n'y a pas de limite de temps pour répondre aux questionnaires, bien que nous avons estimé que cela devrait vous prendre environ 20 minutes.

Compte tenu des mesures de confidentialité qui seront prises, votre participation ne devrait vous causer aucun préjudice pas plus qu'elle ne vous profitera directement. Vos réponses devraient nous permettre de contribuer au développement des connaissances en marketing. Les informations recueillies resteront strictement confidentielles, et ne seront utilisées que pour l'avancement des connaissances et la diffusion des résultats globaux dans des forums savants ou professionnels.

Vous êtes complètement libre de refuser de participer à ce projet, et vous pouvez décider en tout temps d'arrêter de répondre aux questions. Le fait de remplir ce questionnaire sera considéré comme votre consentement à participer à notre recherche. Si vous avez des questions concernant cette recherche, vous pouvez contacter le chercheur principal, Monsieur Mathieu Arles-Dufour au numéro de téléphone et/ou à l'adresse de courriel indiqués ci-dessous.

Merci de votre précieuse collaboration!

Mathieu Arles-Dufour
mathieu.arles-dufour@hec.ca

☐ ***J'affirme que j'ai pris connaissance des renseignements sur la présente recherche***

☐ ***J'accepte de m'inscrire au panel de la chaire de recherche RBC Groupe Financier (HEC Montréal) lors de cette expérience (en étape 1) afin d'être sollicité pour participer aux futures enquêtes et recherches de la chaire***

☐ ***Je comprends que le fait de répondre au questionnaire (en étape 3) correspond à donner mon consentement à participer à la recherche***

Le comité d'éthique de la recherche de HEC Montréal a statué que la collecte d'information liée à la présente étude satisfait aux normes éthiques en recherche auprès des êtres humains. Pour toute question en matière d'éthique, vous pouvez contacter le secrétariat de ce comité au (514) 340-6257.

Participer et commencer l'expérience -->>

Introduction à la recherche pour Test

Sites Internet : 1, 2A, 2B
Étape : Test
Population concernée : Personnes du panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Page d'introduction à la recherche mentionnant les renseignements liés à la recherche et le recrutement en parallèle pour le panel de la Chaire de Commerce Électronique RBC Groupe Financier

HEC MONTRÉAL

Bonjour Madame, bonjour Monsieur,

Je suis étudiant en maîtrise de marketing à l'école des Hautes Études Commerciales (HEC Montréal). Dans le cadre de ma formation, j'effectue une recherche sur les attitudes des consommateurs face aux pratiques commerciales des marchands électroniques. Vous allez donc être soumis à une expérimentation sur les attitudes des consommateurs face aux pratiques commerciales des marchands électroniques.

Vous avez donc choisi de prendre part à cette étude et donc de participer à cette expérience se déroulant en trois étapes :

- S'inscrire à notre programme de recherche RBC Groupe Financier sur les habitudes d'écoute et d'acquisition de la musique en ligne en répondant à une première courte enquête. Ne vous inquiétez pas, aucune compétence n'est requise.
- Naviguer sur le site Internet Sirius et s'informer sur ce que propose ce marchand en termes de service
- Répondre au questionnaire de la recherche

Vous devez vous inscrire et répondre au questionnaire pour courir la chance de gagner au tirage au sort le iPod nano 4 Gigas

Lors de cette étude, ayez à l'esprit que vous êtes sur un site expérimental de la chaire de recherche RBC Groupe Financier (HEC Montréal). Votre identité en tant que participant ne pourra être retracée à partir des résultats que nous diffuserons. Tous les renseignements personnels collectés seront gardés en sécurité et en toute confidentialité par la chaire de recherche RBC Groupe Financier (HEC Montréal) malgré tout ce que vous pourrez lire lors de votre expérience dans les scénarios ou les politiques sur les renseignements personnels proposés. Notez que l'expérience commence dès que vous avez cliqué sur « Participer et commencer l'expérience ».

Répondez sans hésitation aux questions incluses dans les questionnaires, car ce sont vos premières impressions qui reflètent généralement le mieux votre pensée. Il n'y a pas de limite de temps pour répondre aux questionnaires, bien que nous avons estimé que cela devrait vous prendre environ 20 minutes.

Compte tenu des mesures de confidentialité qui seront prises, votre participation ne devrait vous causer aucun préjudice pas plus qu'elle ne vous profitera directement. Vos réponses devraient nous permettre de contribuer au développement des connaissances en marketing. Les informations recueillies resteront strictement confidentielles, et ne seront utilisées que pour l'avancement des connaissances et la diffusion des résultats globaux dans des forums savants ou professionnels.

Vous êtes complètement libre de refuser de participer à ce projet, et vous pouvez décider en tout temps d'arrêter de répondre aux questions. Le fait de remplir ce questionnaire sera considéré comme votre consentement à participer à notre recherche. Si vous avez des questions concernant cette recherche, vous pouvez contacter le chercheur principal, Monsieur Mathieu Arles-Dufour au numéro de téléphone et/ou à l'adresse de courriel indiqués ci-dessous.

Merci de votre précieuse collaboration!

Mathieu Arles-Dufour
mathieu.arles-dufour@hec.ca

☐ ***J'affirme que j'ai pris connaissance des renseignements sur la présente recherche***
☐ ***Je comprends que le fait de répondre au questionnaire (en étape 3) correspond à donner mon consentement à participer à la recherche***

Le comité d'éthique de la recherche de HEC Montréal a statué que la collecte d'information liée à la présente étude satisfait aux normes éthiques en recherche auprès des êtres humains. Pour toute question en matière d'éthique, vous pouvez contacter le secrétariat de ce comité au (514) 340-6257.

Participer et commencer l'expérience -->>

Mise en situation pour Pré Test et Test

Sites Internet : 1, 2A, 2B
Étape : Pré-Test et test
Population concernée : Personnes hors panel et panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Bienvenue sur la Chaire de Commerce Électronique RBC Groupe Financier (HEC Montréal)

Étape 1 : Nous tentons de comprendre vos habitudes d'écoute et d'acquisition de la musique en ligne.

Inscrivez vous de suite à notre programme de recherche RBC Groupe Financier sur les habitudes d'écoute et d'acquisition de la musique en ligne en répondant à notre courte enquête.

Grâce aux informations que vous allez nous fournir, vous nous permettrez par la suite, et cela sur une période d'un an à compter d'aujourd'hui, de :

- Mieux connaître votre comportement avec la musique en ligne en répondant à diverses enquêtes.
- Vous demandez d'évaluer des sites Internet musicaux.

En vous inscrivant, vous consentez à participer à ces enquêtes et évaluations de sites musicaux et êtes d'accord pour faire l'objet d'un monitoring lors de vos prochaines navigations en expérience.

Étape 2 : Naviguez sans plus attendre sur le site Sirius, site proposant un service de radio satellite, et informez vous sur ce que propose ce cybermarchand en terme de services

Étape 3 : Répondez finalement au questionnaire portant sur :

- Vos impressions à la suite de votre inscription au programme de recherche sur les habitudes d'écoute et d'acquisition de la musique en ligne.
- Votre navigation sur Sirius.

Continuer -->>

Page centrale de l'expérience pour Pré Test et Test

Sites Internet : 1, 2A, 2B
Étape : Pré Test et test
Population concernée : Personnes hors panel et panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Page index de l'expérience redirigeant vers les différentes étapes à réaliser. Cette page comporte un cadre navigable dans lequel est incorporé le site Sirius

HEC MONTRÉAL Chaire de Commerce Électronique RBC Groupe Financier

Vous êtes à présent sur la page principale de l'expérience. Dans le cadre droit se situe le site Sirius ; Dans le cadre gauche se situe les instructions et liens pour compléter toutes les étapes de l'expérience.

Etape 1 : Nous tentons de comprendre et de suivre au mieux votre comportement en matière de téléchargement de musique. Inscrivez vous à notre programme pour participer à nos futures recherches sur la musique et courir ainsi la chance de gagner un prix exceptionnel pour chaque étude réalisée.

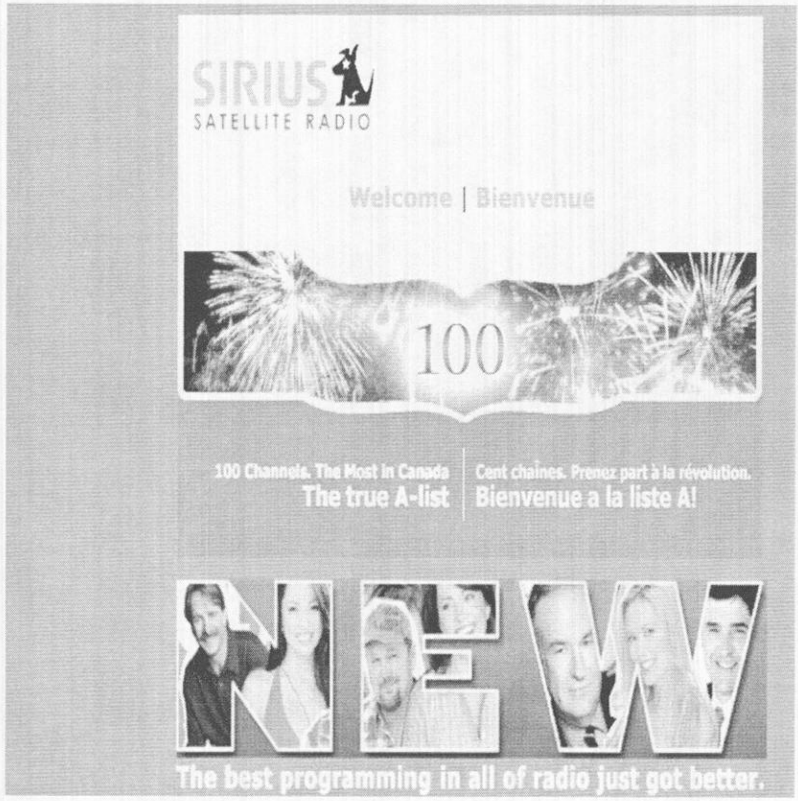
Indice étape 1 : Lors de votre inscription prenez le temps de bien mesurer les conséquences de votre acte sur l'utilisation qui sera faite de vos renseignements personnels.

INSCRIVEZ-VOUS

Étape 2 : Naviguez librement sur Sirius dans le cadre droit de la page. Informez-vous sur ce que propose ce marchand en termes de services. Dès que vous avez terminé votre navigation, passez à l'étape 3.

Étape 3 : Après inscription et navigation sur Sirius, accédez au questionnaire.

QUESTIONNAIRE



Inscription au programme de recherche sur la musique pour Pré Test et Test (cf. : étape 1)

Sites Internet : 1, 2A, 2B
Étape : Pré Test et Test
Population concernée : Personnes hors panel et panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Page index d'inscription au programme pour participer à de futures recherches sur la musique en ligne et ainsi courir la chance de gagner l'incitatif à la recherche.

Inscrivez vous dès maintenant en répondant à nos questions sur vos habitudes d'écoute et acquisition de la musique en format numérique sur Internet...

Lorsque vous vous inscrivez, vous courez la chance de gagner le nouveau iPod Nano 4 gigas de Apple. Votre inscription vous donnera la possibilité de participer à d'autres recherches sur le Podcasting et de tenter, par la même occasion, votre chance pour d'autres fabuleux prix en argent (500$) ou cadeaux.

Vos renseignements seront enregistrés et vous participerez automatiquement au triage au sort après avoir repondu au questionnaire lors de l'étape 3.

Politique sur la protection des renseignements personnels

1- Avez-vous déjà utilisé votre ordinateur pour écouter de la musique ?
○ Oui ○ Non

2- Avez-vous déjà utilisé votre ordinateur pour écouter de la radio sur Internet?
○ Oui ○ Non

3- Avez-vous déjà utilisé un logiciel pour télécharger, conserver ou écouter de la musique ?
○ Oui ○ Non

4- Possédez vous un baladeur numérique MP3 ?
○ Oui ○ Non

De quelle façon, vous procurez vous de la musique en format numérique ?

5- Achat de musique en ligne (iTunes music store, ...)
○ Jamais ○ Rarement ○ Plusieurs fois par mois ○ Plusieurs fois par semaine

6- Logiciels P2P (eDonkey, Limewire, emule...)
○ Jamais ○ Rarement ○ Plusieurs fois par mois ○ Plusieurs fois par semaine

7- Souscription à un service de musique payant (Napster, ...)
○ Jamais ○ Rarement ○ Plusieurs fois par mois ○ Plusieurs fois par semaine

8- Utilisation de logiciels pour transférer sa musique sur CD en format numérique
○ Jamais ○ Rarement ○ Plusieurs fois par mois ○ Plusieurs fois par semaine

9- Partage avec les amis
○ Jamais ○ Rarement ○ Plusieurs fois par mois ○ Plusieurs fois par semaine

10- Combien d'argent dépensez-vous par mois pour l'achat de musique en ligne ?
○ 0$ ○ Moins de 5$ ○ Entre 5 et 15$ ○ Entre 15 et 30$ ○ Plus de 30$

11- Combien de fichiers musicaux possédez vous sur votre ordinateur ?
○ Aucun ○ Moins de 10 ○ Entre 10 et 100 ○ Entre 100 et 1000 ○ Plus de 1000

Veuillez compléter le questionnaire suivant afin que nous puissions vous contacter si vous êtes l'heureux gagnant du iPod nano 4 gigas de Apple.

Nom : _____

Prénom : _____

Année de naissance : _____

Courriel : _____

Adresse postale : _____

Code postal : _____

Ville : _____

Province : _____

Soumettre

Politique sur la protection des renseignements personnels

Politique sur la protection des renseignements personnels pour Pré Test et Test (cf. : étape 1, site 2A)

Sites Internet : 2A
Étape : Pré Test et test
Population concernée : Personnes hors panel et panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Politique sur la protection des renseignements personnels pour le site 2A. Cette politique est statique en opt-out et se situe sur la page d'inscription au programme de recherche sur la musique

Politique sur la protection des renseignements personnels

Divulguez vos renseignements personnels en toute sécurité grâce à la mise en place de la technologie d'encryptage la plus puissante qui soit actuellement disponible sur le marché. La technologie SSL 128 bits.

Vous allez recevoir sous peu nos infolettres et bien d'autres informations susceptibles de vous intéresser.
Veuillez nous indiquer par courriel si vous désirez ne pas recevoir ces offres.

Vous allez recevoir sous peu des offres de nos partenaires commerciaux susceptibles de vous intéresser. Veuillez nous indiquer par courriel si vous désirez ne rien recevoir.

Dans le but de vous offrir un experience personnalisée, nous recevons et nous enregistrons vos informations personnelles. Nous utilisons notamment des « cookies » qui seront intégrer automatiquement dans votre ordinateur. Si vous souhaitez naviguer anonymement, certaines sociétés developpent des logiciels exprès. Voici les adresses de quelques-unes d'entre elles : http://www.anonymizer.com, http://www.idzap.com, http://www.somebody.net. Nous ne garantissons pas l'efficacité de ces produits.

Fermer la fenêtre

Politique sur la protection des renseignements personnels pour Pré-Test et Test (cf. : étape 1, site 2B)

Sites Internet : 2B
Étape : Pré Test et Test
Population concernée : Personnes hors panel et panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Politique sur la protection des renseignements personnels pour le site 2B. Cette politique est dynamique en opt-in et se situe sur la page d'inscription au programme de recherche sur la musique

Politique sur la protection des renseignements personnels

Divulguez vos renseignements personnels en toute sécurité grâce à la mise en place de la technologie d'encryptage la plus puissante qui soit actuellement disponible sur le marché. La technologie SSL 128 bits.

À tout moment, vous pouvez accéder à toute l'information que vous nous avez transmise afin de la vérifier, la modifier ou la supprimer.

☐ Informez nous, en cochant cette case, si vous souhaitez recevoir des infolettres et bien d'autres informations susceptibles de vous intéresser.
☐ Informez nous, en cochant cette case, si vous souhaitez recevoir des offres de nos partenaires commerciaux susceptibles de vous intéresser.
☐ Informez nous en cochant cette case si vous souhaitez naviguer anonymement. Aucun cookies ne seront enregistrés sur votre ordinateur.

Fermer la fenêtre

Page d'introduction au questionnaire final pour Pré Test et Test (cf. : étape 3)

Sites Internet : 2A
Étape : Pré Test et Test
Population concernée : Personnes hors panel et panel de la Chaire de la Commerce Électronique RBC Groupe Financier

Note : Page d'introduction au questionnaire final. Cette étape est la troisième et dernière à réaliser pour les individus sondés.

Renseignements relatifs au questionnaire

Nous sommes dans la dernière étape, veuillez bien répondre au questionnaire. **Vous devez remplir le questionnaire pour valider votre participation au tirage au sort et courir la chance de gagner le iPod nano 4 gigas**.

Information concernant le questionnaire :

- Lisez attentivement les questions ou affirmations puis veuillez cocher les cases correspondant à votre réponse ou degré d'accord.
- A la fin du questionnaire, cliquez sur « soumettre » pour valider ce dernier
- Ensuite, vous serez dirigé vers une page de remerciements, confirmant votre inscription pour courir la chance de gagner le iPod nano.

Merci de votre collaboration!

Continuer