Sécurité des paiements et développement du commerce électronique*

David BOUNIE†et Marc BOURREAU‡

19 mars 2004

Résumé

Cet article aborde la question de la sécurité des paiements sur Internet, et propose un cadre formel pour en étudier l'impact sur le développement du commerce électronique. Nous montrons, dans le cadre d'une offre concurrentielle de sécurité des paiements, que le faible développement des échanges peut être attribué au risque de fraude perçu par les consommateurs honnêtes, mais pas à la fraude des consommateurs opportunistes, qui a elle tendance à augmenter les quantités échangées. Nous montrons aussi que, même si le niveau de sécurité peut-être plus élevé avec un monopole sur la sécurité, une concurrence entre offreurs de sécurité est toujours (1) préférable pour stimuler le développement du commerce électronique et (2) socialement souhaitable.

Mots-clés : Sécurité ; Paiement électronique ; Commerce électronique ; Internet.

Codes JEL : L1 ; L86.

*Nous remercions Pierre Morin, ainsi que deux rapporteurs anonymes, pour leurs suggestions et leurs remarques.

†ENST, Département EGSH, Paris, France. E-mail : david.bounie@enst.fr. Adresse : ENST, Département EGSH, 46 rue Barrault, 75013 Paris, France.

‡ENST, Département EGSH, et CREST-LEI, Paris, France. E-mail : marc.bourreau@enst.fr.

1 Introduction

Différentes études suggèrent que les failles dans la sécurité des paiements sur Internet freinent le développement du commerce électronique. Une étude CREDOC/Raffour Interactif, reprise par un rapport d'information de l'assemblée nationale [2001], indique : « *Interrogés sur ce qu'ils considèrent comme un « frein » à la décision d'achat sur Internet, 67% des internautes évoquent la sécurité des modes de paiement, 50% le surcoût lié à la livraison, 47% la réutilisation possible des données personnelles, 44% le service après vente (...)* ». Ce constat n'est pas propre à la France : des sondages réalisés auprès des internautes anglais (Experian [2001]) et américains (PaymentOne [2003]) révèlent les mêmes craintes. Les internautes ne sont du reste pas les seuls inquiets. Comme le montre une note récente de l'INSEE (INSEE [2001]), les e-marchands sont également réticents à la vente en ligne, dans la mesure où une partie des transactions sont soit contestées, soit annulées, ou constituent des tentatives de fraude. Ainsi, selon une étude CyberSource [2002] conduite auprès de 341 e-marchands implantés dans le monde, la fraude s'éléverait en moyenne à 3% du chiffre d'affaires, 22% de ces e-marchands enregistrant des taux de fraude supérieurs à 5% du chiffre d'affaires.

Dans ce contexte de manque de confiance dans le paiement sur Internet, de nombreux systèmes de paiement électronique sont proposés aux agents économiques afin de sécuriser leurs transactions. Ces systèmes peuvent être regroupés au sein de cinq grandes classes. Une première classe est constituée de *protocoles de sécurisation* des paiements par carte bancaire adossés ou non à un mécanisme de signature électronique (*Secure Electronic Transaction*, *Secure Socket Layer*). Une deuxième classe de systèmes est articulée autour de comptes provisionnés par les internautes et ouverts auprès d'intermédiaires non-bancaires. Dans ces systèmes, des identifiants et mots de passe se substituent à la carte bancaire pour authentifier les internautes et autoriser l'intermédiaire à régler les positions débitrices et créditrices des e-marchands et internautes (*Paypal*, *Easycode*). Une troisième classe de systèmes, les *systèmes privés de fidélisation*, permet le transfert de points de fidélité constituant un réel pouvoir d'achat entre les partenaires du réseau (*Beenz*, *i-point*). Une quatrième classe appellée *système de recouvrement de créances* permet aux abonnés de fournisseurs d'accès Internet de consommer en ligne des produits et services qui seront payés avec la facture téléphonique (*W-HA*, *Password*). Enfin, la cinquième classe de systèmes a trait à de nouveaux instruments de paiement appartenant à *la monnaie électronique* : le porte-monnaie électronique (*Avant*) et le porte-monnaie virtuel (*Ecash*).

Parmi l'ensemble de ces systèmes, la première classe constituée de protocoles de sécurisation des paiements par carte bancaire est la plus utilisée sur Internet. Au sein de cette classe, trois grandes offres de sécurisation des paiements caractérisées par des niveaux de sécurité croissants sont en concurrence : le système *Secure Socket Layer (*SSL), avec ou sans intermédiaire, non adossé à un mécanisme de signature électronique et le système de type *Secure Electronic Transaction* ou *Cyber-COMM* adossé à un mécanisme de signature électronique. Le

système SSL sans intermédiaire se caractérise par une double asymétrie d'information entre internautes et e-marchands. Il ne permet pas de lever l'ambiguïté d'une fraude ou d'une contestation éventuelle sur le paiement, à l'initiative de l'internaute ou du e-marchand. Le système SSL avec intermédiaire permet de résoudre le problème d'asymétrie d'information du côté de l'internaute, en faisant intervenir un intermédiaire bancaire ou non-bancaire. Cet intermédiaire endosse, pour la circonstance, le rôle de tiers de confiance dans les transactions et protège donc l'internaute des e-marchands malintentionnés. Le e-marchand n'est cependant pas protégé des risques de contestation ou de fraude de la part d'internautes opportunistes. Enfin, le système avec signature électronique de type *Secure Electronic Transaction* ou *Cyber-COMM* répond à cette dernière difficulté en supprimant toute asymétrie d'information entre internautes et e-marchands et donc toute possibilité de fraude à l'initiative soit d'un e-marchand malintentionné soit d'un internaute opportuniste.

Dans le cadre d'une concurrence de ces offres de sécurisation des paiements par carte bancaire sur Internet, deux séries de questions émergent. La première a trait à l'impact de la sécurisation des paiements en ligne sur le développement du commerce électronique. Plus précisément, une sécurisation imparfaite (système SSL avec ou sans intermédiaire) a-t-elle réellement une incidence négative sur les quantités de biens et services commercialisées sur Internet ? Les systèmes de paiement avec signature électronique, en supprimant la fraude, sont-ils plus appropriés ? La deuxième série de questions concerne l'influence de la structure de marché de l'offre de sécurité des paiements sur le développement du commerce électronique. Une structure de marché concurrentielle de l'offre de sécurité des paiements est-elle socialement préférable à une structure de marché de type monopolistique ? En d'autres termes, quel peut être l'impact d'une initiative bancaire ou d'une politique publique ayant pour objectif l'exclusion, sur le marché de l'offre de sécurité des paiements, de toute solution concurrente proposée par un intermédiaire non-bancaire au motif du monopole des établissements de crédit en matière de gestion des instruments de paiement ? L'objectif de cet article est de proposer un cadre formel pour répondre à ces questions.

Le reste de l'article est organisé comme suit. Dans une première partie, nous exposons les principes techniques de la sécurité des paiements par carte bancaire et les modèles d'affaires qui en découlent. Dans une deuxième partie, nous présentons le modèle. Dans une troisième partie, nous analysons l'impact du niveau de sécurité des paiements sur le développement du commerce électronique, en supposant que l'offre de sécurité est concurrentielle. Dans une quatrième partie, nous étudions l'impact de la structure de marché de l'offre de sécurité sur le développement du commerce électronique et le bien-être collectif. Dans une cinquième partie, nous concluons cet article.

2 La sécurité des paiements sur Internet : principes techniques et offres de sécurisation

2.1 Quelques éléments d'ordre technique

Plusieurs problèmes techniques sont à résoudre pour sécuriser les paiements sur Internet. Le premier a trait à la *confidentialité* des données. Ce problème est généralement résolu par l'usage de systèmes cryptographiques qui permettent le codage d'un message intelligible en un texte chiffré incompréhensible (sachant que le destinataire légitime doit pouvoir déchiffrer le texte chiffré et obtenir le texte clair). Le deuxième problème technique concerne la garantie de l'origine (*authenticité*) et de l'*intégrité* des messages expédiés. En d'autres termes, les interlocuteurs doivent être assurés que les messages n'ont pas été modifiés durant leur transit sur le réseau et que ceux-ci proviennent bien de leur partenaire en relation. Ces deux problèmes sont généralement résolus par l'emploi d'une signature électronique. Enfin, le troisième problème technique concerne l'*authentification* des utilisateurs. Autrement dit, il convient de s'assurer que les dispositifs - *i.e.* les clés électroniques - qui permettent de chiffrer et déchiffrer les messages appartiennent bien aux utilisateurs déclarés. Pour garantir cette authentification, un certificat électronique émis par une autorité de certification (entreprise, banque, administration) est utilisé. Le certificat électronique garantit le lien entre une clé et son "propriétaire" (une personne, un routeur, un serveur).

L'ensemble de ces problèmes techniques doivent donc être résolus pour assurer un niveau de sécurité maximal des paiements sur Internet. Pourtant, si tous les systèmes de paiement électronique garantissent la confidentialité et l'intégrité des données, seuls quelques systèmes permettent de satisfaire les exigences d'authenticité des messages et d'authentification des auteurs des paiements. Plusieurs offres de sécurisation des paiements par carte bancaire caractérisées par des niveaux de sécurité croissants sont alors en concurrence sur le marché. La partie qui suit présente ces offres de sécurisation.

2.2 Les offres de sécurisation des paiements par carte bancaire sur Internet

Trois types d'offre se sécurisation coexistent.

2.2.1 Le système SSL sans intermédiaire

Le système *Secure Socket Layer* (SSL) est un protocole de sécurisation des transactions. Ce protocole, conçu à l'origine par Netscape, et normalisé par l'*Internet Engineering Task Force* sous le nom de *Transport Layer Security* (TLS), permet de transmettre de manière sécurisée le numéro de carte bancaire sur Internet. SSL est aujourd'hui le système le plus utilisé sur Internet. Selon le 9ème baromètre du commerce électronique en France, 71,8% des sites marchands qui permettaient d'exécuter une transaction en ligne au premier juin

2001 (vente ou réservation intégralement en ligne) offraient une sécurisation SSL. Comme les sources du standard SSL/TLS sont libres et gratuites pour des applications commerciales, ce dernier peut être exploité individuellement par les e-marchands.

Quatre acteurs sont présents dans la transaction : l'internaute, le e-marchand, l'autorité de certification et la banque du e-marchand. Ce dernier, par l'intermédiaire éventuellement de son hébergeur, exploite le protocole SSL sur son serveur. Mais pour faire usage du protocole, il doit faire appel à une autorité de certification qui lui délivre un certificat électronique. En outre, pour offrir le paiement par carte bancaire en ligne, le e-marchand doit remplir un contrat de paiement à distance avec sa banque. Sa banque, affiliée au réseau des cartes bancaires, s'assure au cours de la transaction de la validité de la carte bancaire et de l'absence d'opposition de la carte. Pour ce service, un pourcentage des ventes est prélevé au e-marchand par sa banque. L'internaute, enfin, ne dispose pas d'équipement logiciel ou matériel pour régler ses transactions et ne paie donc aucun prix pour le service de sécurisation. Il envoie seulement, dans le cadre d'un formulaire sécurisé sur son navigateur web, son numéro de carte bancaire au e-marchand accompagné de son identité et des références de son achat.

Caractéristique 1 : *Dans le modèle SSL sans intermédiaire, une double asymétrie d'information existe entre le e-marchand et l'internaute.*

La faiblesse de ce système réside dans la double asymétrie d'information qui existe entre le e-marchand et l'internaute au cours de la transaction. Le e-marchand, d'une part, n'est pas assuré de l'existence de l'internaute et n'est pas à l'abri d'une répudiation tardive de l'acte de paiement dans la mesure où l'utilisateur ne signe pas électroniquement la transaction. L'internaute, d'autre part, est peu enclin à donner son numéro de carte bancaire au e-marchand dans la mesure ou il n'est ni garanti de la fiabilité du serveur web sur lequel est stocké le numéro de carte bancaire, ni assuré que le e-marchand ne réutilisera pas à son profit le numéro de carte bancaire. Cette double asymétrie d'information demeure même si, en France, la Loi sur la Sécurité Quotidienne du 15 novembre 2001 contient certaines dispositions protègeant le porteur de la carte bancaire du risque de fraude. L'article L 132-4 de cette loi stipule que la "*responsabilité du titulaire [d'une carte bancaire] n'est pas engagée si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de sa carte*". Le troisième alinéa du même article précise également que "*si le titulaire conteste par écrit avoir effectué un paiement ou un retrait, les sommes contestées lui sont recréditées sur son compte par l'émetteur de la carte ou restituées, sans frais, au plus tard dans le délais d'un mois à compter de la réception de la contestation*"[1]. En dépit de ces protections, une aversion au risque de fraude pour les consommateurs demeure dans la mesure où un délai plus ou moins long

[1] Le titulaire d'une carte dispose de 70 jours à compter de la date de l'opération contestée pour déposer sa réclamation. Ce délai peut être prolongé contractuellement (alinéa 6 de l'article L. 132-4).

peut exister entre la demande de remboursement des frais de la fraude et le crédit du compte bancaire.

Pour faire face au problème de double asymétrie d'information, un autre modèle s'est progressivement imposé.

2.2.2 Le système SSL avec intermédiaire

Dans le système SSL avec intermédiaire, le e-marchand fait appel à un intermédiaire – un offreur de sécurité – pour exploiter le protocole SSL. L'offreur de sécurité implémente le protocole sur le serveur marchand, distribue le certificat électronique au e-marchand (acheté au tiers de confiance) et assure la maintenance. La prestation est généralement un tarif binôme composé d'un tarif d'abonnement et d'un tarif fixe sur chaque transaction ou d'un tarif variable sous forme de commission. L'offreur de sécurité peut être un acteur bancaire (*Cybermut* du Crédit mutuel, *P@iement CIC*, etc.), ou alors un acteur non-bancaire, comme *Experian*, *Atos Origin*. On peut estimer que le marché de l'offre de sécurité des paiements par SSL est concurrentiel.

Caractéristique 2 : *Dans le modèle SSL avec intermédiaire, une seule asymétrie d'information existe entre le e-marchand et l'internaute.*

L'originalité de cette offre réside dans la réduction de l'asymétrie d'information qui existe entre le e-marchand et l'internaute. Deux principales fonctions sont ainsi assurées par l'intermédiaire : d'une part, celui-ci se porte garant de l'existence du e-marchand et, d'autre part, il s'engage à ne pas communiquer au e-marchand les références bancaires de l'internaute. Par rapport à l'offre sans intermédiaire, ce modèle a alors l'avantage de réduire les risques de fraude du côté du e-marchand. Cependant, toujours du fait de l'absence de signature électronique du porteur de la carte bancaire au cours de la transaction, ni l'intermédiaire ni le e-marchand ne peuvent authentifier avec certitude l'internaute. Dans ce cas, l'intermédiaire ne peut pas repérer que le numéro de carte bancaire utilisé par un acheteur ne lui appartient pas, à moins qu'il ne s'agisse d'une carte volée ou perdue enregistrée dans le fichier des cartes en opposition du réseau des Cartes Bancaires "CB". Dans ce modèle, il existe alors toujours une asymétrie d'information entre le e-marchand et l'internaute qui est à l'origine de nombreux problèmes. Selon une étude réalisée par Experian en Angleterre, sur un panel de 800 marchands, 40% d'entre eux affirmaient « *avoir été visités plus d'une fois par le même fraudeur et 18% d'entre eux plus de trois fois avant que les fraudes n'aient été détectées et le compte fermé* ». Or, dans la mesure où les faiblesses techniques du protocole SSL ne permettent pas d'authentifier le fraudeur – la majorité des plaintes déposées par les e-marchands étant de toute manière classées sans suite par les autorités policières (Experian [2002]) – les e-marchands mais également les banques des e-marchands supportent intégralement les coûts de la fraude. Un dernier modèle de sécurisation a été proposé afin de répondre à la problématique de l'authentification de l'internaute.

2.2.3 Le système avec signature électronique

Les banques se sont associées à plusieurs reprises pour mettre au point des protocoles de sécurisation des paiements qui authentifient l'internaute dans la transaction : le système *Secure Electronic Transaction* proposé par Visa et MasterCard pour les cartes à piste magnétique et le système Cyber-COMM (Visa, MasterCard, Groupement des Cartes Bancaires, etc.) pour les cartes à puce[2]. Ces systèmes ont pour ambition de réduire les risques de fraude en garantissant aux e-marchands le paiement des ventes effectuées en ligne et en supprimant pour les consommateurs le droit de répudiation des paiements. Pour ce faire, ils utilisent un système de signature électronique authentifiant à distance l'internaute.

Caractéristique 3 : *Dans le modèle avec signature électronique, il n'existe aucune asymétrie d'information entre le e-marchand et l'internaute ; le niveau de sécurité est maximal. Mais, le coût d'un système de paiement électronique est une fonction croissante du niveau de sécurité du système.*

Le système de sécurisation avec signature électronique met en relation cinq acteurs : le porteur de la carte bancaire, le e-marchand, leurs banques respectives et l'offreur de sécurité. Pour adhérer à la solution, le porteur doit se porter acquéreur soit d'un lecteur de carte à puce sécurisé s'il possède une carte à puce soit d'un certificat électronique (porteur étranger muni d'une carte à piste magnétique). De même, le e-marchand obtient un certificat électronique auprès de sa banque qui l'autorise à accepter le paiement par carte bancaire. Ces dispositifs matériels ou logiciels ont pour fonction d'authentifier l'internaute et le e-marchand au cours de la transaction. L'internaute est donc assuré qu'il est en liaison avec un e-marchand certifié, c'est-à-dire reconnu par une banque et, réciproquement, le e-marchand est assuré de l'identité de l'internaute via sa signature électronique. Mais, la sécurisation des paiements est coûteuse car elle implique un équipement logiciel ou matériel pour les internautes et les e-marchands. Dans le cas de la solution par carte à puce, par exemple, les internautes doivent s'équiper d'un lecteur de carte à puce pour un prix de l'ordre de soixante euros. Les e-marchands sont également redevables d'un tarif trinôme : une commission fixe sur chaque transaction, une commission variable sur le montant des ventes réalisées et un abonnement à la solution. En conclusion, si le système de sécurisation par signature électronique permet bien de garantir un niveau de sécurité plus élevé, les équipements et l'infrastructure technique augmentent considérablement les coûts de production du service de sécurité des paiements et réduit d'autant la probabilité d'adoption de la solution par les internautes et les e-marchands.

Dans la suite de l'article, nous proposons un cadre formel pour étudier l'impact du niveau de sécurité des paiements sur le développement du e-commerce.

[2] Un projet européen de normalisation d'un lecteur de carte à puce du nom de FINREAD (acronyme de Financial Transactional IC Card Reader) est aujourd'hui en phase de test auprès de plusieurs instances bancaires au niveau européen.

3 Le modèle

Sur le marché du commerce électronique, les e-marchands se concurrencent sur la quantité de biens et services vendus aux internautes consommateurs. Pour réaliser le paiement des transactions électroniques, les consommateurs et les e-marchands utilisent un système de paiement électronique. Parmi les consommateurs, certains sont "opportunistes" (c'est-à-dire qu'ils fraudent s'il est intéressant et possible pour eux de le faire) et d'autres "honnêtes" (non-fraudeurs). Nous considérons deux types de systèmes de paiement électronique : un système de sécurité basse et un système de sécurité haute. La fraude est possible lorsque le niveau de sécurité est bas, mais impossible lorsque le niveau de sécurité est haut.

3.1 Les e-marchands

Sur le marché du commerce électronique, n e-marchands se font concurrence sur les quantités produites, avec $n \geq 2$. Chaque e-marchand $i \in \{1, 2, ..., n\}$ produit une quantité q_i d'un bien homogène à destination des consommateurs, et vend ce bien au prix p_i. Pour simplifier l'analyse, nous normalisons le coût marginal de production à zéro[3] et il n'y a pas de coûts fixes. Pour commercialiser leur production, les e-marchands utilisent un système de sécurité, de niveau *bas* ou de niveau *haut*.

Le niveau de sécurité bas Lorsque le niveau de sécurité est *bas*, la fraude est possible. Un consommateur opportuniste peut frauder en donnant son numéro de carte bancaire et en contestant la dépense ou en donnant un numéro de carte bancaire volé ou fictif. Le marchand ne peut pas authentifier l'internaute consommateur. Ce cas correspond, par exemple, au modèle SSL.

Le niveau de sécurité haut Lorsque le niveau de sécurité est *haut*, la fraude n'est pas possible, car le marchand authentifie avec certitude le consommateur. Par exemple, si un consommateur opportuniste utilise sa propre carte bancaire, il ne peut pas contester la dépense, car il a apposé sa signature[4]. Ce cas correspond, par exemple, à un système de paiement avec lecteur de carte à puce où l'internaute signe électroniquement la transaction.

Nous supposons que tous les e-marchands adoptent le même système de sécurité. Cette hypothèse est justifiée dans la mesure où les e-marchands sont identiques dans notre modèle[5].

[3] Du fait de cette hypothèse, un marchand réalise une marge nulle en cas de fraude. Dans la section 7, nous revenons sur cette hypothèse et nous montrons que nos résultats restent valables si on suppose que le coût marginal de production est strictement positif.

[4] Nous supposons que les fraudes en ligne dues au vol de la carte bancaire *et* du numéro confidentiel sont négligeables.

[5] Le modèle pourrait être étendu pour étudier les possibilités de différenciation des systèmes de sécurité entre e-marchands.

Les systèmes de sécurité sont fournis sur un marché concurrentiel (section 4) ou monopolistique (section 5). Le tarif pratiqué pour la sécurisation des transactions est une taxe, t, sur chaque unité vendue. Nous supposons que les consommateurs ne paient pas directement pour la sécurisation des paiements. En particulier, les consommateurs ne supportent pas le coût des matériels et logiciels éventuellement nécessaires du côté de l'utilisateur final (comme, par exemple, un lecteur de cartes à puce). Les e-marchands supportent seuls ces coûts, même s'ils peuvent les transférer indirectement sur les consommateurs finals au travers des prix des biens finals.

Le coût marginal par transaction du niveau de sécurité bas est normalisé à zéro. Le coût marginal du niveau de sécurité haut est égal à $c > 0$.

3.2 Les consommateurs

Les consommateurs ont une disposition à payer τ pour le bien offert en ligne. Nous supposons que τ est uniformément réparti dans le segment $[0, 1]$. Un consommateur achète zéro ou une unité du bien.

Par ailleurs, les consommateurs peuvent être *honnêtes* ou *opportunistes*. Les consommateurs opportunistes, en proportion $1 - \theta$ avec $\theta \in]0, 1]$, fraudent si cela leur est profitable. Comme nous ignorons les possibilités de sanction (poursuites policières, etc.), un consommateur opportuniste fraudera toujours si cela est possible, c'est-à-dire si le niveau de sécurité est bas[6]. Les consommateurs honnêtes, en proportion θ, ne fraudent jamais.

Nous supposons aussi que le numéro de carte bancaire d'un consommateur honnête peut être dérobé s'il achète en ligne et que le niveau de sécurité est bas. Nous notons K la perte espérée correspondante[7]. Nous supposons que K est fixe et que $K \in [0, 1]$; en particulier, K est indépendant de la proportion $1 - \theta$ de consommateurs opportunistes. A la fin de la section 4, nous discutons du cas où K augmente avec la proportion de consommateurs opportunistes.

Enfin, nous supposons qu'avec un système SSL *sans* intermédiaire, $K > 0$, car les serveurs des marchands sur lesquels sont stockés les numéros de carte bancaire peuvent être mal sécurisés. Avec un système SSL *avec* intermédiaire, nous considérons que $K \approx 0$.

[6] Dans notre modèle, comme dans celui de Picard (1996), la proportion $1 - \theta$ de consommateurs "opportunistes" est exogène. La proportion de consommateurs "fraudeurs" est, elle, fonction du choix de sécurité des e-marchands. En effet, les consommateurs opportunistes ne deviennent fraudeurs que s'il leur est possible de frauder, c'est-à-dire si le niveau de sécurité est faible. Des extensions possibles de ce modèle consisteraient à introduire une menace de poursuites par les e-marchands ou une relation entre le niveau de sécurité et la proportion des consommateurs opportunistes capables de frauder.

[7] La perte espérée K correspond à la probabilité de vol du numéro de carte multipliée par le coût d'opportunité du temps passé à se faire rembourser si le consommateur repère la fraude à temps et à la perte dans le cas où il ne la repère pas à temps.

4 Offre de sécurité concurrentielle

Dans cette section, nous étudions l'impact du niveau de sécurité (bas ou haut) sur le développement du commerce électronique, lorsque les systèmes de paiement sécurisé sont fournis sur un marché concurrentiel. Dans ce contexte, la taxe t^c prélevée par les offreurs de sécurité en concurrence est égale, à l'équilibre, au coût marginal de production du service de sécurité, c'est-à-dire que $t_B^c = 0$ pour le niveau de sécurité bas et $t_H^c = c$ pour le niveau de sécurité haut.

Nous commençons par étudier l'équilibre du jeu de concurrence en quantité avec un niveau de sécurité haut. Puis, nous résolvons le même jeu avec un niveau de sécurité bas.

4.1 Niveau de sécurité haut

Comme les consommateurs opportunistes ne peuvent pas frauder lors de leurs achats en ligne, ils se comportent comme des consommateurs honnêtes. Pour les consommateurs, les e-marchands sont des substituts parfaits. Par conséquent, les prix sont identiques, soit

$$p_i = p_j = \widehat{p}.$$

Le consommateur marginal, qui est indifférent entre acheter un bien en ligne et ne rien acheter, a une disposition à payer $\tau^* = \widehat{p}$. Comme par hypothèse, la disposition à payer des consommateurs est uniformément distribuée sur l'intervalle $[0, 1]$,

$$\sum_{j=1}^{n} q_j = 1 - \widehat{p}.$$

Le marchand en ligne i maximise son profit,

$$\begin{aligned} \Pi_i &= (p_i - c)\, q_i \\ &= \left(1 - \sum_{j=1}^{n} q_j - c\right) q_i, \end{aligned}$$

par rapport à q_i. A l'équilibre, la quantité produite par chaque marchand est égale à

$$q_H^c = \frac{1-c}{n+1},$$

la quantité totale produite est $Q_H^c = nq_H^c$ et chaque e-marchand obtient le profit

$$\Pi_H^c = \left(\frac{1-c}{n+1}\right)^2,$$

où l'indice H désigne le niveau de qualité haut.

4.2 Niveau de sécurité bas

S'il achète le bien homogène au prix p_i, un consommateur honnête de disposition à payer τ obtient comme surplus net

$$\tau - p_i - K.$$

Le consommateur honnête marginal est donc défini par la disposition à payer $\tau^* = \widehat{p} + K$. Pour les consommateurs opportunistes, un niveau de sécurité bas signifie qu'ils peuvent acheter en ligne en utilisant un autre numéro de carte bancaire que le leur. Le "prix" qu'ils paient pour le bien est donc égal à zéro et leur surplus net est égal à leur disposition à payer, τ. Tous les consommateurs opportunistes acquièrent donc le bien en ligne en fraudant. La demande totale pour le bien s'écrit

$$D = (1 - \widehat{p} - K)\,\theta + 1 - \theta.$$

A l'équilibre, offre et demande se rencontrent. Nous pouvons donc écrire

$$\sum_{j=1}^{n} q_j = (1 - \widehat{p} - K)\,\theta + 1 - \theta,$$

soit encore

$$\widehat{p} = \frac{1}{\theta}\left(1 - \sum_{j=1}^{n} q_j\right) - K.$$

Considérons maintenant le marchand en ligne i. S'il réalise une transaction avec un consommateur, il ignore si ce consommateur est honnête ou opportuniste. Etant donné la demande provenant des consommateurs honnêtes ($(1 - \widehat{p} - K)\,\theta$) et la demande provenant des consommateurs opportunistes ($1 - \theta$), du point de vue d'un vendeur, un acheteur (c'est-à-dire un consommateur qui achète le bien) est honnête avec une probabilité ν et fraudeur avec une probabilité $1 - \nu$[8], avec

$$\nu = \frac{(1 - \widehat{p} - K)\,\theta}{(1 - \widehat{p} - K)\,\theta + 1 - \theta}.$$

Comme un prix strictement positif conduit certains consommateurs honnêtes à ne pas acheter le bien, la proportion d'acheteurs honnêtes (ν) est plus faible que la proportion de consommateurs honnêtes dans la population (θ). Le biais est d'autant plus important que $\widehat{p}$ ou K sont grands.

Le marchand i maximise $\Pi_i = \nu p_i q_i$ par rapport à q_i. En posant

$$Q = \sum_{j=1}^{n} q_j,$$

[8] Ou de manière équivalente, la part des ventes qui provient des consommateurs honnêtes est égale à ν tandis que la part des ventes qui provient des consommateurs fraudeurs est égale à $1 - \nu$.

et en remplaçant ν par sa valeur, on obtient

$$\Pi_i = \frac{\theta + Q - 1}{\theta} (1 - Q - \theta K) \frac{qi}{Q}.$$

Dans l'annexe A, nous montrons qu'à l'équilibre symétrique, la quantité produite par chaque marchand est

$$q_B^c = \frac{2 - (1 + K)\theta}{2(n+1)} + \frac{\sqrt{A}}{2n(n+1)},$$

où l'indice "B" désigne le niveau de qualité bas et

$$A = \theta^2 n^2 (1 - K)^2 + 4(1 - \theta)(1 - \theta K).$$

La quantité totale produite est $Q_B^c = nq_B^c$ et chaque e-marchand obtient le profit d'équilibre

$$\Pi_B^c = \frac{\left(n\theta - 2(1-\theta) - n\theta K + \sqrt{A}\right)\left(2 + n\theta(1-K) - 2\theta K - \sqrt{A}\right)}{4n(n+1)^2\theta}.$$

Lemme 1 *La quantité échangée à l'équilibre, Q_B^c, décroît avec la proportion θ de consommateurs honnêtes.*

Preuve. La quantité échangée par chaque marchand, q_B^c, a le même sens de variation que la quantité totale, Q_B^c. On trouve que

$$\frac{\partial^2 q_B^c}{\partial \theta^2} = \frac{2(K-1)^2(n-1)}{nA^{3/2}}.$$

Comme $n \geq 2$, $\partial^2 q_B^c / \partial \theta^2$ est strictement positif pour tout θ, ce qui implique que $\partial q_B^c / \partial \theta$ est croissant en θ. Nous allons maintenant montrer que $\partial q_B^c / \partial \theta$ est négatif en $\theta = 1$, ce qui impliquera que $\partial q_B^c / \partial \theta$ est négatif pour toute valeur de θ. On trouve effectivement que

$$\left.\frac{\partial q_B^c}{\partial \theta}\right|_{\theta=1} = -\frac{1 + n^2 K}{n^2(n+1)}$$

est négatif. La quantité totale à l'équilibre, nq_B^c, décroît donc avec θ. ■

Lemme 2 *Le prix d'équilibre décroît avec la proportion θ de consommateurs honnêtes.*

Preuve. Le prix d'équilibre est

$$p_B^c = \frac{1}{\theta}(1 - Q_B^c) - K.$$

On trouve que

$$\frac{\partial p_B^c}{\partial \theta} = \frac{2 - \theta - \theta K - \sqrt{A}}{\theta^2 (n+1) \sqrt{A}}.$$

Comme le dénominateur est positif, il suffit de montrer que le numérateur est négatif. Comme $\theta \leq 1$ et $K \leq 1$, alors $2 - \theta - \theta K \geq 0$. On trouve que

$$(2 - \theta - \theta K)^2 - A = -\left(n^2 - 1\right)(1 - K)^2 \theta^2$$

est négatif, ce qui implique que $\partial p_B^c / \partial \theta < 0$. ■

Lorsque la proportion de consommateurs honnêtes (θ) augmente dans la population, deux effets interviennent. Tout d'abord, des consommateurs honnêtes se substituent à des consommateurs opportunistes, ce qui *diminue* la demande pour les biens vendus en ligne. En effet, tous les consommateurs opportunistes consomment, car ils ne paient pas pour les biens acquis en ligne, alors qu'une partie seulement des consommateurs honnêtes consomment, en fonction de leur disposition à payer et du prix du bien. Ensuite, le lemme 2 montre qu'un second effet intervient : lorsque la proportion de consommateurs honnêtes augmente, le prix du bien baisse, ce qui tend à *augmenter* la demande des consommateurs honnêtes. Le lemme 1 montre que le premier effet domine le second effet.

Lemme 3 *Lorsque le risque perçu par les consommateurs honnêtes (K) augmente, la quantité échangée diminue.*

Preuve. La quantité échangée à l'équilibre, nq_B^c, est la somme de deux termes décroissants en K. Par conséquent, nq_B^c décroît avec K. ■

Par rapport au lemme 1, un troisième effet intervient : lorsque le risque perçu par les consommateurs honnêtes (K) augmente, la quantité échangée diminue car la demande provenant des consommateurs honnêtes diminue elle aussi.

La proposition suivante est une conséquence des lemmes 1 et 3.

Proposition 1 *Si $K > c$, il existe $\widetilde{\theta}(K) \in]0,1[$ tel que la quantité échangée à l'équilibre sur le marché est plus forte avec un système de sécurité bas qu'avec un système de sécurité haut si $\theta \leq \widetilde{\theta}(K)$. Si $K \leq c$, la quantité échangée est toujours plus forte avec un système de sécurité bas qu'avec un système de sécurité haut.*

Preuve. Nous savons que q_B^c décroît avec θ ; nous en étudions les valeurs aux bornes $\theta = 0$ et $\theta = 1$. Quand θ tend vers zéro, q_B^c tend vers $1/n$. Comme on a toujours

$$\frac{1}{n} > \frac{1 - c}{n + 1},$$

alors $q_B^c(\theta) > q_H^c$ quand θ est proche de zéro. Quand θ tend vers 1, q_B^c tend vers

$$\frac{1 - K}{n + 1}.$$

On a $q_B^c(1) < q_H^c$ si et seulement si $K > c$. Si cette condition est vérifiée, comme q_B^c décroît avec θ, il existe $\widetilde{\theta}(K) \in]0,1[$ tel que $q_B^c(\theta) > q_H^c$ lorsque $\theta < \widetilde{\theta}(K)$ et $q_B^c(\theta) < q_H^c$ lorsque $\theta > \widetilde{\theta}(K)$. Si $K \leq c$, on a $q_B^c(\theta) \geq q_H^c$ pour tout θ. ■

La proposition 1 montre que les deux paramètres de la fraude - la proportion $1-\theta$ de consommateurs opportunistes et la perte espérée K des consommateurs honnêtes - ont deux effets opposés sur les quantités échangées sur le marché électronique. D'un côté, plus il y a de consommateurs opportunistes, plus les quantités échangées seront importantes. D'un autre côté, plus le risque encourru par les consommateurs honnêtes est élevé, plus les quantités échangées seront faibles.

Ce résultat suggère que le passage du système SSL sans intermédiaire ($K > 0$) au système SSL avec intermédiaire ($K \simeq 0$) permet le développement des échanges commerciaux sur Internet, car il réduit le niveau de la perte espérée K. Par contre, le passage du système SSL avec intermédiaire à un système de sécurité haute a un impact négatif sur les quantités échangées, même si cela correspond à une réduction de la fraude[9].

Jusqu'à maintenant, nous avons supposé que K ne dépendait pas de la proportion $1-\theta$ de consommateurs opportunistes. Nous pourrions aussi supposer que le risque de vol du numéro de carte bancaire est d'autant plus élevé qu'il y a une forte proportion de consommateurs opportunistes. Par exemple, si on suppose que $K(\theta) = 1-\theta$, on peut montrer que la quantité échangée à l'équilibre, Q_B^c, décroît puis croît avec la proportion θ de consommateurs honnêtes. Lorsque la proportion θ de consommateurs honnêtes est forte, le risque de vol du numéro de carte bleue est faible ; il augmente à mesure que la proportion de consommateurs honnêtes diminue. Lorsque les consommateurs sont majoritairement opportunistes, le risque de vol devient fort, mais il concerne peu de consommateurs ; l'impact sur la demande à l'équilibre est donc faible. Le résultat de la proposition 1 reste valide[10].

4.3 Niveau de sécurité à l'équilibre

Nous étudions maintenant le niveau de sécurité à l'équilibre. Comme le marché des systèmes de sécurité est concurrentiel, ce sont les *marchands* qui déterminent le niveau de sécurité des paiements par leur décision d'adoption : ils adoptent un système de qualité haute plutôt qu'un système de qualité basse si et seulement si

$$\Pi_H^c \geq \Pi_B^c. \tag{1}$$

Lorsque θ tend vers 0, Π_B^c tend également vers 0. Pour des valeurs suffisamment petites de θ, la relation (1) est donc toujours vérifiée. L'idée est que, si la

[9] Dans ce modèle, nous supposons qu'il n'y a pas d'entrée sur le marché du commerce électronique. Avec un processus d'entrée endogène, un niveau de sécurité haut pourrait stimuler l'entrée en augmentant les profits des e-marchands, ce qui aurait un effet positif sur les quantités échangées. L'effet global reste ambigü.

[10] On peut montrer qu'il existe $\widetilde{\theta}$ tel que la quantité échangée avec un niveau de sécurité bas est *supérieure* à la quantité échangée avec un niveau de sécurité haut quand $\theta < \widetilde{\theta}$ et *inférieure* quand $\theta > \widetilde{\theta}$.

fraude prend des proportions importantes (θ faible), le profit des e-marchands est fortement réduit sans la mise en place d'un niveau de sécurité élevé. Lorsque θ tend vers 1, Π_B^c tend vers $(1-K)^2/(n+1)^2$. Dans ce cas, la relation (1) est satisfaite si et seulement si $K > c$. Autrement dit, le niveau de sécurité haut est adopté si le coût direct pour les consommateurs honnêtes des achats en ligne avec un niveau de sécurité bas (K) est supérieur au coût de fourniture d'un niveau de sécurité haut (c).

Du fait de la complexité de l'expression de Π_B^c, il s'avère impossible de résoudre l'inégalité (1) dans un cas plus général. Nous recourons donc à des simulations. Lorsque n n'est pas trop grand, on observe que Π_B^c croît avec θ[11]. Dans ce cas, si $c < K$, les e-marchands adoptent toujours un système de sécurité haute. Si $c > K$, il existe une valeur seuil de θ, en deça de laquelle un système de sécurité haute est adoptée, alors qu'au delà de ce seuil, les e-marchands adoptent un système de sécurité basse. Cette situation est illustrée par la figure 1. Sur cette figure, nous avons posé $n = 8$, $K = 0,1$ et $c = 0,2$. Pour des valeurs de θ inférieures à 0,46, les e-marchands adoptent des systèmes de sécurité haute, et pour des valeurs de θ supérieures à 0,46, ils adoptent des systèmes de sécurité basse.

[FIGURE 1 A PEU PRES ICI]

5 Offre de sécurité monopolistique

Au cours de l'année 2000, un consortium des principales banques françaises a proposé et fait la promotion d'un système de sécurité haute, intitulé "Cyber-COMM" (cf. section 2). Pour étudier l'intérêt social de cette initiative, nous déterminons, dans cette section, l'équilibre sur le marché du commerce électronique lorsque l'offreur de sécurité est un monopole ou un consortium agissant comme un monopole. Nous reportons la comparaison d'une structure concurrentielle et d'une structure monopolistique pour la sécurité des paiements à la section suivante.

5.1 Niveau de sécurité haut

Le monopole de l'offre de sécurité choisit une taxe, t, sur les quantités produites de façon à maximiser son profit, en anticipant les décisions des e-marchands après fixation de la taxe. La détermination de l'équilibre sur le marché du commerce électronique est identique à celle de la section 4. Le profit d'un e-marchand i s'écrit $\Pi_i = (p_i - t)\, q_i$. A l'équilibre, la quantité offerte par chaque marchand est égale à

$$q_H^*(t) = \frac{1-t}{n+1}. \tag{2}$$

[11] Pour des valeurs de n suffisamment élevées, le profit Π_B^c croît puis décroît avec θ.

Le monopole maximise son profit, $\pi_H(t) = (t-c)\, nq_H^*(t)$, par rapport à t, sous contrainte que $\Pi_i \geq 0$. En écrivant la condition du premier ordre du programme de maximisation du monopole *sans contrainte*, on détermine l'expression de la taxe optimale, $t_H^m = (1+c)/2$. En introduisant t_H^m dans (2), on obtient la quantité d'équilibre

$$q_H^m = \frac{1-c}{2(n+1)}.$$

A l'équilibre, le profit par e-marchand est

$$\Pi_H^m = \frac{(1-c)^2}{4(n+1)^2},$$

la contrainte ($\Pi_i \geq 0$) est donc vérifiée. Le profit du monopole de la sécurité est

$$\pi_H^m = \frac{(1-c)^2 n}{4(n+1)}.$$

5.2 Niveau de sécurité bas

Supposons maintenant que le niveau de sécurité soit bas. Le e-marchand i maximise son profit

$$\Pi_i = \nu(p_i - t)\, q_i - (1-\nu)\, t q_i,$$

par rapport à q_i, en prenant le niveau de la taxe t comme donnée. Du fait de la taxe t, chaque marchand réalise maintenant une perte t pour chaque fraude[12]. En remplaçant ν et p_i par leur expression, le profit du marchand i peut s'écrire

$$\Pi_i = \frac{\theta(1+K) - (1-Q)^2 - \theta Q(1+t+K) - K\theta^2}{\theta Q} q_i.$$

La détermination de l'équilibre de Nash conduit à la quantité à l'équilibre

$$q_B^*(t) = \frac{(2-\theta-\theta t-\theta K)\, n + \sqrt{A'}}{2n(n+1)} \tag{3}$$

avec $A' = \theta^2 n^2 \left[(1+t)^2 + K(K-2+2t)\right] + 4(1-\theta) - 4\theta\left(n^2 t + K\right) + 4K\theta^2$.

L'offreur de sécurité maximise son profit, $\pi_B(t) = tnq_B^*(t)$, par rapport à t, sous contrainte que $\Pi_i \geq 0$. Nous commençons par déterminer l'optimum *sans contrainte*. La taxe optimale à l'optimum sans contrainte, t_B^{m*}, est

$$t_B^{m*} = \frac{4(1-\theta)(1-K\theta) + \theta^2 n^2 (1-K)^2}{2\theta n^2 (2-\theta-K\theta)}.$$

[12] En règle générale, l'intermédiaire bancaire ou non-bancaire ne garantit pas le marchand contre l'utilisation frauduleuse du numéro de carte bancaire par un internaute, en raison de l'absence d'authentification forte de l'internaute (Cf. supra). L'intermédiaire demande le remboursement au marchand du montant de la fraude. Un seul contre-exemple existe en France : dans le cadre de l'affaire SAMI Bureautique/Banque Populaire Toulouse Pyrénées jugée le 23 janvier 2003, la Cour d'appel de Toulouse s'est prononcée en faveur de SAMI Bureautique pour le non-remboursement des fraudes aux porteurs de carte bancaire

En injectant l'expression de t_B^{m*} dans (3), on obtient la quantité produite par chaque e-marchand à l'équilibre,

$$q_B^{m*} = \frac{2-\theta-K\theta}{2\left(n+1\right)},$$

et le profit par marchand à l'équilibre est égal à

$$\Pi_B^{m*} = \frac{\theta^2 n^2 \left(1-K\right)^2 - 4\left(2n+1\right)\left(1-\theta\right)\left(1-K\theta\right)}{4\theta n^2 \left(n+1\right)^2}.$$

Le lemme suivant détermine le domaine de validité de l'optimum sans contrainte.

Lemme 4 *Il existe* $\underline{\theta} \in]0,1[$ *tel que* $\Pi_B^{m*} \geq 0$ *si* $\theta \geq \underline{\theta}$ *et* $\Pi_B^{m*} < 0$ *si* $\theta < \underline{\theta}$.

Preuve. En effet, Π_B^{m*} est strictement négatif lorsque θ tend vers 0, strictement positif lorsque θ tend vers 1 et Π_B^{m*} croît avec θ puisque

$$\frac{\partial \Pi_B^{m*}}{\partial \theta} = \frac{\left(4+8n\right)\left(1-\theta^2 K\right) + \theta^2 n^2 \left(1-K\right)^2}{4\theta^2 n^2 \left(n+1\right)^2}$$

est positif. Il existe donc $\underline{\theta} \in]0,1[$ tel que $\Pi_B^{m*} \geq 0$ si $\theta \geq \underline{\theta}$ et $\Pi_B^{m*} < 0$ si $\theta < \underline{\theta}$. ■

Lorsque $\theta < \underline{\theta}$, le monopole fixe la taxe maximale $\widehat{t}$ telle que $\Pi_i \geq 0$, puisque $\pi_B\left(t\right)$ croît avec t. Comme Π_i décroît avec t, à l'optimum sous contrainte, on a $\Pi_i\left(\widehat{t}\right) = 0$. On trouve que

$$\widehat{t} = \frac{4-2\theta-2K\theta-4\sqrt{1-\theta-K\theta+K\theta^2}}{2\theta}.$$

Pour résumer, à l'équilibre, le profit par e-marchand est

$$\Pi_B^m = \begin{cases} \frac{\theta^2 n^2 (1-K)^2 - 4(2n+1)(1-\theta)(1-K\theta)}{4\theta n^2 (n+1)^2} & \text{si} \quad \theta > \underline{\theta} \\ 0 & \text{si} \quad \theta \leq \underline{\theta} \end{cases},$$

et le profit de l'offreur de sécurité en monopole est

$$\pi_B^m = \begin{cases} \frac{\theta^2 n^2 (1-K)^2 + 4(1-\theta)(1-\theta K)}{4n(n+1)\theta} & \text{si} \quad \theta > \underline{\theta} \\ \frac{2-\theta-K\theta-2\sqrt{(1-\theta)(1-K\theta)}}{\theta}\sqrt{\left(1-\theta\right)\left(1-K\theta\right)} & \text{si} \quad \theta \leq \underline{\theta} \end{cases}.$$

A l'image des lemmes 1, 2 et 3 établis dans la section 4, nous pouvons également analyser l'influence de la part des consommateurs honnêtes, θ, et du risque perçu par les consommateurs honnêtes, K, sur la quantité totale et le prix à l'équilibre. Les calculs effectués[13] montrent que dans le cadre d'une offre monopolistique de sécurité des paiements, les résultats des lemmes 1, 2 et 3 restent valides. Les mêmes effets économiques sont à l'oeuvre.

[13] Nous tenons à la disposition des lecteurs intéressés les preuves des calculs.

5.3 Niveau de sécurité à l'équilibre

Comme l'offre de sécurité est monopolistique, c'est l'*offreur de sécurité* qui choisit le niveau de sécurité des paiements. Il fournit un système de sécurité haute plutôt qu'un système de sécurité basse si et seulement si

$$\pi_H^m \geq \pi_B^m. \tag{4}$$

Lorsque θ tend vers 0, π_B^m tend également vers 0. Pour des valeurs suffisamment petites de θ, l'offreur de sécurité choisit donc un niveau de sécurité élevé, puisque la relation (4) est vérifiée. Lorsque θ tend vers 1, π_B^m tend vers $n\left(1-K\right)^2/4\left(n+1\right)$. Dans ce cas, la relation (4) est alors satisfaite si et seulement si $c < K$.

Comme dans la section 4, du fait de la complexité de l'expression de π_B^m, il s'avère impossible de résoudre l'inégalité (4) dans un contexte plus général. Des simulations numériques suggèrent que π_B^m croît avec θ. Dans ce cas, si $c < K$, l'offreur de sécurité adopte toujours un système de sécurité haute. Si $c > K$, il existe une valeur seuil de θ, en deça de laquelle l'offreur adopte un système de sécurité haute, alors qu'au delà de ce seuil, il adopte un système de sécurité basse.

[FIGURE 2 A PEU PRES ICI]

Cette situation est illustrée par la figure 2. Pour cette figure, nous avons retenu les mêmes valeurs de paramètres que pour la figure 1 ($n = 8$, $K = 0,1$ et $c = 0,2$). Pour ces valeurs des paramètres, on trouve que $\underline{\theta} = 0.65$ et que le monopole de la sécurité choisit un niveau de sécurité haut pour $\theta < 0,77$ et un niveau de sécurité bas pour $\theta > 0,77$. Si on compare la figure 1 à la figure 2, on observe que les choix de sécurité avec une offre concurrentielle et une offre monopolistique pour la sécurité des paiements sont identiques lorsque $\theta < 0,46$ (sécurité haute) ou $\theta > 0,77$ (sécurité basse). Lorsque $\theta \in [0,46; 0,77]$, un monopole sur la sécurité adopte un niveau de sécurité haut, tandis qu'une offre de sécurité concurrentielle conduit à un niveau de sécurité bas.

6 L'impact de la sécurité des paiements sur le volume du commerce électronique

Dans cette section, nous cherchons à déterminer si les incitations à commercialiser un système de sécurité haute sont plus fortes avec une structure monopolistique ou avec une structure concurrentielle et s'il serait socialement souhaitable de conférer un monopole sur la sécurisation des paiements. Une réponse positive pourrait justifier un soutien des pouvoirs publics à un consortium de banques proposant un système de paiement de sécurité haute.

Nous comparons une offre concurrentielle et une offre monopolistique de la sécurité suivant trois critères : le niveau de sécurité des paiements, les volumes échangés à l'équilibre sur le marché du commerce électronique et, enfin, le bien-être social.

6.1 Niveaux de sécurité

Nous commençons par comparer le choix de sécurité des paiements, suivant que les systèmes de sécurité sont fournis sur un marché concurrentiel ou par un offreur en monopole. Les incitations à adopter un niveau de sécurité haute sont égales à $\pi_H^m - \pi_B^m$ dans le cas d'une offre monopolistique et à $\Pi_H^c - \Pi_B^c$ dans le cas d'une offre concurrentielle. Des systèmes de sécurité haute sont adoptés si ces incitations sont positives, des systèmes de sécurité basse sont adoptés dans le cas contraire.

Lemme 5 *Si $\theta = 1$, le choix du niveau de sécurité est identique que l'offre de sécurité soit monopolistique ou concurrentielle.*

Preuve. En effet, en posant $\theta = 1$, on trouve que

$$\pi_B^m = \frac{n\,(n+1)}{4}\Pi_B^c,$$

et que

$$\pi_H^m = \frac{n\,(n+1)}{4}\Pi_H^c,$$

ce qui implique que la condition (1) est équivalente à la condition (4). ■

Par conséquent, les incitations à adopter un système de sécurité haute ne sont différentes dans un contexte de concurrence et de monopole sur l'offre de sécurité que lorsqu'il existe des consommateurs opportunistes, c'est-à-dire lorsque $\theta < 1$.

Lemme 6 *Pour des valeurs de θ proches de 1 mais différentes de 1 :*

- *Si $n \in \{2, 3\}$, les incitations à adopter un système de sécurité haute sont plus fortes avec une offre de sécurité concurrentielle qu'avec une offre monopolistique.*
- *Si $n \geq 4$, les incitations à adopter un système de sécurité haute sont plus fortes avec une offre de sécurité monopolistique qu'avec une offre concurrentielle.*

Preuve. Comme

$$\pi_H^m = \frac{n\,(n+1)}{4}\Pi_H^c,$$

la condition (4) est équivalente à $\Pi_H^c \geq 4\pi_B^m / \left(n^2 + n\right)$. Posons

$$H = \Pi_B^c - \frac{4}{n\,(n+1)}\pi_B^m.$$

Si $H > 0$, la condition (4) peut être vérifiée sans que la condition (1) le soit. Ceci signifie qu'il existe des cas où un monopole de la sécurité choisit la sécurité haute alors qu'avec un marché concurrentiel de la sécurité conduit à l'adoption de systèmes de sécurité basse. Si $H < 0$, le cas inverse se présente : il existe des

cas où la sécurité est basse avec une offre de sécurité monopolistique et haute avec une offre de sécurité concurrentielle.

Nous allons montrer que pour des valeurs de θ proches de 1, $H < 0$ si $n \in \{2, 3\}$ et $H > 0$ si $n \geq 4$. Comme nous étudions des valeurs proches de 1, nous restreignons l'analyse aux valeurs de θ telles que $\theta > \underline{\theta}$. En remplaçant Π_B^c et π_B^m par leurs valeurs, on trouve que $H(1) = 0$ et que

$$\left.\frac{\partial H}{\partial \theta}\right|_{\theta=1} = \frac{-(n-3)(1-K)}{n^2(n+1)}.$$

Lorsque $n = 2$, cette dérivée est strictement positive, ce qui implique que $H < 0$ pour des valeurs de θ proches de 1. Lorsque $n \geq 4$, cette dérivée est strictement négative, ce qui prouve que $H > 0$ pour des valeurs de θ proches de 1 mais strictement inférieures à 1.

Enfin, pour $n = 3$, la dérivée première est nulle. Nous calculons donc la dérivée seconde de H par rapport à θ en $\theta = 1$. Il s'agit d'une fonction qui ne dépend que de K. Une simulation montre que la dérivée seconde en $\theta = 1$ est strictement négative, quel que soit K. Par conséquent, lorsque $n = 3$, nous avons $H < 0$ pour des valeurs de θ proches de 1. ■

Le second point de ce lemme est illustré par les figures 1 et 2. Le premier point du lemme peut être observé en posant $n = 2$ pour ces mêmes figures. On observe alors que pour $\theta \in [0,54; 0,74]$, une offre concurrentielle de la sécurité conduit à un niveau de sécurité haute, tandis qu'une offre de sécurité en monopole conduit à un niveau de sécurité basse.

Dans la suite de l'article, nous nous plaçons dans le cas de figure où la sécurité des paiements peut être plus élevée avec un monopole sur l'offre de sécurité qu'avec une concurrence entre offreurs de sécurité. Nous cherchons alors à déterminer si un monopole sur l'offre de sécurité peut être socialement souhaitable.

6.2 Volumes du commerce électronique

En termes d'échanges sur le marché du commerce électronique, à niveau de sécurité constant, une concurrence sur l'offre de sécurité des paiements est a priori toujours préférable à un monopole. En effet, la taxe du monopole va réduire les quantités échangées. Cette intuition est confirmée par le lemme suivant.

Lemme 7 *A niveau de sécurité égal, la quantité échangée à l'équilibre est plus faible si l'offre de sécurité est monopolistique que si elle est concurrentielle.*

Preuve. Considérons d'abord que le niveau de sécurité est haut, quelle que soit la structure de marché de l'offre de sécurité des paiements (monopolistique ou concurrentielle). On remarque que $q_H^m = q_H^c/2$; on a donc $Q_H^m < Q_H^c$.

Supposons maintenant que le niveau de sécurité est bas pour les deux structures de marché. Comme $\partial^2 \Pi_i / \partial q_i \partial t < 0$, il s'ensuit que $q_B^*(t)$ décroît avec t. Par conséquent, nous avons $q_B^c > q_B^m$, puisque $q_B^c = q_B^*(0)$, $q_B^m = q_B^*(t_B^m)$ et $t_B^m > 0$. On en conclut que $Q_B^c > Q_B^m$. ■

Un monopole sur la sécurité des paiements ne peut donc avoir un effet bénéfique sur les volumes du commerce électronique que dans le cas où le niveau de sécurité est haut en monopole et bas en concurrence. Nous nous plaçons maintenant dans cette situation.

Trois effets interviennent. Tout d'abord, comme la fraude est impossible avec un niveau de sécurité haut, les quantités échangées ont tendance à être plus faibles qu'avec un niveau de sécurité bas. Ensuite, comme le risque de vol du numéro de carte bancaire disparaît si la sécurité est haute, les quantités échangées ont tendance à augmenter. Enfin, la taxe fixée par le monopole de la sécurité réduit les quantités à l'équilibre.

Lemme 8 *Supposons que le niveau de sécurité soit haut en monopole et bas en concurrence. Si* $K \leq (1+c)/2$*, la quantité échangée à l'équilibre est plus forte si l'offre de sécurité est concurrentielle que si elle est monopolistique.*

Preuve. D'après le lemme 1, $q_B^c(\theta)$ décroît avec θ. Comparons $q_B^c(1)$ à q_H^m. On trouve que

$$q_B^c(1) = \frac{1-K}{n+1},$$

tandis que

$$q_H^m = \frac{1-c}{2(n+1)}.$$

En comparant $q_B^c(1)$ et q_H^m, nous trouvons que $q_B^c(1) \geq q_H^m$ si et seulement si $K \leq (1+c)/2$. Si cette condition est vérifiée, alors $q_B^c(\theta) \geq q_H^m$ est vraie pour tout θ, car $q_B^c(\theta)$ décroît avec θ. Il s'ensuit que $Q_B^c(\theta) \geq Q_H^m$. ■

Le lemme 8 montre que, même si le niveau de sécurité est plus élevé avec un monopole sur la sécurité, une concurrence entre offreurs de sécurité est toujours préférable pour stimuler le développement du commerce électronique.

Dans le lemme, nous supposons que $K \leq (1+c)/2$. Lorsque $K > (1+c)/2$, il est possible que, pour des valeurs suffisamment élevées de θ, les quantités échangées soient plus fortes avec une offre monopolistique de la sécurité qu'avec une offre concurrentielle. Cependant, ceci n'est valable que si l'offreur en monopole choisit un niveau de sécurité haut tandis qu'une offre concurrentielle conduit à un niveau de sécurité bas. Or, la condition $K > (1+c)/2$ implique que $K > c$. Dans les sections 1 et 4, nous avons vu que dans ce cas ($K > c$), une offre concurrentielle et une offre monopolistique de la sécurité conduisaient toutes deux au niveau de sécurité haut[14].

6.3 Bien-être collectif

Le bien-être collectif est défini comme la somme des profits des e-marchands, des offreurs de sécurité et du surplus des consommateurs. Notons $\sigma \in \{c, m\}$

[14] Rappelons que ce "résultat" repose sur des simulations.

la structure de marché de l'offre de sécurité. Lorsque le niveau de sécurité est haut, le bien-être collectif est égal à

$$W_H^\sigma = n\Pi_H^\sigma + \int_{p_H^\sigma}^1 (\tau - p)\, d\tau + \pi_H^\sigma.$$

Lorsque le niveau de sécurité est bas, le bien-être collectif est

$$W_B^\sigma = n\Pi_B^\sigma + \theta \int_{p_B^\sigma + K}^1 (\tau - p - K)\, d\tau + (1-\theta) \int_0^1 \tau d\tau + \pi_B^\sigma.$$

Du fait de la complexité des expressions, il est difficile de réaliser un étude de bien-être dans un cas général. Nous procédons donc à une étude analytique dans le cas où $\theta = 1$, ce qui correspond à la réalité observée (un taux de fraudeurs relativement faible) et nous recourons à des simulations pour une généralisation.

A niveau de sécurité identique, une offre concurrentielle sur la sécurité des paiements est a priori préférable socialement à une offre monopolistique. Ceci peut être démontré dans le cas où θ est proche de 1. Dans ce cas, on trouve que

$$W_H^c = \frac{n\,(n+2)\,(1-c)^2}{2\,(n+1)^2},$$

et que

$$W_H^m = \frac{n\,(3n+4)\,(1-c)^2}{8\,(n+1)^2}.$$

En comparant W_H^m et W_H^c, on trouve que $W_H^c > W_H^m$ si et seulement si $8+4n > 4+3n$, condition qui est toujours vérifiée. En comparant de la même manière W_B^m et W_B^c, on trouve que, lorsque θ tend vers 1, $W_B^c - W_B^m$ tend vers

$$\frac{n\,(n+4)}{(n+1)^2}\frac{(1-K)^2}{8},$$

qui est une expression strictement positive. Par conséquent, on a $W_B^c > W_B^m$ quand θ est proche de 1.

Lorsque le niveau de sécurité des paiements est haut avec une offre de sécurité en monopole et bas avec une offre de sécurité concurrentielle, ce résultat reste-t-il valable ? La figure 3 propose une simulation de ce cas de figure pour les mêmes valeurs de paramètres que nous avions retenues pour les figures 1 et 2 ($n = 8$, $K = 0,1$ et $c = 0,2$).

[FIGURE 3 A PEU PRES ICI]

La figure montre que $W_B^c > W_H^c$ pour tout θ. Comme nous savons de surcroît que $W_H^c > W_H^m$, ceci implique que $W_B^c > W_H^m$ pour tout θ. Par conséquent, une offre de sécurité concurrentielle est préférable socialement à une offre de sécurité monopolistique, même si l'offreur de sécurité en monopole offre un niveau de sécurité plus élevé que les offreurs en concurrence. En fait, dans ce cas, le monopole sur la sécurité introduit deux types de distorsion : une distorsion sur les quantités, mais aussi une distorsion sur le niveau de sécurité choisi (haut alors qu'il serait souhaitable qu'il soit bas).

7 Extensions

Dans cette section, nous analysons deux extensions possibles de notre modèle. Tout d'abord, nous montrons que l'introduction d'un coût marginal de production strictement positif ne modifie pas les résultats du modèle. Ensuite, nous discutons le cas d'une atomisation des e-marchands ($n \to \infty$).

7.1 Coût marginal de production

Dans notre modèle, nous avons supposé que le coût marginal de production était nul. Cette hypothèse, qui nous permet de simplifier les expressions, a une incidence particulière : lorsque le niveau de sécurité est bas, les e-marchands réalisent une marge nulle avec les consommateurs fraudeurs. Ainsi, même si la fraude est très importante (pour des petites valeurs de θ), les e-marchands restent viables, c'est-à-dire que $\Pi_i \geq 0$.

On peut montrer que l'introduction d'un coût marginal de production, r, strictement positif ne modifient pas nos résultats[15]. L'introduction d'un coût marginal de production a plusieurs effets. Tout d'abord, bien évidemment, à l'équilibre, les quantités produites et les profits diminuent avec le niveau de ce coût marginal. Par ailleurs, lorsque le niveau de sécurité est bas et que la proportion de consommateurs opportunistes est élevée (θ proche de zéro), les e-marchands réalisent des pertes s'ils entrent sur le marché du commerce électronique. Comme, dans ce cas, ils préfèrent ne pas produire, ceci montre que le marché du commerce électronique n'existe pas lorsque θ est faible et que le niveau de sécurité est bas.

Logiquement, les incitations à adopter des systèmes de sécurité haute augmentent avec le coût marginal de production, que l'offre de sécurité soit concurrentielle ou monopolistique. On peut enfin montrer par simulation que l'ordre des valeurs du bien-être social en fonction des deux structures du marché de la sécurité (concurrence ou monopole) et du niveau de sécurité (bas ou haut) reste inchangé quand r augmente. En d'autres termes, l'analyse de bien-être de la section 6 reste valide.

7.2 Atomisation des e-marchands

Dans le cas d'une atomisation concurrentielle des e-marchands ($n \to \infty$), nos résultats restent également valables. Dans ce cas de figure, on peut montrer qu'un offreur de sécurité en monopole choisit le niveau de sécurité haute plutôt que le niveau de sécurité basse si et seulement si

$$1 - c > \theta\,(1 - K)\,. \tag{5}$$

Pour le cas d'une offre de sécurité concurrentielle, la condition d'adoption de sécurité haute devient

$$1 - c > \sqrt{(1 - K)\,(1 - \theta K)}. \tag{6}$$

[15] Une démonstration formelle de la discussion qui suit est fournie dans une note annexe, disponible à l'adresse Internet suivante : http ://www.enst.fr/egsh/bourreau/note_seccom.pdf.

Dans les deux cas, on peut remarquer qu'une augmentation des consommateurs fraudeurs (c'est-à-dire une baisse de θ) ou une augmentation du coût du vol du numéro de carte bleue (c'est-à-dire une augmentation de K) favorisent l'adoption de systèmes de sécurité haute. Par ailleurs, comme la partie droite de la condition (6) est supérieure à la partie droite de la condition (5), les incitations à adopter un système de sécurité haute sont toujours plus fortes avec un monopole sur la sécurité qu'avec une concurrence entre offreurs de sécurité.

8 Conclusion

Dans cet article, nous avons étudié l'impact de la sécurité des paiements sur le développement du commerce électronique.

Notre analyse montre que la fraude sur Internet a deux dimensions. D'une part, si la présence de consommateurs fraudeurs a un impact négatif sur les profits des marchands en ligne, elle n'a pas en tant que telle d'impact négatif sur les quantités échangées sur le marché électronique. D'autre part, le risque de vol du numéro de carte bancaire perçu par les consommateurs honnêtes a un effet négatif direct sur les quantités échangées. Toute initiative juridique qui tend à protéger les consommateurs honnêtes du coût de la fraude, ainsi que le garantit la récente Loi sur la Sécurité Quotidienne, concourt alors à promouvoir le développement du e-commerce. De la même manière, le passage d'un système SSL sans intermédiaire à un système SSL avec intermédiaire a un effet positif, parce que le risque de vol du numéro de carte bancaire est réduit. Ce n'est pas nécessairement le cas si l'on passe d'un système SSL avec intermédiaire à un système de sécurisation avec signature électronique.

Nous avons aussi étudié l'impact de la structure de marché de l'offre de sécurité des paiements sur le marché du commerce électronique. Pour cela, nous avons comparé une structure concurrentielle à une structure monopolistique. Les incitations à l'adoption d'un système de sécurité haute (sécurisation avec signature électronique) sont plus fortes lorsque l'offre de sécurité est monopolistique que lorsqu'elle est concurrentielle si le nombre de e-marchands est suffisamment élevé. Cependant, du fait du caractère distorsif du monopole sur le marché du commerce électronique, la quantité échangée à l'équilibre est toujours plus faible si l'offre de sécurité est monopolistique. De même, nous avons montré que le bien-être collectif était toujours supérieur avec une concurrence entre offreurs de sécurité. Un monopole sur la sécurisation des paiements n'est donc pas socialement souhaitable.

La question du bien-fondé d'une concurrence entre systèmes de paiement ne se pose pas seulement dans le cas d'Internet. Par exemple, cette question se pose aussi dans le cadre des réseaux de téléphonie mobile de 2ème et 3ème génération. Les opérateurs de télécommunications peuvent-ils être autorisés à développer leur propre système de paiement par facture et s'imposer en tant qu'intermédiaire dans les paiements (Randoux [2003]) ? De même, le développement du micropaiement dans le commerce traditionnel ou sur Internet pose la question de son émission par les acteurs des réseaux de transport, les four-

nisseurs d'accès Internet, etc. Dès lors, après un renouveau des travaux centrés sur la privatisation de l'offre de monnaie de premier rang (Figuet et Kaufman [1998]) et la déréglementation de l'offre de monnaie de second rang (Scialom [1995]), l'intégration des technologies de l'information et de la communication dans les systèmes de paiement de détail pose la question cruciale de la légitimité du monopole bancaire dans la gestion des instruments de paiement.

Références

[1] CyberSource [2002], *Online Fraud Report : Online Credit Card Fraud Trends and Merchant's Response.*

[2] Experian [2001], *Internet fraud : a growing threat to online retailers*, Experian White Paper.

[3] Figuet J.M. et Kaufman P.,[1998], "Systèmes interbancaires de paiements, effets de réseau et fonctionnement des économies monétaires", *Revue d'Économie Politique*, 108, 3, Mai-Juin.

[4] INSEE Première [2001], "Le commerce de détail s'initie à la vente sur Internet", 771, avril.

[5] PaymentOne [2003], *Online Payments Strategies and Preferences Poll 2003.*

[6] Picard, P. [1996], "Auditing claims in the insurance market with fraud : the credibility issue", *Journal of Public Economics*, 63, 27-56.

[7] Rapport d'information de l'assemblée nationale [2001], *Renforcer la sécurisation du commerce électronique*, n° 3229.

[8] Randoux Y. [2003], "L'Europe des paiements scripturaux numériques", *Cahiers du Numérique*, Vol. 4, N°1, 17-44.

[9] Scialom L. [1995], "Les modèles de paiement concurrentiels : Eléments d'analyse critique", *Revue Economique*, vol.46, n°1, Janvier, pp 35-55

A Annexe

Le marchand en ligne i maximise

$$\Pi_i = \frac{\theta + Q - 1}{\theta} (1 - Q - \theta K) \frac{qi}{Q}$$

par rapport à q_i. On écrit la condition du premier ordre de maximisation de Π_i par rapport à q_i. On obtient que $\partial \Pi_i / \partial q_i = 0$ si et seulement si

$$\left(1 - \theta - \theta K - Q^2 + \theta^2 K\right) q_i - Q (1 - Q - \theta) (1 - Q - \theta K) = 0.$$

Comme nous cherchons l'équilibre symétrique du jeu, on pose $q_i = q$ et $Q = nq$. La condition du premier ordre s'écrit alors, après division par q,

$$\left(1 - \theta - \theta K - n^2 q^2 + \theta^2 K\right) - n (1 - nq - \theta) (1 - nq - \theta K) = 0.$$

Cette équation du second degré en q a deux racines. Dans la mesure où le coefficient du terme en q^2 est négatif et que nous cherchons le maximum de la fonction Π_i, la solution de notre problème de maximisation est la plus grande des deux racines, soit

$$q_B^c = \frac{2-(1+K)\,\theta}{2\,(n+1)} + \frac{\sqrt{\theta^2 n^2\,(1-K)^2 + 4\,(1-\theta)\,(1-\theta K)}}{2n\,(n+1)}.$$

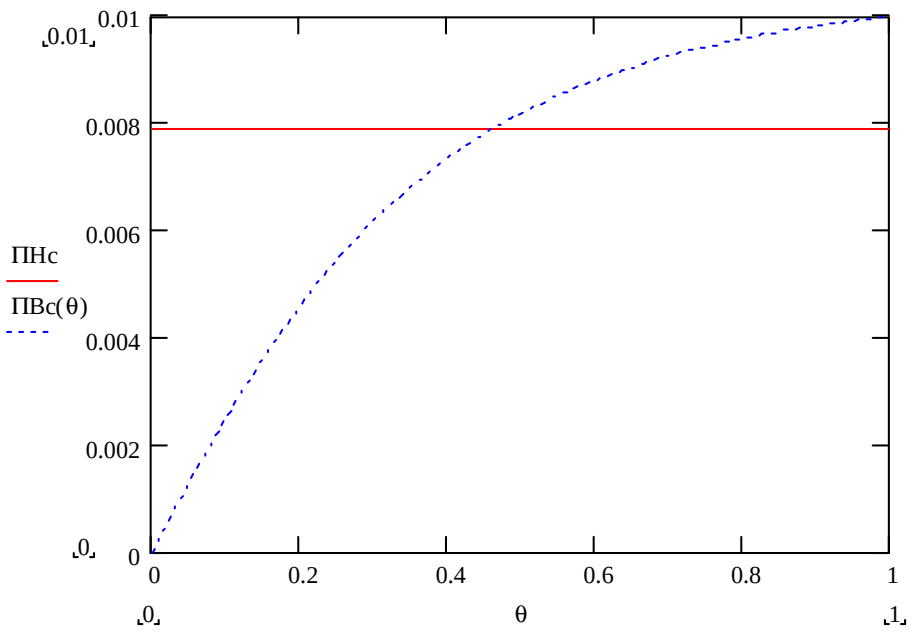

FIG. 1 – Choix de sécurité avec une offre de sécurité concurrentielle

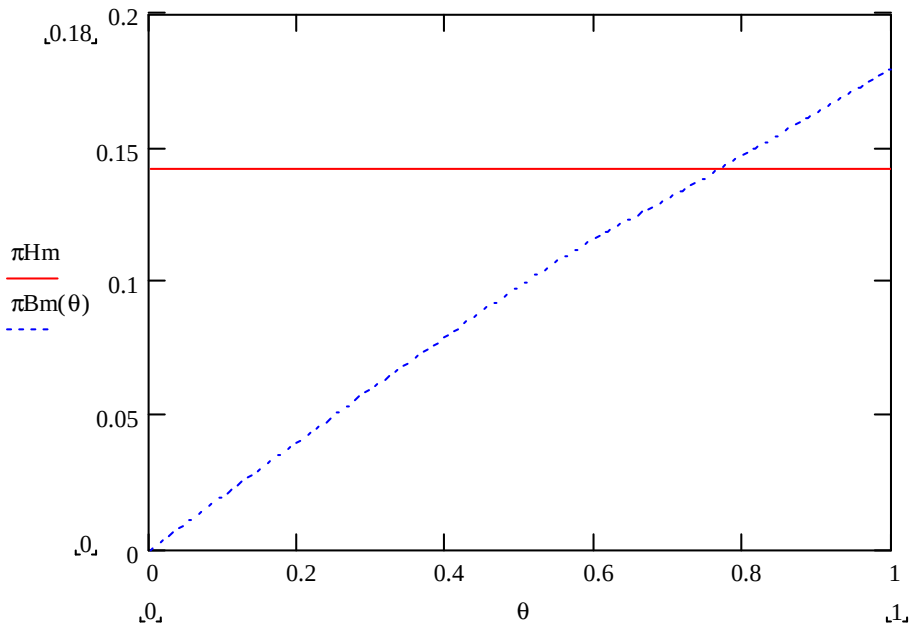

FIG. 2 – Choix de sécurité avec une offre de sécurité monopolistique

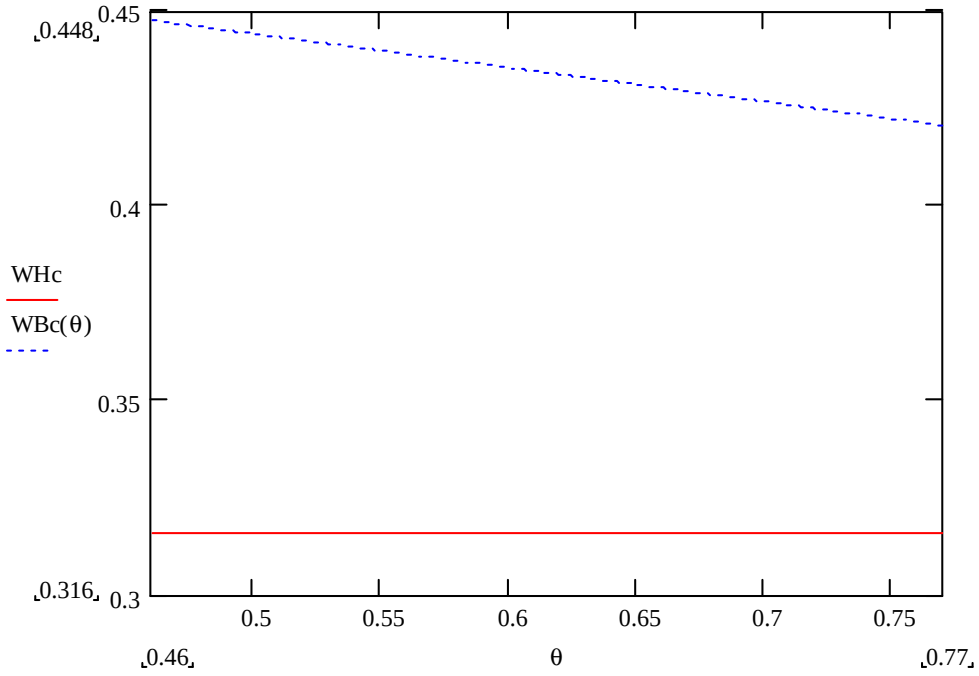

FIG. 3 – Bien-être avec offre de sécurité concurrentielle et niveau de sécurité bas ou haut