LES COMPORTEMENTS DE VIE PRIVÉE FACE AU COMMERCE ÉLECTRONIQUE

Une économie de la gratification immédiate

Alessandro Acquisti, Michèle Francine MBo'o Ida et Fabrice Rochelandet

La Découverte | « Réseaux »

2011/3 n° 167 | pages 105 à 130

ISSN 0751-7971
ISBN 9782707169020

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-reseaux-2011-3-page-105.htm

LES COMPORTEMENTS DE VIE PRIVÉE FACE AU COMMERCE ÉLECTRONIQUE

Une économie de la gratification immédiate

Alessandro ACQUISTI

Traduction en français :
Michèle Francine MBo'o Ida et Fabrice Rochelandet

DOI: 10.3917/res.167.0105

La protection de la vie privée reste une question fondamentale en matière de commerce électronique[1]. En 2000, une étude de PriceWaterhouse-Coopers révélait qu'environ deux tiers des consommateurs interrogés « *achèteraient plus en ligne s'ils étaient certains que les sites commerciaux n'utilisent pas leurs informations personnelles à d'autres fins* » (ebusinessforum.com, 2000). Une étude de la Federal Trade Commission rapportait en 2000 que 67 % des consommateurs étaient « très inquiets » quant à la préservation des données personnelles transmises en ligne (FTC, 2000). Une enquête de CBS News en 2005 indiquait que la majorité des Américains considéraient que leur vie privée était « sérieusement menacée ». Plus récemment, une enquête de Turow (2009) a révélé qu'une grande majorité d'Américains sont réfractaires à la publicité ciblée en raison de ses conséquences sur la vie privée.

Toutefois, les études dans ce domaine de recherche ainsi que les expériences et les données empiriques montrent des résultats très différents. Spiekermann et al. (2002), Chellappa et Sin (2002), Harn et al. (2002), Jupiter Research (2002) ont démontré que même les individus soucieux de leur intimité sont disposés à révéler des détails d'ordre privé par commodité ou à négocier la divulgation d'informations très personnelles en échange de récompenses relativement faibles. L'échec de plusieurs services en ligne visant à préserver l'anonymat des utilisateurs d'Internet (Brunk, 2002) apporte de façon indirecte une preuve supplémentaire de la réticence de la plupart des individus à faire des efforts pour protéger leurs informations personnelles.

La dichotomie entre les attitudes en matière de vie privée et le comportement effectif a été largement analysée dans la littérature. Diverses interprétations de ce phénomène ont été proposées (Acquisti et Grossklags, 2003 ; Syverson, 2003 ; Shostack, 2003 ; Vila et al., 2003). Dans cet article, nous analysons principalement le processus décisionnel des individus en considérant la

1. Une version précédente de cet article a été publiée sous le titre « Privacy in Electronic Commerce and the Economics of Immediate Gratification », Alessandro Acquisti. Actes de l'ACM Electronic Commerce Conference (ACM EC), ACM, 21-29, 2004. Voir Acquisti (2004).

problématique de la vie privée et les éventuelles insuffisances de ce processus. Nous nous focalisons sur les (mauvaises) interprétations des individus concernant la manière de gérer les risques encourus lorsque des informations personnelles sont révélées. Nous n'abordons pas la question de savoir si les gens doivent effectivement se protéger. Nous ferons quelques observations à propos de cette question dans la section 5 où nous discuterons également des stratégies permettant une validation empirique de notre théorie.

Nous appliquons les résultats de l'économie comportementale. Dans l'approche économique traditionnelle, l'hypothèse de base est que les gens sont prévoyants et font des choix bayésiens : ils prennent en compte la façon dont leur comportement actuel peut affecter leur bien-être futur et leurs préférences. Par exemple, Becker et Murphy (1988) étudient les modèles d'addiction rationnelle. Cette approche peut être comparée à celles qui voient dans la décision de ne pas protéger sa vie privée, un choix rationnel étant donné les (supposés) faibles niveaux de risque qui sont en jeu. Pourtant, les travaux dans le champ de l'économie comportementale ont mis en évidence différentes formes d'incohérences psychologiques (problèmes d'autocontrôle, actualisation hyperbolique, biais pour le présent, etc.) qui sont en contradiction avec l'approche rationnelle de l'agent économique. Dans cet article, nous nous appuyons sur ces travaux pour aboutir aux conclusions suivantes :

Nous montrons qu'il est peu probable que les individus puissent agir de façon rationnelle au sens économique lorsqu'ils doivent prendre des décisions sensibles en matière de vie privée.

Nous montrons que les modèles alternatifs du comportement personnel et d'incohérences temporelles des préférences sont en adéquation avec la dichotomie entre les attitudes et le comportement et peuvent, de ce fait, mieux s'appliquer aux données actuelles. Par exemple, ces modèles peuvent expliquer les résultats présentés dans Spiekermann et al. (2001). Leur expérimentation montre que les individus qui affichent une préférence pour la préservation de la vie privée sont également ceux qui sont disposés à révéler des quantités variables d'informations personnelles moyennant de petites récompenses.

En particulier, nous montrons que les individus auraient tendance à se protéger insuffisamment contre les risques d'atteinte à leur vie privée et à divulguer une quantité excessive d'informations personnelles même lorsqu'ils seraient méfiants vis-à-vis des risques encourus.

Nous montrons que sous certaines conditions, l'ampleur des coûts perçus en matière de vie privée ne sera pas un facteur dissuasif à l'égard de comportements que l'individu admet pourtant comme étant risqués.

Nous montrons en référence aux travaux similaires en économie de la gratification immédiate (Rabin et O'Donoghue, 2000), que même les individus considérés comme « avertis » peuvent, sous certaines conditions, devenir « myopes » concernant leur vie privée.

Nous concluons que le fait d'apporter plus d'informations et de sensibiliser davantage les gens dans un environnement autorégulé ne suffit pas à protéger la vie privée des individus. De meilleures technologies assorties d'une diminution des coûts d'adoption et de protection seraient certainement plus utiles. Toutefois, des réponses plus fondamentales en matière de comportement humain doivent également être considérées dans la mesure où la vie privée doit être protégée.

Dans la section suivante, nous proposons un modèle d'agents rationnels devant prendre des décisions sensibles en matière de vie privée. Dans la section 3, nous montrons les difficultés que comporte un modèle de processus décisionnel basé sur la rationalité complète. Dans la section 4, nous montrons de quelles manières les modèles comportementaux basés sur le biais de gratification immédiate peuvent mieux expliquer le contraste attitudes-comportement et être appliqués aux données disponibles. Dans la section 5, nous résumons nos arguments et discutons nos conclusions.

UN MODÈLE DE RATIONALITÉ DANS LA DÉCISION DE PRÉSERVATION DE LA VIE PRIVÉE

Certains travaux se sont basés sur la dichotomie entre les attitudes et les comportements de vie privée pour conclure que les individus agissent rationnellement quand il est question de vie privée. Selon ce point de vue, les individus accepteraient de petites récompenses en échange d'informations personnelles car ils anticiperaient des préjudices futurs minimes (lorsqu'ils sont actualisés avec le temps et selon leur probabilité d'apparition). Dans cette partie, nous recherchons les hypothèses qui sous-tendent l'idée que le comportement personnel s'appuierait sur une rationalité parfaite s'agissant des décisions en matière de vie privée.

Depuis Posner (1978, 1981) et Stigler (1980), les économistes se sont intéressés à la question de la vie privée, mais ce n'est que récemment que des modèles formalisés ont été développés (Acquisti et Varian, 2005 ; Calzolari et Pavan, 2004 ; Taylor, 2002 ; Vila et al., 2003). Alors que ces travaux se concentrent sur l'analyse des interactions sur le marché entre un agent et d'autres parties prenantes, nous nous intéressons ici à la modélisation du processus décisionnel d'un seul individu. Nous cherchons à savoir si les individus peuvent être rationnels au sens économique (s'ils sont prévoyants, font des choix bayésiens, maximisent leur utilité, etc.) lorsqu'il s'agit de protéger leurs informations personnelles.

Le concept de la vie privée, défini comme un droit à être laissé tranquille (Warren et Brandeis, 1890), a évolué avec le rôle prépondérant de l'information dans notre société. Dans une société de l'information, le soi est exprimé, défini et influencé à travers et par l'information et les technologies de l'information. Les frontières entre les sphères privée et publique s'estompent. La vie privée est donc devenue plus une *suite* d'intérêts à multiples facettes qu'un concept unique et sans ambiguïté. D'où l'intérêt de discuter de sa valeur (si elle n'est pas établie) une fois que le contexte d'analyse a été clairement spécifié. Cela nécessite souvent l'étude d'un réseau de relations entre un sujet, des informations données (relatives au sujet), d'autres aspects (qui pourraient avoir plusieurs liens intéressants ou être en associés à ces informations ou à ce sujet) et le contexte dans lequel de telles relations peuvent avoir lieu.

Pour comprendre comment un agent rationnel pourrait gérer ces relations complexes, nous modélisons dans l'équation 1 le processus décisionnel de l'agent économique rationnel qui doit faire des arbitrages en matière de vie privée lorsqu'il effectue une certaine transaction.

$$\max_{d} U_t = \delta(v_E(a), p^d(a)) + \gamma(v_E(t), p^d(t)) - c_t^d \qquad (1)$$

Dans l'équation 1, δ et γ sont des formes fonctionnelles non spécifiées qui décrivent les relations pondérées entre les bénéfices espérés d'une série d'événements *v* et les probabilités d'apparition de ces événements *p*. Plus précisément, l'utilité *U* de la réalisation d'une transaction *t* (la transaction étant toute action – pas nécessairement une opération monétaire – qui implique *éventuellement* la révélation d'informations personnelles) est égale à une fonction du bénéfice *espéré* $v_E(a)$ de la préservation (ou non) de certaines informations privées pendant cette transaction, et la probabilité de maintenir [ou de ne pas maintenir] cette

information privée lorsqu'on utilise la technologie *d*, $p^d(a)\,[1-p^d(a)]$; plus une fonction du bénéfice *espéré* $v_E(t)$ de la réalisation (ou non) de la transaction (en révélant probablement une information personnelle), et la probabilité de finaliser [ou de ne pas finaliser] la transaction avec une technologie donnée *d*, $p^d(t)\,[1-p^d(t)]$; moins le coût de l'utilisation de la technologie *t*, c_t^d.[2]

La technologie *d* peut faciliter ou non la protection de la vie privée. L'équation 1 intègre la dualité implicite dans les questions relatives à la vie privée dans la mesure où les résultats dans l'équation 1 peuvent être positifs ou négatifs : il s'agit à la fois des coûts et des bénéfices obtenus suite à la révélation ou à la protection des informations personnelles ; et les coûts et les bénéfices de la finalisation d'une transaction, $v_E(t)$, devraient être distingués des coûts et bénéfices de la protection d'une *information* privée, $v_E(a)$. Par exemple, il est possible d'avoir une réduction dans une librairie en ligne en révélant son identité. Inversement, ceci peut aussi impliquer d'avoir une facture importante à cause de la discrimination par les prix. Protéger sa vie privée financière en évitant de divulguer les informations de sa carte de crédit en ligne peut être une protection contre des pertes futures et des ennuis relatifs au vol de son identité. Cependant, cela peut rendre plus gênantes ses opérations d'achats en ligne et donc plus coûteuses.

Les paramètres fonctionnels δ et γ incluent le poids des variables et les attitudes qu'un individu peut avoir lorsqu'il décide de préserver ses données privées (par exemple, son rapport à sa vie personnelle ou le fait de penser que la vie privée est un droit dont le respect doit être garanti par l'autorité publique) et d'effectuer certaines transactions. Notons que v_E et *p* peuvent se rapporter à des *ensembles* de gains et les probabilités de réalisation associées. Les bénéfices sont seulement *espérés* parce qu'ils peuvent dépendre d'autres ensembles d'événements et de leurs probabilités associées, indépendamment de la probabilité que la transaction soit finalisée ou que les informations restent privées. En d'autres termes, $v_E()$ et $p^d()$ peuvent être interprétés comme des paramètres multivariés dans lesquels on retrouve beaucoup d'autres variables, prévisions et fonctions du fait de la complexité du réseau décrivant la vie privée (cf. ci-dessus).

Au cours du temps, la probabilité de garder une certaine information privée ne dépendra plus seulement de la technologie choisie *d* mais aussi des efforts

2. Voir aussi Acquisti et al. (2003).

des autres parties pour s'approprier cette information. Ces efforts peuvent dépendre, entre autres, de la valeur attendue que les autres parties accordent à cette information. La probabilité de garder l'information privée va également dépendre de l'environnement dans lequel la transaction a lieu. De la même manière, le gain espéré de la préservation de l'information privée sera aussi une suite de distributions de probabilité dépendant au cours du temps, de plusieurs paramètres. Imaginez que la probabilité de garder vos transactions privées confidentielles soit très élevée quand votre banque est aux Bermudes : la valeur espérée de la préservation de la confidentialité de vos informations financières va dépendre de plusieurs autres éléments.

Un agent rationnel devrait, *en théorie*, choisir la technologie *d* qui maximise son gain espéré dans l'équation 1. Il choisirait vraisemblablement de finaliser sa transaction avec l'aide d'une technologie de protection de ses données personnelles. Il pourrait peut-être décider de réaliser sa transaction sans protection. Peut-être ne finalisera-t-il même pas la transaction ($d = 0$). Par exemple, l'agent pourrait prendre en considération les coûts et les avantages de l'envoi d'un courrier électronique via un système anonyme MIX-net (Chaum, 1981) et les comparer avec les coûts et les bénéfices de l'envoi de ce courrier électronique à travers un canal conventionnel et non anonyme. L'importance des paramètres dans l'équation 1 va changer selon la technologie choisie. Les systèmes MIX-net pourraient diminuer les pertes attendues des intrusions dans la vie privée. Les systèmes conventionnels, non anonymes, de courrier électronique pourraient, quant à eux, garantir une fiabilité comparativement supérieure et (éventuellement) réduire les coûts des opérations.

RATIONALITÉ ET DISTORSIONS PSYCHOLOGIQUES

L'équation 1 propose une feuille de route très complète (même si elle est intentionnellement générique) pour naviguer à travers les différents arbitrages en matière de vie privée, mais qu'en fait, aucun humain n'est en mesure d'utiliser.

Nous faisons allusion à certaines difficultés lorsque nous avons noté que plusieurs niveaux de complexité étaient dissimulés derrière les concepts de « valeur espérée de conserver certaines informations privées » et de « probabilité » de pouvoir effectivement le faire. Plus précisément, un agent est confronté à trois problèmes lorsqu'il compare les arbitrages implicitement contenus dans l'équation 1 : une information incomplète concernant *tous* les paramètres ; un

pouvoir *limité* pour traiter toute l'information disponible ; la difficulté à ne pas dévier de la logique rationnelle de maximisation de l'utilité. Ces trois problèmes sont précisément les mêmes questions auxquelles les gens doivent répondre quotidiennement lorsqu'ils sont amenés à prendre des décisions en matière de vie privée. Nous discutons de chacune de ces questions en détail.

Information incomplète

À quelle information l'individu a-t-il accès lorsqu'il est amené à prendre des décisions sensibles relativement à sa vie privée ? Par exemple, est-il conscient des intrusions dans sa vie privée et des risques associés ? Que sait-il de l'existence et des caractéristiques des technologies de protection ?

Les transactions économiques sont souvent caractérisées par les problèmes d'information incomplète ou asymétrique. Les différentes parties prenantes peuvent ne pas disposer de la même quantité d'informations pour réaliser une transaction donnée et être confrontés à des incertitudes quant à certains de ses aspects importants (Akerlof, 1970). Presque tous les paramètres de l'équation 1 sont affectés par l'information incomplète et en particulier, l'estimation des coûts et des bénéfices. Les coûts et bénéfices associés à la protection de la vie privée et aux intrusions sont à la fois monétaires et immatériels. Les coûts monétaires incluent par exemple des coûts d'adoption (qui sont probablement fixes) et des coûts d'usage (qui sont variables) des technologies de protection – si l'individu décide de se protéger lui-même. Ils peuvent inclure les coûts financiers liés à l'usurpation de l'identité, s'il s'avère que les informations de l'individu n'ont pas été correctement protégées. Les coûts immatériels peuvent inclure les coûts d'apprentissage de la technologie de protection, les coûts de changement d'une application à l'autre, les stigmas sociaux lorsqu'on utilise les technologies visant la préservation de l'anonymat, et beaucoup d'autres aspects. De même, les bénéfices de la protection (ou de l'absence de protection) des informations personnelles peuvent aussi être facilement évalués en termes monétaires (la remise que vous obtenez en échange de la révélation de données personnelles) ou être intangibles (le sentiment de protection lorsque vous envoyez des mails cryptés).

Il est difficile pour un individu d'estimer toutes ces variables. Les technologies de l'information peuvent rendre les atteintes à la vie privée omniprésentes et invisibles. Un grand nombre d'avantages relatifs à la protection ou à l'intrusion dans la vie privée peuvent être décelés ou établies seulement de

manière *ex post* à travers une expérience vécue. Considérons par exemple les difficultés dans l'utilisation des technologies de cryptage et de protection de la vie privée décrites dans Whitten et Tygar (1999) ou la difficulté à prédire de quelle manière les informations personnelles d'un individu, une fois mises en ligne sur un réseau social, pourront être utilisées par d'autres membres ou par les gestionnaires de ce réseau.

En outre, les calculs implicites dans l'équation 1 dépendent de l'information incomplète concernant la distribution des probabilités des événements futurs. Ces distributions peuvent être estimées après la connaissance de données comparables – par exemple, la probabilité qu'une transaction par carte bancaire entraînera une fraude peut être calculée en utilisant les statistiques existantes. Pour d'autres événements, la distribution des probabilités peut être très difficile à estimer parce que l'environnement est très dynamique – par exemple, la probabilité d'être sujet à une usurpation d'identité dans les cinq prochaines années à cause de certaines données que vous divulguez *maintenant*. Pour d'autres événements encore, cette distribution peut être complètement subjective – par exemple, la probabilité qu'une nouvelle forme d'attaque sur un système crypté, actuellement sécurisé, puisse ouvrir l'accès à toutes vos communications personnelles cryptées d'ici quelques années. Cela soulève un autre problème : celui de la rationalité limitée.

Rationalité limitée

Est-ce que l'individu est capable de *calculer* tous les paramètres pertinents pour son choix ? Ou est-il rationnellement limité ?

Par rapport à notre objet, la rationalité limitée désigne l'incapacité à évaluer et comparer l'étendue des avantages associés aux diverses stratégies que l'individu peut choisir dans des situations sensibles en matière de vie privée. Elle se rapporte aussi à l'incapacité de traiter toute l'information stochastique liée aux risques et probabilités d'événements permettant de calculer les coûts et les bénéfices en matière de vie privée.

Dans la théorie économique standard, l'agent est supposé disposer à la fois d'une rationalité et d'un pouvoir « computationnel » illimité pour traiter l'information. Cependant, les êtres humains sont incapables de traiter toute l'information en leur possession et d'en tirer des conclusions pertinentes (Simon,

1982). Dans le scénario que nous considérons, une fois qu'un individu fournit des informations personnelles à d'autres parties, il perd littéralement tout contrôle de cette information. Cette perte de contrôle s'étend aux autres parties et persiste pour des périodes de temps indéterminées. Étant dans une position d'asymétrie informationnelle par rapport à la partie avec qui il réalise une transaction, ses décisions doivent être basées sur des évaluations stochastiques, et l'intensité des facteurs qui peuvent affecter l'individu deviennent très difficiles à agréger, à calculer et à comparer[3]. La rationalité limitée va influer sur le calcul des paramètres dans l'équation 1, et en particulier δ, γ, $v_E()$ et $p_t()$. Les coûts cognitifs engendrés en essayant de calculer la meilleure stratégie peuvent être si élevés que l'individu va simplement recourir à des heuristiques simples.

Distorsions psychologiques

Finalement, même si un individu a accès à toute l'information et peut la traiter de façon appropriée, il aura très vraisemblablement toujours des difficultés à suivre la logique rationnelle présentée dans l'équation 1. Un large pan de la littérature économique et psychologique a confirmé l'impact de diverses formes de distorsions psychologiques sur le processus décisionnel de l'individu. La question de la vie privée semble être un terrain d'étude qui englobe beaucoup de ces distorsions : l'actualisation hyperbolique, la sous-assurance, les problèmes d'autocontrôle, la gratification immédiate, et bien d'autres. La dichotomie traditionnelle entre l'état d'esprit et le comportement, observée dans plusieurs aspects de la psychologie humaine et étudiée dans la littérature en psychologie sociale depuis LaPierre (1934) et Corey (1937), peut aussi apparaître dans le domaine de la vie privée en raison de ces distorsions.

Par exemple, les individus ont tendance à actualiser « hyperboliquement » leurs coûts et bénéfices futurs (Rabin et O'Donoghue, 2000 ; O'Donoghue et Rabin, 2001). En économie, l'actualisation hyperbolique implique l'incohérence temporelle des préférences personnelles ; les événements futurs seraient ainsi actualisés à des taux différents par rapport aux événements à plus court terme. L'actualisation hyperbolique peut influencer les décisions en matière de vie privée, par exemple lorsque l'on actualise fortement la probabilité (fai-

3. L'utilité négative provenant des potentiels abus relatifs à l'utilisation des informations personnelles d'un individu pourrait être un choc aléatoire dont la probabilité et l'ampleur sont extrêmement variables. Par exemple, une information apparemment inoffensive pourrait devenir un argument crucial ou avoir des répercussions dangereuses en matière de droit.

ble) de risques futurs (forts) tels que l'usurpation d'identité[4]. Un autre aspect lié à l'actualisation hyperbolique est la tendance des individus à s'assurer insuffisamment contre certains risques (Kunreuther, 1984).

De façon générale, les individus peuvent se fixer des contraintes quant à leur comportement futur, lesquelles limitent leur propre réalisation en matière d'utilité maximale : les gens peuvent vraiment vouloir se protéger, mais à cause du biais d'autocontrôle, ils ne suivront pas cette voie et opteront plutôt pour une gratification immédiate. « Les individus ont tendance à sous-estimer les effets des changements de leurs états, et donc ils projettent d'une manière erronée leurs préférences de consommation actuelles sur leurs préférences futures. Au-delà de la simple suggestion que les gens ne prédisent pas correctement leurs goûts futurs, ce biais de projection suppose une tendance systématique de ces perceptions erronées qui peut mener à des erreurs systématiques dans des environnements de choix dynamiques (Lowenstein et al., 2003, p. 2).

En outre, les individus souffrent d'un biais d'optimisme (Weinstein, 1989), la perception erronée que sous des conditions similaires, ses risques sont plus faibles que ceux des autres individus. Le biais d'optimisme peut nous amener à penser que nous ne serons pas la cible d'intrusions dans notre vie privée.

Les individus rencontrent des difficultés lorsqu'ils font face à des risques cumulatifs. Slovic (2000) montre, par exemple, que si les jeunes fumeurs sont conscients des risques du tabagisme à long terme, ils ne font pas complètement la relation cumulative entre les risques faibles associés à chaque cigarette supplémentaire et l'intensification progressive d'un grave danger. Les difficultés à faire face à des risques cumulatifs concernent aussi la vie privée parce que nos informations personnelles, une fois qu'elles sont publiées, peuvent rester disponibles pendant une longue période de temps. Et dans la mesure où elles peuvent être reliées à d'autres données, les « zones d'anonymats » (Serjantov et Danezis, 2002, Diaz et Seys, 2002) dans lesquels nous souhaitons rester cachés, se réduisent progressivement. Par conséquent, le risque total lié à la divulgation de différentes informations personnelles est supérieur à la somme des risques individuels associés à chacune des informations révélées.

Par ailleurs, il est plus facile de gérer les actions et les effets qui se situent dans un futur proche. Il est plus difficile de se concentrer sur les actions et les

4. Une description plus rigoureuse et une application de l'actualisation hyperbolique sont présentées dans la section 4.

conséquences qui sont prévues dans un futur lointain étant donné notre capacité de prévision limitée. Le comportement peut ainsi changer selon les prévisions établies, même si les préférences restent identiques (Jehiel et Lilico, 2002). Ce phénomène pourrait aussi affecter les décisions en matière de vie privée, puisque les coûts de la protection sont généralement immédiats, alors que les bénéfices (absence d'intrusions) s'avèrent moins visibles et s'étaleront sur des périodes futures.

Pour résumer, lorsque nous devons prendre des décisions sensibles concernant notre vie privée, nous ne disposons presque jamais de toutes les données nécessaires pour faire un choix bien informé. Cependant, même si nous les avions, nous serions probablement incapables de les traiter correctement. Et même si nous étions capables de le faire, nous finirions toujours par agir en dépit de notre meilleur jugement personnel. Nous allons présenter dans la section suivante un modèle traitant du comportement et des attitudes en matière de vie privée, basé sur certaines de ces conclusions et en particulier, sur le modèle de la gratification immédiate.

VIE PRIVÉE ET ÉCONOMIE DE LA GRATIFICATION IMMÉDIATE

Le problème de la gratification immédiate (qui est lié aux concepts de l'incohérence temporelle, de l'actualisation hyperbolique et du biais d'autocontrôle) est décrit par O'Donoghue et Rabin (2001, p. 4) de la manière suivante : « Les préférences relatives d'un individu pour un bien-être à une période rapprochée par rapport à une date plus éloignée deviennent de plus en plus fortes au fur et à mesure que l'échéance la plus tôt se rapproche. […] Les individus ont des problèmes d'autocontrôle provoqués par une tendance à rechercher une gratification immédiate d'une manière que leur "soi-à-long-terme" n'apprécie pas de la même façon. » Par exemple, si vous avez seulement deux alternatives, le lundi vous déclarerez certainement préférer travailler 5 heures le samedi plutôt que 5 heures 30 le dimanche. Mais à mesure que le samedi s'approche, vous allez probablement préférer reporter votre travail au dimanche.

Cette simple observation a des implications plutôt importantes en économie où la cohérence temporelle des préférences est le modèle dominant. Considérons d'abord le modèle traditionnel de l'utilité que les agents retirent de la consommation : le modèle suggère que l'utilité est actualisée de façon exponentielle au fil du temps :

$$U_t = \sum_{\tau=t}^{T} \delta^{\tau} u_{\tau} \tag{2}$$

Dans l'équation 2, l'utilité cumulée U à la date t est la somme actualisée de toutes les utilités du temps t (le présent) au temps T (le futur). δ est le taux d'actualisation qui prend une valeur comprise entre 0 et 1. Une valeur 0 implique que l'individu actualise à tel point que l'utilité des périodes futures vaut zéro aujourd'hui. Une valeur 1 implique que l'individu est tellement patient qu'il n'actualise pas ses utilités futures. Le taux d'actualisation est utilisé en économie pour rendre compte du fait qu'avoir un dollar dans un an a certainement une valeur mais pas autant qu'avoir ce dollar *maintenant*. Dans l'équation 2, si tous les u_{τ} étaient constants – par exemple, 10 – et avait une valeur de 0,9, alors au temps $t = 0$ (c'est-à-dire *maintenant*), u_0 aurait une valeur de 10, mais u_1 vaudrait 9.

En modifiant le modèle traditionnel de l'utilité actualisée, Laibson (1994), puis Rabin et O'Donoghue (2000) ont proposé un modèle qui prend en compte les éventuelles incohérences temporelles des préférences. Considérons l'équation 3 :

$$U_t(u_t, u_{t+1}, ..., u_T) = \delta^t u_t + \beta \sum_{\tau=t+1}^{T} \delta^t u_{\tau} \tag{3}$$

Supposons que $\delta, \beta \in [0,1]$. δ est le taux d'actualisation pour l'utilité intertemporelle comme dans l'équation 2. β est le paramètre qui rend compte de la tendance individuelle à retirer une satisfaction immédiate (une forme d'incohérence temporelle des préférences). Lorsque β est égal à 1, le modèle retrace le modèle traditionnel de la cohérence temporelle des choix, et l'équation 3 est identique à l'équation 2. Cependant, lorsque β est égal à 0, l'individu ne se soucie de rien d'autre que du moment présent. En fait, chaque β inférieur à 1 représente un biais d'autocontrôle.

La littérature expérimentale a démontré de façon rigoureuse que les êtres humains ont tendance à avoir des problèmes d'autocontrôle, même s'ils déclarent le contraire : nous avons tendance à éviter et à reporter les activités indésirables, même si cela va demander de fournir davantage d'efforts le moment venu ; et nous avons tendance à nous engager de façon excessive dans des activités plaisantes, même si cela pourrait nous causer de la souffrance, voire diminuer notre utilité dans le futur.

Ce cadre d'analyse peut être appliqué à l'étude des attitudes et du comportement en matière de vie privée. Considérons, par exemple, le cas des réseaux sociaux en ligne que nous avons déjà évoqué dans ce manuscrit. Un utilisateur de Facebook peut apprécier un intérêt immédiat bien qu'immatériel du fait de télécharger une photo de jeunesse, peut-être légèrement embarrassante, sur son profil : il peut effectivement avoir un certain plaisir à partager cette photo avec ses amis et à lire les commentaires sympathiques de ses pairs sur cette photo. Toutefois, cet utilisateur aura tendance à n'accorder que très peu d'attention aux coûts liés à la possibilité que cette photo puisse, quelque temps plus tard, être aussi accessible à des individus autres que ses amis – par exemple, son patron ou son superviseur. D'un autre côté, protéger sa vie privée signifie quelquefois, se protéger d'un certain nombre de tracas (télémarketeurs, ou les personnes qui lorgnent à travers votre fenêtre et observent votre façon de vie – voir Shostack (2003)) ; mais cela représente quelquefois une sorte d'assurance contre des risques futurs mais seulement incertains.

Par conséquent, dans les études réalisées à la date $t = 0$, les sujets interrogés sur leur attitude à l'égard des risques en matière de vie privée, peuvent considérer de façon mentale, certains coûts de la protection personnelle à un moment plus lointain $t = s$ et comparer ces coûts avec ceux évités des intrusions dans la vie privée à une date beaucoup plus lointaine $t = s + n$. Leurs alternatives à la date 0 de l'étude sont représentées dans l'équation 4.

$$\min_{wrt\ x} DU_0 = \beta\left[(E(c_{s,p})\delta^s x) + (E(c_{s+n,i})\delta^{s+n}(1-x))\right] \tag{4}$$

x est une variable indicatrice qui peut prendre les valeurs 0 et 1. Elle représente le choix de l'individu – les coûts que l'individu choisit de supporter : le coût prévu de sa protection personnelle au temps *s*, $E(c_{s,p})$ (dans ce cas $x = 1$), ou les coûts attendus si l'individu fait l'objet d'intrusions dans sa vie privée à une date ultérieure *s*+*n*, $E(c_{s+n,i})$.

L'individu essaie de minimiser la désutilité *DU* associée à ces coûts par rapport à *x*. Comme il actualise les deux événements futurs avec le même taux d'actualisation (mais à des périodes différentes), pour certaines valeurs des paramètres, l'individu peut conclure que payer pour se protéger lui-même représente une certaine valeur. En particulier, cela se vérifie lorsque :

$$E(c_{s,p})\delta^s x < E(c_{s+n,i})\delta^{s+n} \tag{5}$$

Considérons maintenant ce qui se passe lorsque l'on parvient au moment $t = s$. À présent, un prix réel devrait être payé pour bénéficier d'une certaine forme de protection (disons, en commençant à crypter de tous vos mails pour vous protéger des intrusions à venir). Maintenant, l'individu va *percevoir* une vision différente des choses :

$$\min_{wrt\ x} DU_s = \delta E(c_{s,p})x + \beta E(c_{n,i})\delta^n(1-x) \tag{6}$$

Notons que rien n'a changé dans l'équation (et certainement pas la perception des risques par l'individu) si ce n'est le *temps*. Si β (le paramètre indiquant le degré des problèmes d'autocontrôle) est inférieur à 1, il est possible que maintenant, l'individu va choisir effectivement de *ne pas* se protéger. Cela va arriver lorsque :

$$\delta E(c_{s,p}) > \beta E(c_{n,i})\delta^n \tag{7}$$

Notons que les inégalités 5 et 7 peuvent être vérifiées simultanément pour $\beta<1$. Au moment de l'enquête, l'individu déclarait honnêtement qu'il voulait *en principe* se protéger. Mais dès qu'il lui est demandé de faire un effort pour se protéger, il choisit de courir le risque d'avoir des intrusions dans sa vie privée.

Des arguments mathématiques similaires peuvent être avancés pour la comparaison entre les coûts immédiats avec des bénéfices immédiats (s'inscrire sur une liste rouge pour éviter les tracas des télémarketeurs pendant son dîner) et les coûts immédiats avec seulement des gains futurs espérés (s'assurer contre le vol d'identité, ou se protéger des fraudes en n'utilisant jamais sa carte de crédit en ligne), particulièrement lorsque les gains espérés dans le futur (ou les risques évités) sont également intangibles : les conséquences immatérielles du fait de vivre (ou non) dans une société de renseignements, ou l'effet dissuasif (ou l'absence) d'être sous surveillance.

Le lecteur aura noté que nous nous sommes focalisés sur les coûts *perçus* (attendus) *E(c)* plutôt que sur les coûts réels. Nous ne connaissons pas les coûts réels et nous ne prétendons pas que les individus les connaissent. Mais nous sommes en mesure de montrer que sous certaines conditions, même les coûts perçus comme étant très élevés (notamment pendant les périodes de débats intenses sur la vie privée) seront ignorés.

Nous pouvons présenter quelques exemples numériques fictifs pour rendre l'analyse plus concrète. Nous présentons quelques scénarios inspirés des calculs effectués par Rabin et O'Donoghue (2000).

Imaginons une économie avec juste quatre périodes (tableau 1). Chaque individu peut souscrire à une carte de fidélité d'un supermarché en révélant des informations personnelles. S'il le fait, l'individu reçoit une remise de 2 pendant la période d'inscription, seulement pour payer une unité à chaque fois, ceci à cause de la discrimination des prix basée sur l'information qu'il a révélée (nous n'essayons pas de rendre plus réaliste cet exemple qui est évidemment abstrait ; le point sur lequel nous insistons est la manière dont les incohérences temporelles peuvent affecter le comportement individuel étant donné les coûts et les bénéfices espérés de certaines actions)[5]. Selon la période que l'individu choisit pour « vendre » ses données, nous avons des bénéfices non actualisés représentés dans le tableau 1.

Tableau 1. Gains (fictifs) espérés de la souscription à un programme de fidélité

	Période 1	**Période 2**	**Période 3**	**Période 4**
Bénéfices de la vente période 1	2	0	0	0
Coûts relatifs à la vente période 1	0	1	1	1
Bénéfices de la vente période 2	0	2	0	0
Coûts relatifs à la vente période 2	0	0	1	1
Bénéfices de la vente période 3	0	0	2	0
Coûts relatifs à la vente période 3	0	0	0	1

Imaginons que l'individu envisage ces différentes alternatives et les actualise suivant l'équation 3. Supposons que $\delta = 1$ pour toutes les catégories d'individus (ceci signifie pour simplifier que nous ne considérons pas l'actualisation inter-temporelle) mais que $\beta = 1/2$ pour les individus caractérisés par une incohérence temporelle de leurs préférences et $\beta = 1$ pour tous les autres individus. L'individu avec des préférences cohérentes dans le temps choisira de souscrire une carte de fidélité à la toute dernière période et obtient un bénéfice de 2-1=1. L'individu ayant des problèmes de gratification immédiate, pour qui

5. On pourrait prétendre qu'à long terme, les cartes de fidélité continuent à procurer des avantages. Nous faisons ici l'hypothèse simplificatrice que ces bénéfices ne sont pas aussi importants que les coûts futurs encourus après avoir révélé ses goûts. Nous supposons aussi que les économies réalisées cessent à la période 4 pour tous les individus, peu importe le moment où les gens choisissent de souscrire à une carte de fidélité.

$\beta = 1/2$, va plutôt percevoir les bénéfices de souscription maintenant ou ceux à la période 3 comme équivalents (0,5) et souscrira tout de suite, se mettant de la sorte dans une situation pire.

Rabin et O'Donoghue (2000) suggèrent aussi qu'outre la distinction entre les individus avec des préférences cohérentes dans le temps et ceux qui sont marqués par des préférences incohérentes dans le temps, il faudrait également distinguer dans les individus avec des incohérences temporelles, ceux qui sont *naïfs* et ceux qui sont *avertis*. Les individus naïfs ayant des incohérences temporelles ne sont pas conscients de leurs problèmes d'autocontrôle – par exemple, ils sont ceux qui prévoient toujours de commencer un régime la *semaine suivante*. Les individus avertis avec des incohérences temporelles *souffrent* du biais de gratification immédiate, mais ils sont au moins conscients de leurs incohérences. Les gens qui sont dans cette catégorie agissent aujourd'hui tout en estimant correctement leurs incohérences temporelles dans le futur.

Maintenant, considérons de quelle manière cette différence affecte les décisions dans un autre scénario représenté dans le tableau 2. Un individu envisage la possibilité d'adopter une technologie donnée de protection de la vie privée. Cela va lui coûter un certain montant à la fois pour se protéger et pour *ne pas* se protéger. S'il décide de se protéger, le coût sera le montant qu'il paye – par exemple – pour une technologie qui protège ses informations personnelles. S'il décide de ne pas se protéger, le coût sera les conséquences relatives aux intrusions dans sa vie privée.

Tableau 2. Coûts (fictifs) de la protection de la vie privée et des intrusions à long terme

	Période 1	**Période 2**	**Période 3**	**Période 4**
Coûts de protection	5	6	8	.
Coûts d'intrusion attendus	.	7	9	15

Nous supposons que *tous* ces coûts agrégés augmentent au cours du temps, bien que les dynamiques soient également distinctes. Au fil du temps, de plus en plus d'informations sur l'individu sont divulguées et il devient plus coûteux d'être protégé des intrusions dans la vie privée. En même temps, cependant, les intrusions deviennent plus fréquentes et malveillantes.

Dans la période 1, l'individu peut se protéger lui-même en dépensant 5, ou alors il peut choisir de faire face dans la période suivante, au risque d'intrusion dans sa vie privée qui va coûter 7. Dans la seconde période, en supposant qu'aucune intrusion n'a déjà eu lieu, l'individu peut encore se protéger en dépensant un peu plus, soit 6 ; ou alors il choisit de faire face au risque d'intrusion dans la période suivante (troisième), ce qui devra lui coûter 9. À la troisième période, il pourrait se protéger en dépensant 8 ou supporter un coût de 15 à la dernière période.

Ici aussi, nous ne cherchons pas à calibrer les valeurs du tableau 2. Nous nous concentrons sur les différents comportements engendrés par l'hétérogénéité dans la cohérence temporelle et la sophistication contre la naïveté. Nous supposons que $\beta = 1$ pour les individus n'ayant pas de problèmes d'autocontrôle et que $\beta = 1/2$ pour tous les autres individus. Nous supposons pour simplifier que $\delta = 1$ pour tous.

Les individus avec des préférences cohérentes dans le temps vont évidemment choisir de se protéger le plus rapidement possible.

À la première période, les individus naïfs avec des préférences temporelles incohérentes vont comparer les coûts liés au fait de se protéger ou bien faire face à une intrusion dans la deuxième période. Ils préféreront attendre jusqu'à la période suivante pour se protéger car $5 > 7 \times (1/2)$. Mais à la seconde période, ils vont comparer $6 > 9 \times (1/2)$ et ainsi, ils vont encore reporter à plus tard leur protection. Ils continueront d'agir ainsi, faisant face à des risques de plus en plus élevés. Finalement, ils risqueront de supporter les coûts d'intrusion les plus élevés (notons une fois de plus que nous supposons simplement que les individus *croient* qu'il existe des risques en matière de vie privée et qu'ils s'accroissent au cours du temps ; nous reviendrons sur ce concept plus tard).

Quant aux individus avertis avec des préférences temporelles incohérentes, ils adopteront une technologie de protection à la période 2 et payer 6. À la période 2, ils réaliseront (correctement) que s'ils attendent jusqu'à la période 3 (ce qu'ils sont tentés de faire, parce que $6 > 9 \times (1/2)$), leur biais d'autocontrôle va les inciter à reporter encore une fois l'adoption d'une technologie (parce que $8 > 15 \times (1/2)$). Par conséquent, ils prévoient qu'ils supporteront un coût de $15 \times (1/2)$, qui est supérieur à 6, soit le coût de se protéger à la période 2. Pourtant, à la période 1, ils prévoient correctement de ne pas attendre après la période 2 pour se protéger. Par conséquent, ils attendent jusqu'à la

période 2, parce que $5 > 6 \times (1/2)$, auquel moment ils adoptent une technologie de protection (voir aussi Rabin et O'Donoghue, 2000).

Pour récapituler, les individus marqués par des préférences temporelles incohérentes, ont tendance à ne pas évaluer pleinement les risques à venir, ainsi que, s'ils sont naïfs, leur incapacité à gérer ces risques. Cela arrive même s'ils sont conscients à la fois de ces risques et du fait qu'ils *s'accroissent*. De notre second scénario, nous avons appris que l'incohérence temporelle peut amener les gens à accepter des risques de plus en plus élevés. Les individus tendent alors à minimiser le fait que si les actions isolées présentent des risques faibles, la répétition de celles-ci forme un dommage considérable : la vie privée présente cet aspect trompeur que l'on se rend réellement compte de sa valeur seulement lorsqu'on l'a perdue. Cette dynamique rend compte de l'essence même de la vie privée et des prétendues zones d'anonymat (Serjantov et Danezis, 2002 ; Diaz et Seys, 2002) où chaque bribe d'information que nous révélons peut être reliée à d'autres, de sorte que la totalité représente plus que la somme des parties.

De plus, Rabin et O'Donoghue (2000) montrent que lorsque les coûts sont immédiats, les individus marqués par une incohérence temporelle ont tendance à tergiverser ; lorsque les gains sont immédiats, ils tendent alors à *préopérer*. Dans notre contexte, les choses sont encore plus intéressantes parce que toutes les décisions en matière de vie privée impliquent à la fois des coûts et des bénéfices. Ainsi, nous refusons l'utilisation de l'eCash (Chaum, 1983) afin d'éviter les coûts de changement de carte de crédit. Mais nous acceptons le risque que notre numéro de carte de crédit puisse être utilisé de façon malveillante sur Internet. Et nous divulguons nos informations personnelles aux supermarchés dans le but d'avoir des réductions immédiates – qui seront probablement utilisées le moment venu pour des stratégies de discrimination par les prix (Acquisti et Varian, 2001 ; Odlyzko, 2003).

Nous avons montré dans le deuxième scénario comment des individus avertis, mais marqués par des incohérences temporelles, choisiront probablement de protéger leurs informations seulement à la période 2. Les personnes averties qui ont des problèmes d'autocontrôle peuvent être plus désorientées, quelquefois même lorsqu'on les compare aux personnes naïves ayant des problèmes d'incohérence temporelle (combien de défenseurs de la vie privée utilisent régulièrement les technologies de protection ?). La logique est que les personnes averties sont conscientes de leurs problèmes d'autocontrôle et au lieu de

les ignorer, ils les intègrent dans leur processus décisionnel. Ceci peut diminuer leur motivation personnelle à se comporter *maintenant* de manière optimale. Les défenseurs avertis de la vie privée se rendent vraisemblablement compte que se protéger contre toute intrusion possible est irréaliste et donc agissent d'une manière peu cohérente à l'instant présent (et se familiariser à cela, comme une sorte d'arbitraire cohérent). Ceci corrobore les résultats de Spiekermann et al. (2002) présentés à la Conférence ACM EC'01. Ces chercheurs montraient en effet que les fervents défenseurs de la vie privée étaient également prêts à révéler des informations personnelles en échange de récompenses monétaires.

Il est aussi intéressant de noter que ces incohérences ne sont pas engendrées par l'ignorance de risques existants ou par la confusion au sujet des technologies disponibles. Les individus que nous avons décrits dans les scénarios théoriques, sont conscients de leurs risques et coûts *perçus*. Toutefois, sous certaines conditions, l'importance de ces responsabilités est presque insignifiante. L'individu va prendre petit à petit des risques de plus en plus élevés, qui auront à long terme, d'importantes implications.

DISCUSSION

Une application des modèles de biais d'autocontrôle et de gratification immédiate à l'analyse du processus décisionnel en matière de vie privée peut apporter une nouvelle perspective dans le débat actuel. Nous avons montré qu'un modèle de comportement rationnel en matière de vie privée n'est pas réaliste, alors que les modèles basés sur les distorsions psychologiques offrent une description plus correcte du processus décisionnel. Nous avons expliqué pourquoi les individus qui souhaitent vraiment protéger leur vie privée, ne seraient pas en mesure de le faire en raison de distorsions psychologiques que la littérature en économie comportementale a bien fait ressortir. Nous avons mis l'accent sur le fait que ces distorsions affectent aussi bien les individus naïfs que des personnes plus averties. De façon surprenante, nous avons aussi constaté que ces incohérences peuvent se produire lorsque la perception des risques de l'absence de protection de la vie privée est perçue de manière significative par les individus.

Les incertitudes supplémentaires, l'aversion aux risques et les diverses attitudes à l'égard des pertes et gains peuvent être des facteurs de confusion dans

notre analyse. Une validation empirique est nécessaire pour calibrer les effets des différents facteurs.

Une analyse empirique peut débuter avec la comparaison des données disponibles sur le taux d'adoption des technologies de protection qui offrent un refuge immédiat contre les intrusions mineures mais pénibles dans la vie privée (par exemple, l'inscription sur les listes « do not call ») avec les données sur l'adoption des technologies qui offrent une protection nettement moins perceptible à l'encontre de risques plus dangereux mais également moins visibles (par exemple, les assurances contre le vol d'identité). Toutefois, seule une approche expérimentale dans un environnement contrôlé et sur différentes périodes de temps pourrait nous permettre de distinguer l'influence de plusieurs facteurs. Les enquêtes seules ne suffisent pas dans la mesure où nous avons montré que les attitudes durant les périodes d'enquête correspondent rarement aux décisions prises le moment venu. Une vérification expérimentale est prévue dans notre programme de recherche en cours.

Les distorsions psychologiques dont nous avons discuté, peuvent être analysées dans le débat actuel sur la manière de traiter la question de la préservation de la vie privée : l'autorégulation industrielle, la protection des individus par leurs propres moyens (à travers la technologie ou d'autres stratégies) ou l'intervention publique. Les conclusions auxquelles nous sommes parvenus suggèrent qu'il est difficile de faire confiance aux individus pour prendre les décisions les plus conformes à leurs intérêts lorsqu'il s'agit de leur vie privée. Cela ne signifie pas pour autant que les technologies de protection de la vie privée sont inefficaces. Au contraire, nos résultats dont le but est de proposer un modèle plus réaliste du comportement des utilisateurs, pourraient être d'une grande utilité pour les technologues dans leur conception de tels outils. Toutefois, nos résultats impliquent aussi que la technologie et la sensibilisation des individus ne peuvent pas à elles seules apporter toutes les solutions au problème de la protection de la vie privée. Des technologies améliorées (avec des faibles coûts d'adoption et de protection) et plus d'informations sur les risques et les opportunités peuvent certainement être d'un grand intérêt. Toutefois, les mécanismes plus fondamentaux du comportement humain doivent également être abordés. L'autorégulation même en présence d'une information et d'une sensibilisation complètes du public ne fonctionnera pas forcément pour les mêmes raisons. Une combinaison de la technologie, de la sensibilisation et des politiques régulatrices – calibrées pour générer et faire respecter les responsabilités et les incitations adéquates des différentes parties - peut être requise pour augmenter le

bien-être associé à la vie privée (comme dans d'autres domaines d'une économie, cf. analyse similaire de Lowenstein et al., 2003).

Observer que les gens ne veulent pas payer pour divulguer leurs informations personnelles ou qu'ils ne se soucient pas de leur vie privée n'est que partiellement vrai. Les gens ne sont pas en mesure d'agir comme des agents rationnels au sens économique en matière de vie privée. Et la question de savoir si « les consommateurs s'en soucient » est différente de celle de savoir si finalement « la vie privée importe ». D'un point de vue *économique*, la question de savoir si la vie privée *devrait* être protégée ou non reste encore ouverte. C'est une question qui implique de définir les contextes spécifiques dans lesquels le concept de vie privée est invoqué. Mais la valeur de la vie privée va au-delà des domaines de la logique économique et de l'analyse coûts/bénéfices, et aboutit aux liens entre les opinions de chacun sur la société et la liberté. Pourtant, même d'un point de vue purement économique, les preuves empiriques suggèrent que les coûts en matière de vie privée (du spamming à l'usurpation d'identité, les intrusions et bien d'autres risques [Privacy Rights Clearinghouse, 2000 ; Community Banker Association of Indiana, 2001 ; Gellman, 2002 ; Shostack, 2003 ; Odlyzko, 2003]) sont élevés et continuent de croître.

Remerciements

L'auteur exprime sa reconnaissance au Berkman Development Fund de l'Univeristé Carnegie Mellon, qui a partiellement financé cette recherche. Il voudrait également remercier Jens Grossklags, Charis Kaskiris, et les trois rapporteurs anonymes pour leurs commentaires avisés.

RÉFÉRENCES

ACQUISTI A. (2004), "Privacy in Electronic Commerce and the Economics of Immediate Gratification", in *Proceedings of the ACM Conference on Electronic Commerce (EC '04)*, pp. 21-29.

ACQUISTI A., R. DINGLEDINE et P. SYVERSON (2003), "On the economics of anonymity", in *Financial Cryptography - FC '03*, pp. 84-102, Springer Verlag.

ACQUISTI A. et J. GROSSKLAGS (2003), "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior", in *2nd Annual Workshop on Economics and Information Security - WEIS '03*.

ACQUISTI A. et H. R. VARIAN (2001), *Conditioning prices on purchase history*, Technical report, University of California, Berkeley. Presented at the European Economic Association Conference, Venice, IT, August 2002. http://www.heinz.cmu.edu/~acquisti/papers/privacy.pdf.

AKERLOF G.A. (1970), "The market for 'lemons:' quality uncertainty and the market mechanism", *Quarterly Journal of Economics*, vol. 84, pp. 488-500.

BECKER G. S. et K. M. MURPHY (1988), "A theory of rational addiction", *Journal of Political Economy*, vol. 96, pp. 675-700.

BRUNK B.D. (2002), "Understanding the privacy space", *First Monday*, 7, http://firstmonday.org/issues/ issue7_10/brunk/index.html.

CALZOLARI G. et A. PAVAN (2001), *Optimal design of privacy policies*, Technical report, Gremaq, University of Toulouse.

CHAUM D. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, vol. 24, n° 2, pp. 84-88.

CHAUM D. (1983), "Blind signatures for untraceable payments", in *Advances in Cryptology - Crypto '82*, Plenum Press, pp. 199-203.

CHELLAPPA R.K. et R. SIN. (2002), "Personalization versus privacy: An empirical examination of the online consumer's dilemma", in *2002 Informs Meeting*.

COMMUNITY BANKER ASSOCIATION OF INDIANA (2001), *Identity fraud expected to triple by 2005*, http://www.cbai.org/Newsletter/December2001/ identity_fraud_de2001.htm.

COREY S. (1937), "Professional attitudes and actual behavior", *Journal of Educational Psychology*, vol. 28, n° 1, pp. 271-280.

DIAZ C., S. SEYS, J. CLAESSENS et B. PRENEEL (2002), "Towards measuring anonymity", in P. Syverson and R. Dingledine, editors, *Privacy Enhancing Technologies - PET '02*. Springer Verlag, 2482.

ebusinessforum.com (2000), *eMarketer: The great online privacy debate*. http://www.ebusinessforum. com/index.asp?doc_id=1785&layout=rich_story.

FEDERAL TRADE COMMISSION (2002), *Identity theft heads the ftc's top 10 consumer fraud complaints of 2001*, http://www.ftc.gov/opa/2002/01/idtheft.htm.

FEDERAL TRADE COMMISSION (2000), *Privacy online: Fair information practices in the electronic marketplace*, http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

GELLMAN R. (2002), *Privacy, consumers, and costs - How the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete*, http://www.epic.org/reports/dmfprivacy.html.

HARN I.-H., K.-L. HUI, T. S. LEE et I.P.L. PNG. (2002), "Online information privacy: Measuring the cost-benefit trade-off", *in 23rd International Conference on Information Systems*.

HARRIS INTERACTIVE (2002), «First major post-9.11 privacy survey finds consumers demanding companies do more to protect privacy; public wants company privacy policies to be independently verified», http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429.

JEHIEL P. et A. LILICO (2002), *Smoking today and stopping tomorrow: A limited foresight perspective*. Technical report, Department of Economics, UCLA.

JUPITER RESEARCH (2002), *Seventy percent of US consumers worry about online privacy, but few take protective action*, http: //www.jmm.com/xp/jmm/press/2002/pr_060302.xml.

KUNREUTHER H. (1984), *Causes of underinsurance against natural disasters*, Geneva Papers on Risk and Insurance.

LAIBSON D. (1994), *Essays on hyperbolic discounting*, MIT, Department of Economics, Ph.D. Dissertation.

LAPIERE R. (1934), "Attitudes versus actions", *Social Forces*, vol. 13, pp. 230-237.

LOWENSTEIN G., T. O'DONOGHUE et M. RABIN (2003), *Projection bias in predicting future utility. Technical report*, Carnegie Mellon University, Cornell University et University of California, Berkeley.

ODLYZKO A. (2003), "Privacy, economics, and price discrimination on the Internet", in *Fifth International Conference on Electronic Commerce*, pp. 355-366, ACM.

O'DONOGHUE T. et M. RABIN (2001), "Choice and procrastination", *Quarterly Journal of Economics*, vol. 116, pp. 121-160. La page citée dans le texte renvoie au document de travail publié en 2000.

POSNER R. A (1978), "An economic theory of privacy", *Regulation*, pp. 19-26.

POSNER R.A (1981), "The economics of privacy"», *American Economic Review*, vol. 71(2), pp. 405-409.

PRIVACY RIGHTS CLEARINGHOUSE (2000), *Nowhere to turn: Victims speak out on identity theft*, accessible sur http: //www.privacyrights.org/ar/idtheft2000.htm.

CBS News (2005), «Poll: Privacy Rights Under Attack", accessible sur http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml.

RABIN M. et T. O'DONOGHUE (2000), "The economics of immediate gratification", *Journal of Behavioral Decision Making*, vol. 13, pp. 233-250.

SERJANTOV A. et G. DANEZIS (2002), "Towards an information theoretic metric for anonymity", in P. Syverson and R. Dingledine, editors, *Privacy Enhancing Technologies - PET '02*. Springer Verlag, LNCS 2482.

SHOSTACK A. (2003), "Paying for privacy: Consumers and infrastructures", in *2nd Annual Workshop on Economics and Information Security - WEIS '03*."

SIMON H.A. (1982), *Models of bounded rationality*, Cambridge, MA, The MIT Press.

SLOVIC P. (2000) "What does it mean to know a cumulative risk? Adolescents' perceptions of short-term and long-term consequences of smoking", *Journal of Behavioral Decision Making*, vol. 13, pp. 259-266.

SPIEKERMANN S., J. GROSSKLAGS et B. BERENDT (2002), "E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior". in *3rd ACM Conference on Electronic Commerce - EC '01*, pp. 38-47.

STIGLER G.J. (1980), "An introduction to privacy in economics and politics", *Journal of Legal Studies*, vol. 9, pp. 623-644.

SYVERSON P. (2003), The paradoxical value of privacy. in *2nd Annual Workshop on Economics and Information Security - WEIS '03*.

TAYLOR C.R. (2002), *Private demands and demands for privacy: Dynamic pricing and the market for customer information*, Department of Economics, Duke University, Duke Economics Working Paper 02-02.

TUROW J., J. KING, C.J. HOOFNAGLE, A. BLEAKLEY et M. HENNESSY (2009), "Americans Reject Tailored Advertising and Three Activities that Enable It", *Annenberg School for Communication*, University of Pennsylvania.

VILA T., R. GREENSTADT et D. MOLNAR (2003), "Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market", in *2nd Annual Workshop on Economics and Information Security - WEIS '03*.

WARREN S. et L. BRANDEIS (1890), "The right to privacy", *Harvard Law Review*, vol. 4, pp. 193-220.

WEINSTEIN N.D (1989), "Optimistic biases about personal risks", *Science*, vol. 24, pp. 1232-1233.

WHITTEN A. et J. D. TYGAR (1999), "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", in *8th USENIX Security Symposium*.