Revue Internationale Multidisciplinaire
D'Economie et de Gestion
ISSN : 2724-7260
Volume 4 : Numéro 2

Peur de rater quelque chose et vulnérabilité des internautes

Salma KHRIFECH

Docteur en Marketing

Faculté des Sciences Economiques et de Gestion de Sfax

Université de Sfax, Tunisie

Salma.khrifech@gmail.com

Pr. Romdhane KHEMAKHEM

Faculté des Sciences Economiques et de Gestion de Sfax

Université de Sfax, Tunisie

rm.khemakhem@gmail.com

Revue Internationale Multidisciplinaire
D'Economie et de Gestion
ISSN : 2724-7260
Volume 4 : Numéro 2

Résumé : Avec l'essor des nouvelles technologies et la généralisation des outils de collecte de données en ligne, les internautes manifestent une préoccupation croissante à l'égard de la protection de leurs données personnelles partagées sur Internet. Le non-respect de la vie privée ainsi que des politiques de confidentialité participe à l'émergence d'une vulnérabilité liée aux données. Dans ce contexte, ce travail de recherche a pour objectif de mieux comprendre le concept de vulnérabilité liée aux données, entendu comme le sentiment d'impuissance ressenti par les internautes face à la gestion et au contrôle de leurs données personnelles, et ceci en identifiant son antécédent à savoir la peur de rater quelque chose (FOMO) et de connaitre son effet sur le comportement des internautes à savoir le changement de site Web. Une enquête est réalisée auprès de 375 répondants. Les résultats ont montré que la peur de rater quelque chose influence la vulnérabilité des internautes suite au partage de données personnelles en ligne, et que cette même vulnérabilité contribue au changement de site Web.

Mots clés : vulnérabilité des internautes suite au partage de données personnelles en ligne, la peur de rater quelques chose, changement de site Web

Abstract: With the rise of new technologies and the widespread use of online data collection tools, Internet users are increasingly concerned about the protection of their personal data shared on the Internet. Failure to respect privacy and confidentiality policies contributes to the emergence of data vulnerability. In this context, the aim of this research is to better understand the concept of data vulnerability, understood as the feeling of powerlessness experienced by Internet users when it comes to managing and controlling their personal data, by identifying its antecedent, namely the fear of missing out (FOMO), and its effect on Internet users' behavior, namely changing websites. A survey was conducted among 375 respondents. The results showed that fear of missing out influences the vulnerability of Internet users following the sharing of personal data online, and that this same vulnerability contributes to website switching.

Keywords: vulnerability of internet users following the sharing of personal data online, fear of missing out, website behavior change

ISSN : 2724-7260
Volume 4 : Numéro 2

Introduction

Depuis leur apparition au début des années 2000, les objets connectés ont connu une croissance phénoménale, et il y aura d'ici 2025, 75.44 milliards d'appareils connectés (Findstack, 2021). La place des objets connectés est aussi importante pour les particuliers que pour les entreprises, ce qui se traduit par une croissance annuelle de 13% (GlobalData, juin 2021). De plus, les revenus du marché des objets connectés vont atteindre les 1000 milliards de dollars à l'horizon 2024 tandis qu'ils étaient de 622 milliards de dollars en 2020 et de 568 milliards de dollars en 2019 (GlobalData, juin 2021).

Aujourd'hui, Internet et les objets connectés ont changé la vie des individus, en la rendant plus facile (Weydert et al., 2019). En effet, Internet offre aux utilisateurs la possibilité de partager de grandes quantités d'informations dans des environnements riches en multimédia (à savoir les plateformes en ligne), ce qui permet de collecter et d'utiliser les données des consommateurs et d'améliorer les revenus marketing des entreprises (McAfee et Brynjolfsson 2012 ; Schumann et al., 2014). En naviguant sur le net, les individus divulguent non seulement des paramètres démographiques personnels, mais également de nombreux faits, expériences et opinions personnels d'une manière volontaire ou involontaire (Weydert et al., 2019).

La divulgation d'informations personnelles en ligne est au cœur des interactions commerciales entre les consommateurs et les entreprises (Stead et al., 2001 ; Maury et al., 2002). Au fur et à mesure que le commerce électronique s'est développé, la taille des empreintes numériques que les consommateurs laissent a augmentée. Les entreprises modernes utilisent ces informations pour mettre en œuvre des stratégies marketing interactives qui permettent d'accentuer leur efficacité en proposant des offres plus ciblées et personnalisées (Hofackeret al., 2015). Ashworth et Free (2006) ainsi montrent que la surveillance du comportement des consommateurs sur le Web est importante pour les entreprises car de nombreux modèles de commerce électronique sont construits autour des données fournies par les consommateurs.

À l'ère des Big data et dans des environnements de plus en plus connectés, les avis des internautes concernant leurs données personnelles sont divergents : certains consommateurs acceptent facilement de partager leurs données personnelles en ligne, notamment en contrepartie de divers avantages, tandis que d'autres sont plus réticents à l'idée de divulguer des informations privées (Kose et Sert, 2016). En effet, la littérature sur les données souligne que de nombreux consommateurs fournissent des informations en échange d'un accès à des contenus, de remises, de récompenses et d'autres avantages. Les récompenses, en particulier, semblent jouer un rôle essentiel dans l'augmentation de la volonté des utilisateurs de partager des informations privées (Mazurek et al., 2019). La plupart des consommateurs sont conscients d'être surveillés par des entreprises et perçoivent cela comme le coût de la participation au monde numérique (Acquisti, 2004 ; Acquisti et al., 2005, 2015, 2016). Rober et al. (2015) ont montré que les individus sont plus susceptibles de partager leurs données personnelles une fois qu'ils reçoivent un avantage de nature monétaire, des services sur mesure, des remises, des offres ciblées et personnalisées.

A l'inverse, les préoccupations concernant la vie privée des utilisateurs en ligne et sa protection ont considérablement augmenté (Karat et al., 2005 ; Mantelero, 2016). La littérature indique que les internautes sont susceptibles de fournir des informations incomplètes ou inexactes en réponse à des préoccupations accrues en matière de confidentialité (Milne et Boza, 1999 ; Sheehan et Hoy, 1999). Les problèmes liés à la confidentialité des informations personnelles sont donc considérés comme l'un des principaux obstacles à la croissance du commerce électronique (Hann et al., 2007 ; Son et al., 2008).

Une étude réalisée par BDM en 2023 a montré que 9 français sur 10 ont des préoccupations concernant la protection de leurs données personnelles partagées en ligne. De plus, les résultats du sondage mené par Boris Benès en 2023 affirment qu'ils utilisent des solutions pour protéger leurs données présentes sur le Web comme la désactivation de la géolocalisation (44%) ou la navigation privée (25%). Les problèmes liés aux données personnelles peuvent même parfois donner lieu à de gigantesques scandales mondiaux. Le meilleur exemple est celui de Cambridge Analytica qui a collecté des informations personnelles sur environ 87 millions d'utilisateurs de Facebook sans leur consentement explicite dans le but de cibler des messages favorables au profit de Donald Trump aux États Unis (Degirmenci, 2020). Ces problèmes, comprenant des dimensions techniques et juridiques (Workman et al., 2008 ; Anderson et Agarwal, 2010 ; Davinson et Sillence, 2010), ont amené le parlement européen à légiférer en proposant en 2016 un règlement pour responsabiliser les organismes à la collecte et au traitement des données personnelles : le RGPD (Règlement Général sur la Protection des Données).

A ce niveau, nous pouvons dire que l'incertitude liée aux informations personnelles en ligne et à leurs utilisations est susceptible d'entrainer une perte contrôle qui crée un déséquilibre entre l'entreprise qui collecte les données et l'individu qui les partage. Ceci développe chez les internautes des sentiments d'impuissance et donc un état de vulnérabilité. Or, la vulnérabilité des internautes face à leurs données personnelles restent peu étudiée (Martin et al., 2017). Ainsi, l'objectif de notre recherche est d'étudier les liens entre la vulnérabilité liée au données personnelles partagées en ligne et son antécédent, à savoir la peur de rater quelque chose. Notre recherche cherche également à déterminer l'effet de cette vulnérabilité sur les conséquences comportementales des internautes suite au partage de données personnelles en ligne, à savoir le changement de site Web. Cet article est, ainsi, organisé comme suit. Tout d'abord, nous présentons une revue de la littérature sur la vulnérabilité des internautes suite au partage de données personnelles en ligne, son antécédent à savoir la peur de rater quelque chose (FOMO) et sa conséquence à savoir le changement de site Web. Ensuite, nous présentons les hypothèses suivies de la méthodologie de recherche appliquée et la discussion des résultats. Enfin, nous clôturons cet article par la présentation des implications, les limites et les voies futures de recherche.

1. Revue de la littérature

1.1. La vulnérabilité des internautes suite au partage de données personnelles en ligne

Le concept de la vulnérabilité tire son origine du mot latin Vulnus, qui signifie « blessure », et à la capacité de souffrance inhérente à l'incarnation humaine. Être vulnérable, c'est être fragile, susceptible de se blesser et de souffrir. Cette susceptibilité est une condition ontologique de la qualité humanité, « *un aspect universel, inévitable et durable de la condition humaine* » (Fineman, 2008, p.8). La vie humaine est conditionnée par la vulnérabilité. En tant qu'êtres sociaux et affectifs, nous sommes vulnérables aux autres de façons différentes : à la perte et au chagrin, à la négligence, au rejet, à l'ostracisme et à l'humiliation (Mackenzie et al., 2014).

Plusieurs définitions du concept de la vulnérabilité sont identifiées dans la littérature. En effet, Chambers (1989) a défini la vulnérabilité comme une variable qui fait référence au stress et à la difficulté de le gérer. Tuner et al. (2003) ont défini la vulnérabilité comme une mesure dans laquelle un système, un sous-système ou une composante du système est susceptible de subir des dommages du fait de l'exposition à un danger, qu'il s'agisse d'une perturbation ou d'un facteur de stress. De plus, Adger (2006) a montré que la vulnérabilité est l'état de sensibilité aux dommages résultant d'une exposition au stress associée aux changements environnementaux et sociaux et à l'absence de capacité d'adaptation. Le concept de vulnérabilité a fait l'objet de débats et discussions dans de multiples contextes, notamment politique (Held, 1987), bioéthique (Kemp, 1999), médical (Lee et al., 1999) ou encore climatique (Omolo et al., 2018).

À partir de travaux pluridisciplinaires sur la vulnérabilité et dans une tentative de synthèse des travaux existants, Baker et al. (2005, p.134) proposent une définition communément admise dans la littérature. Selon eux, *« la vulnérabilité des consommateurs est l'impuissance qui découle d'un déséquilibre dans les interactions du marché ou de la consommation de messages et de produits de marketing. Cela se produit lorsque le contrôle n'est pas entre les mains d'un particulier, créant ainsi une dépendance à l'égard de facteurs externes afin de créer une équité sur le marché. La vulnérabilité réelle découle de l'interaction d'états, de caractéristiques individuelles et de conditions externes dans un contexte où les objectifs de consommation peuvent être entravés et où l'expérience affecte les perceptions personnelles et sociales de soi* ». Selon Baker et al. (2005), tout le monde a le potentiel d'être vulnérable. Pour conceptualiser l'expérience de vulnérabilité des consommateurs, Baker et al. (2005) ont proposé un modèle qui montre différents éléments qui peuvent aboutir à la création de l'expérience de vulnérabilité des consommateurs. Ainsi, les déterminants déclenchant la vulnérabilité des consommateurs sont divisés en trois catégories, dont deux sont internes, les caractéristiques individuelles et les états individuels, tandis que le troisième est externe avec les facteurs en dehors de la sphère personnelle d'influence ou de contrôle du client (Baker et al., 2005). Le modèle illustre également les résultats de l'expérience de la vulnérabilité sur le consommateur. La vulnérabilité peut avoir un impact sur la perception de soi actuelle et future de l'individu (Baker et al., 2005) ou conduire à l'inconfort social et à l'exclusion des clients (Beudaert et al., 2017).

Dans un monde de plus en plus connecté, le suivi continu et omniprésent de nos activités en ligne a lancé des débats publics et universitaires sur les Big data, la confidentialité et l'équité (Bol et al., 2020). Les opportunités d'exploiter les grandes quantités de données personnelles

que nous produisons en ligne sont énormes. Les utilisateurs, bien que soucieux de leur vie privée, apprécient dans le même temps les avantages d'une publicité et d'un contenu plus pertinents par rapport à leurs besoins (Aguirre et al., 2016 ; Strycharz et al., 2018). Mais les consommateurs peuvent croire que les nouvelles technologies facilitent les pratiques d'exploitation et augmentent ainsi leurs chances d'être victimes (Ratchford et Barnhart, 2012). La recherche de Elms et Tinson (2012) a souligné que la technologie rend également les consommateurs vulnérables. Xu (2012) a affirmé que l'augmentation de l'utilisation d'Internet a conduit à une énorme quantité de données personnelles partagées et stockées en ligne qui peuvent être utilisées à différentes fins et par différentes parties. Ceci remet en question la gestion des informations personnelles et la notion de confidentialité. Pour résoudre ce problème, Gundecha et al. (2011) ont montré que la majorité des sites Web offre aux utilisateurs plusieurs paramètres de confidentialité pour protéger leurs informations personnelles partagées en ligne. Ils ont également montré que ces paramètres sont souvent mal expliqués aux utilisateurs. Dans cette recherche doctorale, nous soutenons l'idée que cette situation peut mettre les utilisateurs d'Internet face à des violations de leur vie privée, d'où la création d'un sentiment de vulnérabilité en ligne.

Gundecha et al. (2011) ont montré qu'à mesure du développement technologique, les problèmes de protection de la vie privée vont au-delà des préoccupations de la vie privée et rendent les utilisateurs plus vulnérables aux attaques en ligne. D'ailleurs, les menaces sont considérées comme des facteurs critiques car elles introduisent des altérations indésirables (Choudhary et al., 2018). Les activités en ligne peuvent donc exposer les utilisateurs à différentes situations de vulnérabilité en ligne, telles que l'utilisation abusive des données, le vol d'identité, le harcèlement en ligne et l'exposition à des contenus inappropriés (Boyd et Ellison, 2008).

La vulnérabilité en ligne est définie comme la capacité de subir des préjudices pour la réputation et le bien-être psychologique ou physique en raison des risques rencontrés lors de la participation à des activités en ligne (Davidson et Martellozzo, 2013). Selon Atiso et al. (2018), la vulnérabilité en ligne est utilisée pour désigner les différentes escroqueries auxquelles les utilisateurs peuvent être exposés (par exemple, des escroqueries commerciales ou amoureuses). Les risques en ligne peuvent prendre de nombreuses formes (Hasebrink et al., 2011), notamment les menaces liées à la confidentialité des données, les rumeurs en ligne, le cyber-harcèlement et l'exposition à des contenus inappropriés et indésirables (Boyd et Ellison, 2008).

La vulnérabilité en ligne a été une source fréquente de débats dans la littérature académique (Staksrud et al., 2013 ; Wilcox et Stephen, 2013) et dans la presse populaire (BBC News, 2015 ; New York Times, 2014). Selon Warner et al. (2019), il est souvent difficile pour les individus d'évaluer les risques potentiels pour leurs données personnelles en ligne, et d'estimer la valeur de ces données. Les individus peuvent donc être vulnérables lorsqu'ils se dévoilent en ligne, puisque leurs données personnelles peuvent être facilement mal interprétées, utilisées à mauvais escient, divulguées et même vendues à des tiers (Riegelsberger et al., 2009). Dinev et Hart

(2004) ont montré que les internautes sont régulièrement exposés à des risques d'abus sur les informations qu'ils divulguent en ligne, ce qui peut augmenter leur perception de vulnérabilité.

Staksrud et al. (2013) suggèrent que le simple fait d'être un utilisateur d'Internet (par exemple en utilisant les réseaux sociaux) ne rend pas une personne susceptible à la vulnérabilité en ligne. Ils ont montré que la vulnérabilité dépend plutôt de la manière dont une personne interagit avec le site Web utilisé. Ainsi, l'exposition de soi et l'obtention de plusieurs réseaux en même temps contribuent à la création de la vulnérabilité en ligne (Staksrud et al., 2013 ; Buglass et al., 2016). Les pratiques quotidiennes en ligne rendent les internautes potentiellement vulnérables, avec des risques de confidentialité posés non seulement par le partage d'informations personnelles, mais aussi par la génération de toute information qui distingue une personne d'une autre, comme l'utilisation ou le partage de données qui associent un identifiant d'appareil à une personne, ce qui pourrait être utilisé pour « *ré-identifier des données anonymes* » (Politou et al., 2018, p.3).

Plus spécifiquement, Martin et al. (2017) définissent la vulnérabilité liée aux données comme une construction composite comprenant (1) l'insécurité, qui est une forme d'instabilité ; (2) l'exposition, comme la peur de révéler quelque chose de privée ; (3) la menace lorsqu'une intention d'infliger des dommages à quelqu'un est perçue ; (4) la susceptibilité, ou la probabilité d'être influencé par quelque chose de particulier ; et (5) la vulnérabilité, ou la possibilité d'être blessé. Martin et al. (2017) ont indiqué que même lorsque les dommages subis par les internautes sont minimes, cela augmente la perception de la vulnérabilité liée aux données personnelles partagées en ligne. Toutefois, les sites Web qui utilisent la transparence peuvent atténuer les effets dommageables de tous les types de vulnérabilité des internautes (Martin et al., 2017). La vulnérabilité liée aux donnes personnelles partagées en ligne intervient lorsque les entreprises ont accès aux données personnelles d'un client (Martin et al., 2017). Ce simple accès signifie que les entreprises disposent de « *dossiers numériques détaillés sur les personnes* » et peuvent s'engager dans un « *transfert d'informations à grande échelle entre diverses entités* » (Solove, 2003, p.2). Dans le but de réduire leur vulnérabilité liée aux données personnelles, les internautes limitent comment et avec qui ils partagent leurs données personnelles en ligne (Acquisti et al., 2012).

Les recherches qui ont étudié la vulnérabilité liée aux données personnelles partagées en ligne sont rares, la littérature ayant surtout investigué la notion plus globale de vulnérabilité en ligne, notamment dans le contexte de l'utilisation des médias sociaux (Sibona et Walczak, 2011 ; Atiso et al., 2018 ; Banerjee, 2019 ; Choudhary et al., 2018 ; Warner et al., 2019). Par exemple, Livingstone et al. (2007) ont conclu que des facteurs tels que le sexe et l'efficacité numérique contribuent à la vulnérabilité des jeunes internautes, lorsqu'il s'agit d'un groupe qui possède une faible capacité de gérer les informations personnelles en ligne.

Pour conclure, nous pouvons dire que l'incertitude liée aux informations personnelles en ligne et à leurs utilisations est susceptible d'entrainer une perte contrôle. Cela contribue à la création d'un déséquilibre entre l'entreprise qui collecte les données et l'individu qui les

ISSN : 2724-7260
Volume 4 : Numéro 2

partage, qui peut générer des sentiments d'impuissance et de la vulnérabilité chez les internautes. Or, la vulnérabilité des internautes en lien avec leurs données personnelles reste peu étudiée dans la littérature (Martin et al., 2017). Notre objectif sera donc de déterminer les facteurs qui entrainent la vulnérabilité des internautes suite au partage de données personnelles en ligne et d'étudier ses conséquences.

1.2. La peur de rater quelque chose (FOMO)

La peur de rater quelque chose (ou Fear of Missing Out, FOMO) a été introduite pour la première fois dans les médias au début des années 2010 (Fake, 2013 ; Morford 2010). À cette période, l'utilisation des médias sociaux avait connu une croissance exponentielle dans le monde, si bien que les chercheurs se sont intéressés à l'idée que les individus peuvent avoir des appréhensions de rater des choses sur ce qui se passe en ligne (Hitlin, 2018 ; Poushter et al., 2018). Wortham (2011) a défini le FOMO comme « un sentiment de malaise et parfois dévorant que vos pairs font, savent ou possèdent plus ou quelque chose de mieux que vous ». Le FOMO a également été définit comme « *une appréhension omniprésente que d'autres pourraient vivre des expériences enrichissantes dont on est absent* » (Przybylski et al., 2013, p.1). Cette peur de rater quelque chose est vue comme un nouveau type de dépendance qui pousse les individus à passer beaucoup plus de temps en ligne car ils craignent de passer à côté de certains développements et de ne pas être informés des nouveautés sur Internet et plus précisément sur les réseaux sociaux (Przybylski et al., 2013 ; Dossey, 2014 ; Buglass et al., 2017 ; Oberst et al., 2017).

Une discussion théorique approfondie sur les définitions menées par Reagle (2015) a identifié l'envie comme un élément clé de FOMO. Ainsi, FOMO implique une comparaison de l'individu entre sa propre situation ou expériences et ce que les autres font et vivent. Il semble donc très plausible que les personnes ayant une orientation de comparaison sociale élevée puissent développer le sentiment de FOMO car elles s'exposent plus souvent aux informations que les autres communiquent sur elles-mêmes, y compris les informations sur leurs activités et expériences.

Le FOMO est également lié à la nouveauté : recevoir de nouvelles informations qui deviennent une source de gratification pour les utilisateurs (Hetz et al., 2015). La peur de rater quelque chose est donc un construit social lié au manque d'accès à diverses formes d'informations (Hetz et al., 2015). Le FOMO est associé à d'autres mécanismes liés aux médias électroniques tels que le multitâche (Reinecke et al., 2017), la pression de l'information (Barber et Santuzzi, 2017), les problèmes de santé mentale (Wiederhold, 2017) en encore des changements de comportement engendrés par l'utilisation d'Internet (Fox et Moreland, 2015). Le FOMO est ainsi fortement associé à l'utilisation des nouvelles technologies et à la peur du jugement des autres (Tomczyk et al., 2018). Le FOMO suppose également des éléments tels que le désir d'être populaire, la peur du rejet et le besoin d'appartenance à des communautés virtuelles (Beyens et al., 2016). Le FOMO est associé à la dépendance aux services en ligne et à l'attachement aux smartphones (Przybylski et al., 2013 ; Alt, 2015 ; Beyens et al., 2016 ; Tras

et Oztemel, 2019 ; Yin et al., 2021). En outre, le FOMO s'est avéré prédire les comportements problématiques d'utilisation des médias, tels que l'utilisation excessive des smartphones (Elhai et al., 2016 ; Fuster et al., 2017), la dépendance aux médias sociaux (Blackwell et al., 2017) ou la communication Internet (Wegmann et al., 2017).

Le FOMO se compose principalement de deux traits psychologiques : le désir d'appartenance et l'anxiété de l'isolement (Beyens et al., 2016). La peur de rater quelque chose peut se matérialiser de différentes façons. Abel et al. (2016) suggèrent d'appréhender le phénomène en termes de vérification impulsive des ressources en ligne. Przybylski et al. (2013) situent le FOMO davantage dans le domaine des comportements sociaux, des relations avec les autres et de la qualité de ces relations.

Plusieurs chercheurs ont focalisé leurs travaux sur la relation entre l'utilisation excessive d'Internet et le FOMO. Les recherches ont montré que les utilisateurs excessifs d'Internet et des médias sociaux passent de moins en moins de temps hors ligne pour participer à des activités réelles, ce qui provoque cette crainte de rater des choses lorsqu'ils ne sont pas en ligne (Duvenage et al., 2020). Ainsi, le FOMO est lié à un fort besoin de rester en ligne, de recevoir des messages, de participer passivement ou activement à l'échange d'informations via les services Internet. Ne pas répondre à ce besoin entraine des conséquences négatives chez les internautes (Hetz et al., 2013). Dans cette recherche, nous postulons que cela peut impacter la vulnérabilité liée au données personnelles.

En effet, une utilisation excessive d'Internet dans des pratiques telles que la présentation de soi et la participation à des réseaux sociaux peut rendre les utilisateurs plus vulnérables à divers dangers (Staksrud et al., 2013 ; Buglass et al., 2016). Comme nous l'avons évoqué précédemment, la vulnérabilité en ligne est définie comme la tendance d'un individu à subir des dommages qui portent atteintes à son bien-être et à sa réputation (Davidson et Martellozzo, 2012). Dans la mesure où le FOMO favorise l'exposition de soi en ligne, cela offre aux individus de nouvelles opportunités d'être confrontés à une vulnérabilité en ligne (Buglasss et al., 2016). Les individus ayant peur de rater des évènements et des informations en ligne pourraient se tourner vers des comportements d'autopromotion afin de renforcer un sentiment d'appartenance, ce qui engendre un partage accru d'informations personnelles et donc une vulnérabilité liée aux données plus importantes (Varchetta et al. (2020). Sur cette base, nous proposons l'hypothèse suivante :

H1 : Le FOMO influence positivement la vulnérabilité des internautes suite au partage de données personnelles en ligne

1.3. Le changement de comportement des internautes

Roos (1999) décrit le changement de comportement comme les clients qui ont partiellement ou totalement changé de fournisseur. Bansal et Taylor (1999, p.203) ont présenté le changement de services comme « *le remplacement ou l'échange du fournisseur de services actuel par un autre fournisseur de services* ». Le changement a été défini comme « un comportement final où

ISSN : 2724-7260
Volume 4 : Numéro 2

le fournisseur (ou le client) se substitue à une autre alternative » (Tahtinen et Halinen, 2002, p.183).

Le changement de comportement de consommateur fait référence à la décision volontaire d'un consommateur de passer d'une option existante à une nouvelle option. Il s'agit d'un phénomène répandu qui peut se produire entre les marques ou au sein d'une même marque (Jiang et al., 2014). En général, le changement de comportement des consommateurs peut s'expliquer par deux types de motifs : l'utilité et le processus. Le changement de comportement axé sur l'utilité postule que les consommateurs changent de produits et/ou de services parce qu'ils s'attendent à ce que la nouvelle option leur apporte une plus grande utilité que l'option en place (Lam et al., 2010). Le changement de comportement axé sur le processus suggère que le processus de prise de décision de changement offre certains avantages psychologiques au consommateur. Dans certaines situations, le consommateur prend même la décision de changement indépendamment de son résultat (Su et al., 2017). Par exemple, les consommateurs modifient parfois leurs choix de consommation simplement pour faire preuve de souplesse dans leurs règles de décision (Drolet, 2002).

La recherche sur le changement de comportement des consommateurs s'est largement concentrée sur la façon dont différents facteurs incitent au changement en augmentant l'utilité attendue de la nouvelle option (Dodson et al.,1978 ; Van et al., 1996), et en diminuant l'utilité de l'ancienne option (Bougie et al., 2003 ; Inman et Zeelenberg 2002), ou les deux (Grover et Srinivasan 1992 ; Deighton et al., 1994). De nombreuses études ont été menées dans une multitude de secteurs, comme les services d'assurance automobile (Antón et al., 2007), les services de réparation automobile et de coiffure (Bansal et al., 2005) ou encore les services de téléphonie fixe (Lopez et al., 2006). A titre d'illustration, Keaveney (1995) a proposé de classer huit catégories de facteurs affectant le changement de comportement des clients : la tarification, les pannes de service, l'attraction par les concurrents, les échecs de rencontre de services, les récupérations de service médiocres, la gêne, l'éthique, la concurrence et les situations involontaires.

Le développement du commerce électronique a généré une grande disponibilité de fournisseurs en ligne qui ont amené les utilisateurs à passer plus fréquemment et plus librement d'un fournisseur de services en ligne à un autre (Bhattacherjee et al., 2012). Ainsi, « *passer à un service en ligne concurrent est presque aussi simple que de télécharger et d'installer, ou de remplir un formulaire d'inscription en ligne* » (Bhattacherjee et al., 2012, p.327). Au cours des dernières années, les chercheurs ont étudié le changement de comportement dans de multiples contextes en ligne, tels que les navigateurs Web (Ye et al., 2008), les portails de collecte de données en ligne (Kim et Son, 2009), les achats en ligne (Zhou, 2014), les réseaux sociaux (Wu et al., 2014), les jeux en ligne (Hou et al., 2011), les e-mails (Kim et al., 2006) ou encore les blogs (Zhang et al., 2009).

Dans certaines études, le changement de comportement est considéré comme le résultat d'une détérioration de la fidélité des consommateurs (Yang et Peterson, 2004 ; Wang et al.,

ISSN : 2724-7260
Volume 4 : Numéro 2

2011 ; Valvi et Fragkos, 2012). De telles études suggèrent qu'une amélioration de diverses caractéristiques de service augmentera la satisfaction des consommateurs qui, à son tour, fidélisera les consommateurs et les empêchera de changer de fournisseur (Lui et al., 2016). Par exemple, si une entreprise fournit une qualité constante mais terne, les consommateurs peuvent perdre leur intérêt initial et changer lorsque des produits plus attractifs sont proposés par des concurrents (Jones et Sasser, 1995). Ce phénomène peut devenir plus visible lorsqu'une innovation technologique émerge (Lui et al., 2016).

Le cadre Push-Pull-Mooring (PPM) est un paradigme dominant dans la littérature sur la migration humaine qui décrit pourquoi les individus se déplacent d'un endroit à un autre (Boyle et al., 1998 ; Bansal et al., 2005). Le cadre PPM s'est par la suite étendu à d'autres disciplines, notamment le marketing pour comprendre le changement de comportement de la clientèle (Bansal et al., 2005 ; Hou et al., 2011). Le cadre PPM comprend trois facteurs : les effet d'incitation, les effets d'attraction et les effets d'amarrage (Wang et al., 2019). Les effets d'incitation et d'attraction, représentent la force agrégée des perceptions d'un fournisseur historique et d'un fournisseur alternatif. Les effets d'amarrage reflètent l'influence agrégée des conditions situationnelles et contextuelles. L'application de ce cadre théorique au comportement des consommateurs reflète la similitude évidente entre les individus migrants d'un endroit à un autre et le changement des consommateurs d'un produit ou service à un autre. Hou et al. (2011), Hsieh et al. (2012), Zhang et al. (2012) ou encore Xu et al. (2013) ont appliqué ce paradigme PPM au niveau de la compréhension du changement de services électroniques. En étudiant les jeux de rôle en ligne, Hou et al. (2011) ont par exemple constaté que les facteurs d'amarrage et d'attraction ont une influence significative sur l'intention de changement par rapport aux facteurs d'incitation. De plus, Hsieh et al. (2012) ont étudié le passage des utilisateurs des blogs à Facebook, et ont constaté que les facteurs d'attraction, d'incitation et d'amarrage ont tous une influence significative sur l'intention de changer de comportement.

De nombreux chercheurs ont montré que les préoccupations liées à la vie privée entrainent un changement de site Web (Dewan et Chen, 2005 ; Son et Kim, 2008 ; Slade et al., 2015). Par exemple, dans le cadre de paiements en ligne, les utilisateurs peuvent passer à d'autres sites Web s'ils pensent que le fournisseur en place n'est pas en mesure de protéger correctement leurs informations personnelles (Wang et al., 2019). Selon Slade et al. (2015), plus les internautes effectuent des paiements en ligne, plus leurs préoccupations liées à la vie privée augmentent, et plus la tendance à changer de site Web augmente. Nous pensons qu'un raisonnement similaire peut être appliqué à notre recherche : plus un consommateur se sent vulnérable sur un site Web par rapport à ses données personnelles, plus il aura tendance à vouloir changer de site. Toutefois, si les études antérieures sur la relation entre les préoccupations liées à la vie privée et le changement de comportement (site Web visité) sont nombreuses, les études sur la relation entre la vulnérabilité et le changement de comportement sont rares (Martin et al., 2017). Ainsi, nous proposons de tester la relation entre la vulnérabilité suite au partage de données personnelles en ligne et le changement de site Web. Nous proposons donc l'hypothèse suivante :

H2 : La vulnérabilité suite au partage de données personnelles en ligne a un effet positif sur le changement de comportement des internautes (site Web)

Le modèle théorique global (voir Figure 1) qui intègre nos hypothèses et qui est testé dans cette étude vise donc à intégrer la littérature soutenant le rôle de la peur de rater quelque chose comme un antécédent de la vulnérabilité des internautes suite au partage de données personnelles en ligne, avec l'idée que ce lien a un effet positif sur le comportement des internautes en ligne.

2. Méthodologie de la recherche

2.1. Les mesures

Différentes échelles destinées à mesurer les variables de notre modèle ont été sélectionnées à partir des travaux antérieurs, traduites et adaptées parfois au contexte de cette étude. Les items utilisés dans notre enquête quantitative ont été mesurée sur l'échelle de Likert qui demeure traditionnellement la plus utilisée en sciences de gestion et offre un traitement statistique de qualité et une grande richesse d'analyse (Evrard et al., 2009). L'échelle Likert permet au répondant d'indiquer son opinion ou son attitude pour chaque proposition sur un continuum entre un pôle négatif (pas du tout d'accord) et un pôle positif (tout à fait d'accord).

Notre questionnaire en ligne comprenait une série d'échelles préétablies, des données démographiques sur l'échantillon et des mesures spécifiques à l'étude.

Données démographiques de l'échantillon : Quatre questions portant sur le genre des répondants, leurs âges, la catégorie socioprofessionnelle et le pays d'origine.

La vulnérabilité des internautes : Nous avons utilisé l'échelle de mesure de la vulnérabilité liée aux données de Martin et al. (2017) composée de cinq items. Il a été demandé aux participants d'indiquer leur sentiment concernant les informations que l'entreprise possède à leur sujet (par exemple « insécurité »). Les réponses à chaque item variaient de « pas du tout d'accord » à « tout à fait d'accord ».

La peur de rater quelque chose : Le FOMO se base sur une échelle de dix items qu'utilise la majorité des recherches menées dans le domaine de l'utilisation d'Internet et des réseaux sociaux (Riordan et al., 2020 ; Rozgonjuk et al., 2021 ; Tomczyk et al., 2018). Nous ajoutons que Buglass et al. (2017) ont étudié la relation entre la vulnérabilité en ligne et le FOMO en utilisant l'échelle de Pryzbylski et al. (2013). Nous avons opté donc pour cette échelle de mesures. Il a été demandé aux participants d'indiquer leurs d'accord ou de désaccord sur les différents items de l'échelle de mesure.

Le changement de comportement des internautes : Le changement caractérise une forme de migration de l'internaute vers un autre site web pour une ou plusieurs des raisons. Pour mesurer le changement de site Web, nous avons utilisé l'échelle de mesure de Palmatier et al. (2007) qui a été mobilisée par plusieurs chercheurs dans le contexte du partage de données personnelles en ligne (Martin et al., 2016). Cette échelle de mesure comporte trois items. Il a été demandé

aux participants d'indiquer leur comportement si un autre site propose le même produit / service mais ne collecte pas de données sur leurs activités en ligne. Les réponses étaient ancrées sur une échelle de Likert à 5 points allant de 1 (Pas du tout d'accord) à 5 (Tout à fait d'accord), les scores les plus élevés indiquant une plus grande propension.

2.2. Echantillon et collecte de données

Le processus d'échantillonnage a commencé par la détermination de la population, qui regroupe « l'ensemble des éléments ou objets qui regroupe les informations recherchées » (Malhotra et al., 2004, p.7). Pour notre recherche, il s'agira des utilisateurs d'Internet. Pour notre travail, nous avons adopter la procédure d'échantillonnage non probabiliste pour sonder une partie de la population des utilisateurs d'Internet en France et en Tunisie. La méthode choisie est celle de l'échantillonnage de convenance.

Différentes recommandations de seuils ont été présentées au niveau de la littérature. Par exemple, Hair et al. (1985) a proposé pour une analyse par la méthode des équations structurelles un échantillon de taille minimale de 100 à 150 individus. Néanmoins une taille de 200 à 300 répondants serait l'idéal. Selon Sörbom et Jöreskog (1989), la taille de l'échantillon doit être égale à 10 fois le nombre de variables observables. Hair et al. (1998), Igalens et Roussel (1998) et Roussel (2005) ont montré que la taille peut être comprise dans un intervalle de 5 à 10 fois le nombre d'items présents dans l'étude. En nous basant sur la dernière fourchette de choix, nous avons décidé d'arrêter la diffusion de notre questionnaire lorsque nous aurons atteint au moins 375 répondants (75 items*5). La durée de collecte s'est étalée sur cinq mois environ à partir d'Avril 2022. Une description de notre échantillon est détaillée dans le tableau 1.

2.3. Analyse de données

Nous avons commencé, dans un premier lieu, par la vérification de la dimensionnalité et de mettre en évidence la fiabilité des mesures. L'ACP est une méthode de la famille des analyses multivariées, qui consiste à transformer des variables liées entre elles (dites « corrélées ») en nouvelles variables décorrélées les unes des autres. Ces nouvelles variables sont nommées composantes principales ou axes principaux. Elle permet de résumer l'information en réduisant le nombre de variables. Dans ce qui suit, nous allons présenter et analyser l'ensemble des résultats obtenus pour chaque échelle de mesure des variables retenues.

Pour tester FOMO, nous avons utilisé une échelle de mesure unidimensionnelle de 10 items. Les résultats de l'ACP montrent que les deux items affichaient des communalités assez faibles (en dessous de 0.4). Nous avons ainsi procédé à une rotation « Varimax ». Le résultat obtenu étant presque similaire, ceci nous a amené à écarter ces deux items. Après épuration, l'ACP présente un seul facteur restituant 41.925 % de la variance. La structure factorielle obtenue est présentée dans le tableau ci-dessous. Tous les items ont une communalité supérieure à 0.5 et la fiabilité respecte les normes requises (α= .855).

Revue Internationale Multidisciplinaire
D'Economie et de Gestion
ISSN : 2724-7260
Volume 4 : Numéro 2

Pour mesurer la vulnérabilité des internautes suite au partage de données personnelles en ligne, nous avons utilisé une échelle de mesure unidimensionnelle composé de cinq items. Les résultats de la purification de cette échelle de mesure via l'ACP montrent un seul facteur restituant 61.714 % de la variance. Les communalités sont supérieures à 0.5 et les corrélations des items avec le construit sont supérieures à 0.7. L'alpha de Cronbach est satisfaisant (0.842). Les items sont ainsi conservés pour le test final.

Pour mesurer le changement de site Web, nous avons utilisé une échelle de mesure unidimensionnelle composée de trois items. Les résultats de l'épuration de l'échelle de mesure révèlent une faible corrélation (inférieur à 0.4) d'un seule item (0.388), que nous avons donc éliminé.

L'analyse factorielle exploratoire (AFE) étant achevée et la structure factorielle de nos construits définie, il convient de faire le point sur la validité de ces construits avant de passer à l'ultime étape du test des hypothèses de la recherche. La réalisation d'une analyse factorielle confirmatoire requiert de la part des chercheurs le recours à des méthodes d'analyse de données de deuxième génération qu'on appelle méthodes d'équations structurelles (Akrout, 2010 ; Wong, 2013 ; Akrout, 2018). Nous réaliserons cette étape en recourant au logiciel AMOS23. L'examen des différents indices montre que le modèle est acceptable et qu'il ajuste suffisamment bien par rapport aux données empiriques, puisque la majorité des indices coïncide avec les seuils critiques fixés. Le tableau suivant synthétise l'ensemble des résultats obtenus :

Tableau 2 : La qualité d'ajustement du modèle de structure

Indices	Khi deux	Khi deux/ddl	DL	GFI	AGFI	RMR	RMSEA	TLI	NFI	CFI
Valeurs	780,368	2,098	372	0,883	0,853	0,060	0,052	0,894	0,839	0,909

Après avoir vérifié la qualité d'ajustement, nous interprétons dans cette partie les paramètres d'estimations du modèle de mesure partiel récapitulés dans le tableau suivant :

Tableau 3 : Résultats d'estimation du modèle de mesure

	Rho de Jöreskog	VME
Vulnérabilité	0,821	0,482
FOMO	0,517	0,497
Changement de site Web	0,787	0,650

La validité convergente teste si les concepts censés être liés le sont effectivement. C'est la capacité d'une mesure à converger vers les résultats obtenus d'autres mesures du même construit. Dans le cas de mesure unique pour le construit, la validité convergente renvoie à la capacité des items à mesurer une même variable (Roussel et Wachew, 2005). Pour Fornell et Larcker (1981), un construit possède une validité convergente satisfaisante lorsque sa VME affiche une valeur supérieure à 0.5. Cependant, des valeurs légèrement inférieures à 0,5 (mais

proches de cette valeur), mais ayant des coefficients de fiabilité élevés (alpha de Cronbach ; Rhô de Jöreskog), demeurent acceptables (Fornell et Larker, 1981). Pour notre présent travail, les valeurs des VME sont toutes supérieures à 0.5.

La validité discriminante teste si les concepts ne devant avoir aucun lien n'en ont effectivement pas. C'est un critère d'appréciation d'un instrument de mesure pour lequel les indicateurs mesurant des phénomènes différents sont faiblement corrélés. C'est aussi la capacité d'une mesure à générer des résultats différents des mesures d'autres construits (Roussel et Wachew, 2005). Pour Fornell et Larcker (1981), pour évaluer la validité discriminante, il faut vérifier que la VME est supérieure au carré des corrélations entre le construit et les autres construits du modèle ou vérifier que la racine carrée de la VME est supérieure à toutes les corrélations entre le construit et les autres construits du modèle. D'après les résultats présentés dans le tableau suivant (Tableau 3), les racines carrées des VME sont supérieures aux différents liens structurels, ce qui confirme que la validité discriminante de notre modèle de mesure est vérifiée.

Tableau 4 : validité discriminante du modèle de mesure

	Vulnérabilité	FOMO	Changement de site Web
Vulnérabilité	0,694		
FOMO	0, 149	0,704	
Changement de site Web	0, 233	0,189	0,806

2.4. Vérification des hypothèses et discussion de résultats

Nous avons postulé une relation entre FOMO et la vulnérabilité suite au partage de données personnelles en ligne. Les résultats de notre recherche nous ont permis de confirmer notre hypothèse (H1) et montrent donc qu'une augmentation du FOMO influence positivement le développement de la vulnérabilité suite au partage de données personnelles en ligne ($\beta = 0{,}156$). Autrement dit, plus l'internaute a un sentiment de peur de rater quelque chose, plus il développe une vulnérabilité liée aux données personnelles. Les améliorations technologiques ont rendu la réception d'informations plus facile, plus instantanée et plus addictive que jamais. Pour ne pas rater quelque chose en ligne, les internautes sont prêts à tout et ce, même si cela se fait au détriment de leurs intérêts. FOMO pousse les internautes à partager davantage leurs données personnelles en ligne afin de satisfaire leur désir d'appartenance sociale. Le fait d'accepter de tout partager en ligne peut mettre les internautes dans des positions fragiles qui permettent de développer de la vulnérabilité liée aux données. Ces résultats confirment ceux de Varchetta et al. (2020) et Buglass et al. (2016 ; 2017) qui ont montré que l'augmentation du FOMO contribue à l'augmentation de la vulnérabilité en ligne.

Nous avons proposé, également, de tester l'effet de la vulnérabilité suite au partage de données personnelles en ligne sur le changement de comportement des internautes, à savoir le changement de site Web. A niveau de la littérature, une grande importance a été accordée à la compréhension et l'explication du concept de changement de site Web en ligne (Han et al., 2011 ; Nikbin et al., 2012 ; Liang et al., 2018). En outre, la littérature a montré l'existence d'une

relation significative entre les préoccupations liées à la vie privée en ligne et le changement de site web (Zhao et al., 2017 ; Bhattacherjee et al., 2012). Les résultats de notre recherche ont confirmé cette hypothèse et montrent que la vulnérabilité liée au données en ligne influence positivement le changement de site web ($\beta = 0{,}385$). En effet, avec les développements digitaux, le nombre de sites Web a augmenté à un rythme sans précédent et la concurrence entre eux est devenue de plus en plus importante, ce qui aboutit à l'amélioration des services proposés en ligne. Ainsi, l'internaute se trouve face à un choix considérable de sites Web, ce qui influence leurs critères de choix. Par conséquent, si l'internaute se sent vulnérable, c'est-à-dire que le site web ne répond pas à ses attentes en termes de respect de la vie privée et de la confidentialité des informations personnelles partagées en ligne, il est évident que ce dernier sera remplacé par un autre. Les internautes cherchent à avoir une expérience satisfaisante, sans problèmes et inquiétudes, et qui ne contribue pas au développement de leur vulnérabilité. Ce résultat est en accord avec celui de Martin et al. (2017) qui montrent que la vulnérabilité en ligne entraine un changement de comportement.

Pour conclure, nous pouvons dire que les résultats de notre recherche nous ont permis de confirmer l'existence de lien entre la peur de rater quelque chose et la vulnérabilité des internautes suite au partage de données personnelles en ligne, et que cette même vulnérabilité contribue au changement de site Web.

3. Conclusion

Ce travail constitue d'abord une continuation des études et des travaux en marketing sur le partage de données personnelles en ligne et la confidentialité des données personnelles partagées en ligne. Ce travail s'inscrit dans l'intersection entre la quantité énorme de données personnelles disponibles en ligne et la croissance technologique, qui conduisent à une ère de gestion de Big data dans laquelle les entreprises sont nécessairement axées sur les données, et ceci à un degré sans précédent (Jun et al., 2018).

Notre motivation pour étudier le concept de vulnérabilité liée aux données personnelles partagées en ligne découle de l'ampleur des problèmes associés au non-respect de la vie privée, mais aussi du peu de travaux ayant été menés sur cette notion (Buglass et al., 2017). Nous contribuons à la littérature sur la vulnérabilité des consommateurs. Jusqu'à présent, la vulnérabilité des consommateurs a été liée à des questions sociétales majeures, telles que la pauvreté (Hoffmann et McNair, 2019), le handicap (Kaufman-Scarborough, 2000) et l'appartenance ethnique (Crockett et Wallendorf, 2004), mais très peu à des questions de protection de la vie privée. En effet, la vulnérabilité n'est pas seulement une question de conscience de l'utilisation possible de ces informations, elle implique également les sentiments et les émotions des individus (Baker et al., 2005). Nous ajoutons donc à la littérature en proposant la notion de vulnérabilité des données des consommateurs et en la conceptualisant comme un sentiment d'impuissance face aux données personnelles partagées en ligne.

En outre, notre travail consiste teste et valide un modèle intégrant un antécédents (la peur de rater quelque chose) et une conséquence comportementale (changement de site Web)

de la vulnérabilité dans le contexte du partage des données personnelles en ligne qui, nous semble-t-il, constitue un champ d'investigation nouveau. A cet effet, les résultats montrent que la peur de rater quelque chose constitue un facteur influençant la vulnérabilité des internautes suite au partage de données personnelles en ligne (Martin et al., 2017). Celle-ci exerce, à son tour, un effet sur le comportement de l'internaute pouvant se traduire par le changement de site Web (Martin et al., 2017).

Au niveau managérial, la validation de notre modèle conceptuel apporte des éclairages concernant les leviers d'action que les entreprises sont appelées à cultiver en interne pour améliorer la relation avec leurs clients dans le contexte du digital. En effet, notre recherche fournit aux praticiens une description complète de ce que signifie la vulnérabilité liée aux données personnelles partagées en ligne en termes d'insécurité, d'exposition, de menace et de susceptibilité (Martin et al., 2017). Les problèmes liés aux données personnelles partagées en ligne génèrent non seulement des inquiétudes chez les consommateurs, mais les mettent également dans des situations de vulnérabilité qui se manifestent sous forme de changement de site Web. Pour cela, il est important pour les entreprises de connaitre les facteurs qui permettent le développement de la vulnérabilité suite au partage de données personnelles en ligne à savoir la peur de rater quelque chose afin d'éviter le changement de comportement des internautes. Cette recherche devrait ainsi aider les entreprises à adopter de meilleures pratiques managériales et éthiques en matière de gestion des données personnelles partagées en ligne suite au développement de la vulnérabilité liée aux données.

En dépit de ses contributions, le présent travail comporte des limites qui peuvent ouvrir des voies pour de nouvelles recherches. Premièrement, une limite liée à la méthode d'échantillonnage peut être soulignée. L'absence d'une base de sondage nous a contraint d'opter pour une méthode non probabiliste, à savoir la méthode d'échantillonnage de convenance. Cette méthode ne garantit pas la représentativité de l'échantillon et la possibilité de générer des résultats représentatifs s'en trouve réduite (Hulley et al. 2007). De futures études pourraient donc répliquer notre étude en adoptant une méthode d'échantillonnage qui permettent d'avoir un échantillon davantage représentatif. Quant à la taille de l'échantillon, il est à noter que l'obtention de résultats représentatifs nécessite une taille suffisamment importante pour permettre de généraliser les résultats. Dans notre recherche, nous avons obtenu une taille relativement réduite (400 répondants). De ce fait, un échantillon de taille plus importante est recommandé.

Par ailleurs, notre recherche a montré l'effet de la vulnérabilité des internautes suite au partage de données personnelles en ligne sur le changement de site Web. Il serait également intéressant d'étudier l'impact de cette vulnérabilité sur les comportements de résistance à la technologie des individus, en mobilisant la théorie de résistance de Ram (1987). Selon Lee (2020), la résistance des utilisateurs est un aspect important du processus d'adoption des nouvelles technologies, et elle peut apparaitre sous la forme de rejet, de report et d'opposition. On peut ainsi supposer que si un individu se sent vulnérable par rapport à ses données

personnelles, il s'opposera à l'adoption d'une innovation. Cela pourrait par exemple être le cas avec le métavers comme semble le suggérer Lee et Chaney (2023).

Bibliographie

Adger, W. N. (2006). Vulnerability. Global Environmental Change, 16(3), 268-281. https://doi.org/10.1016/j.gloenvcha.2006.02.006

Aguirre, A. J., & Hahn, W. C. (2018). Synthetic Lethal Vulnerabilities in KRAS -Mutant Cancers. Cold Spring Harbor Perspectives in Medicine, 8(8), a031518.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox : The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. Journal of Retailing, 91(1), 34-49. https://doi.org/10.1016/j.jretai.2014.09.005

Atiso, K., & Kammer, J. (2018). User Beware : Determining Vulnerability in Social Media Platforms for Users in Ghana. Library Philosophy and Practice, 2018.

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building Understanding of the Domain of Consumer Vulnerability. Journal of Macromarketing, 25(2), 128-139. https://doi.org/10.1177/0276146705280622

Banerjee, S., Black, R., Mishra, A., & Kniveton, D. (2019). Assessing vulnerability of remittance-recipient and nonrecipient households in rural communities affected by extreme weather events : Case studies from South-West China and North-East India. Population, Space and Place, 25(2), e2157. https://doi.org/10.1002/psp.2157

Bansal, G., & Nah, F. F.-H. (2022). Internet Privacy Concerns Revisited : Oversight from Surveillance and Right To Be Forgotten as New Dimensions. Information & Management, 59(3), 103618. https://doi.org/10.1016/j.im.2022.103618

Bansal, G., Zahedi, F. "Mariam", & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems, 49(2), 138-150. https://doi.org/10.1016/j.dss.2010.01.010

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information & Management, 53(1), 1-21. https://doi.org/10.1016/j.im.2015.08.001

Bansal, H. S., & Taylor, S. F. (1999). The Service Provider Switching Model (SPSM) : A Model of Consumer Switching Behavior in the Services Industry. Journal of Service Research, 2(2), 200-218. https://doi.org/10.1177/109467059922007

Beudaert, A., & Nau, J.-P. (2021). The vulnerability of consumers with disabilities : The benefits of taking time into account. Recherche et Applications En Marketing (English 196 Bibliographie Edition), 36(4), 2-23. https://doi.org/10.1177/2051570721995625

Beyens, I., Frison, E., & Eggermont, S. (2016). "I don't want to miss a thing" : Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress. Computers in Human Behavior, 64, 1-8. https://doi.org/10.1016/j.chb.2016.05.083

Bhattacherjee, A., Limayem, M., & Cheung, C. M. K. (2012). User switching of information technology : A theoretical synthesis and empirical test. Information & Management, 49(7), 327-333. https://doi.org/10.1016/j.im.2012.06.002

Bougie, R., Pieters, R., & Zeelenberg, M. (2003). Angry Customers don't Come Back, They Get Back : The Experience and Behavioral Implications of Anger and Dissatisfaction in Services. Journal of the Academy of Marketing Science, 31(4), 377-393. https://doi.org/10.1177/0092070303254412

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites : Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Brennan, C., Sourdin, T., Williams, J., Burstyner, N., & Gill, C. (2017). Consumer vulnerability and complaint handling : Challenges, opportunities and dispute system design. International Journal of Consumer Studies, 41(6), 638-646. https://doi.org/10.1111/ijcs.12377

Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. M. (2016). When 'friends' collide : Social heterogeneity and user vulnerability on social network sites. Computers in Human Behavior, 54, 62-72. https://doi.org/10.1016/j.chb.2015.07.039

Buglass, S. L., Binder, J. F., Betts, L. R., & Underwood, J. D. M. (2017). Motivators of online vulnerability : The impact of social network site use and FOMO. Computers in Human Behavior, 66, 248-255. https://doi.org/10.1016/j.chb.2016.09.055

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks : Testing the moderating effects of perceived controllability and prior experience. Computers in Human Behavior, 26(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Cho, H., Li, P., & Goh, Z. H. (2020). Privacy Risks, Emotions, and Social Media : A Coping Model of Online Privacy. ACM Transactions on Computer-Human Interaction, 27(6), 1-28. https://doi.org/10.1145/3412367

Cho, J., Bello, M. S., Christie, N. C., Monterosso, J. R., & Leventhal, A. M. (2021). Adolescent emotional disorder symptoms and transdiagnostic vulnerabilities as predictors of young adult substance use during the COVID-19 pandemic : Mediation by substance-related coping behaviors. Cognitive Behaviour Therapy, 50(4), 276-294. https://doi.org/10.1080/16506073.2021.1882552

Choudhary, K., Boori, M. S., & Kupriyanov, A. (2018). Spatial modelling for natural and environmental vulnerability through remote sensing and GIS in Astrakhan, Russia. The Egyptian Journal of Remote Sensing and Space Science, 21(2), 139-147. https://doi.org/10.1016/j.ejrs.2017.05.003

Choudhary, K., Boori, M. S., & Kupriyanov, A. (2018). Spatial modelling for natural and environmental vulnerability through remote sensing and GIS in Astrakhan, Russia. The Egyptian Journal of Remote Sensing and Space Science, 21(2), 139-147. https://doi.org/10.1016/j.ejrs.2017.05.003

Choudhary, K., Boori, M. S., & Kupriyanov, A. (2018). Spatial modelling for natural and environmental vulnerability through remote sensing and GIS in Astrakhan, Russia. The Egyptian Journal of Remote Sensing and Space Science, 21(2), 139-147. https://doi.org/10.1016/j.ejrs.2017.05.003

Dewan, A. M., & Yamaguchi, Y. (2009). Land use and land cover change in Greater Dhaka, Bangladesh : Using remote sensing to promote sustainable urbanization. Applied Geography, 29(3), 390-401. https://doi.org/10.1016/j.apgeog.2008.12.005

Diener, E., Kesebir, P., & Lucas, R. (2008). Benefits of Accounts of Well-Being—For Societies and for Psychological Science. Applied Psychology, 57(s1), 37-53. https://doi.org/10.1111/j.1464-0597.2008.00353.x

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413-422. https://doi.org/10.1080/01449290410001715723

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet Users' Privacy Concerns and Beliefs About Government Surveillance : An Exploratory Study of Differences Between Italy and the United States. Journal of Global Information Management (JGIM), 14(4), 57-93. https://doi.org/10.4018/jgim.2006100103

Dodson, J. A., Tybout, A. M., & Sternthal, B. (1978). Impact of Deals and Deal Retraction on Brand Switching. Journal of Marketing Research, 15(1), 72-81. https://doi.org/10.1177/002224377801500109

Dogan, V. (2019). Why Do People Experience the Fear of Missing Out (FoMO) ? Exposing the Link Between the Self and the FoMO Through Self-Construal. Journal of Cross Cultural Psychology, 50(4), 524-538. https://doi.org/10.1177/0022022119839145

Drolet, A. (2002). Inherent Rule Variability in Consumer Choice : Changing Rules for Change's Sake. Journal of Consumer Research, 29(3), 293-305. https://doi.org/10.1086/344433

Duvenage, M., Correia, H., Uink, B., Barber, B. L., Donovan, C. L., & Modecki, K. L. (2020). Technology can sting when reality bites : Adolescents' frequent online coping is ineffective with momentary stress. Computers in Human Behavior, 102, 248-259. https://doi.org/10.1016/j.chb.2019.08.024

Dyussembayeva, S., Viglia, G., Nieto-Garcia, M., & Invernizzi, A. C. (2020). It makes me feel vulnerable! The impact of public self-disclosure on online complaint behavior. International Journal of Hospitality Management, 88, 102512.

Echeverri, P., & Salomonson, N. (2019). Consumer vulnerability during mobility service interactions : Causes, forms and coping. Journal of Marketing Management, 35(3-4), 364-389. https://doi.org/10.1080/0267257X.2019.1568281

Elmastas, D., & Candan, F. B. (2018). A Study on the Relationship between Personality Traits and Consumer Complaint Behavior. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3224378

Elms, J., & Tinson, J. (2012). Consumer vulnerability and the transformative potential of Internet shopping : An exploratory case study. Journal of Marketing Management, 28(11-12), 1354-1376. https://doi.org/10.1080/0267257X.2012.691526

Entemeyer, D. (1996). Etude micromécanique du comportement thermomécanique des alliages à mémoire de forme.

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites : An exploration of the relational and psychological stressors associated with Facebook use and affordances. Computers in Human Behavior, 45, 168-176. https://doi.org/10.1016/j.chb.2014.11.083

Foxall, G. R., & Greenley, G. E. (1999). Consumers' Emotional Responses to Service Environments. Journal of Business Research, 46(2), 149-158. https://doi.org/10.1016/S0148-2963(98)00018-6

Grewal, R., Cote, J. A., & Baumgartner, H. (2004). Multicollinearity and Measurement Error in Structural Equation Models : Implications for Theory Testing. Marketing Science, 23(4), 519-529. https://doi.org/10.1287/mksc.1040.0070

Grover, R., & Srinivasan, V. (1992). Evaluating the Multiple Effects of Retail Promotions on Brand Loyal and Brand Switching Segments. Journal of Marketing Research, 29(1), 76-89. https://doi.org/10.1177/002224379202900107

Gundecha, P., Barbier, G., & Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, 511-519. https://doi.org/10.1145/2020408.2020489

Gundecha, P., Barbier, G., & Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, 511-519. https://doi.org/10.1145/2020408.2020489

Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (s. d.). Patterns of risk and safety online.

Hetz, P. R., Dawson, C. L., & Cullen, T. A. (2015). Social Media Use and the Fear of Missing Out (FoMO) While Studying Abroad. Journal of Research on Technology in Education, 47(4), 259-272. https://doi.org/10.1080/15391523.2015.1080585

Hou, A. C. Y., Chern, C.-C., Chen, H.-G., & Chen, Y.-C. (2011). 'Migrating to a new virtual world' : Exploring MMORPG switching through human migration theory. Computers in Human Behavior, 27(5), 1892-1903. https://doi.org/10.1016/j.chb.2011.04.013

Jiang, Y., Zhan, L., & Rucker, D. D. (2014). Power and Action Orientation : Power as a Catalyst for Consumer Switching Behavior. Journal of Consumer Research, 41(1), 183-196. https://doi.org/10.1086/675723

Jiang, Z. (Jack), Heng, C. S., & Choi, B. C. F. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. Information Systems Research, 24(3), 579-595. https://doi.org/10.1287/isre.1120.0441

Lam, S. K., Ahearne, M., Hu, Y., & Schillewaert, N. (2010). Resistance to Brand Switching when a Radically New Brand is Introduced : A Social Identity Theory Perspective. Journal of Marketing, 74(6), 128-146. https://doi.org/10.1509/jmkg.74.6.128

Lee, M. S. W., & Chaney, D. (2023). The psychological and functional factors driving metaverse resistance. Internet Research, ahead-of-print(ahead-of-print). https://doi.org/10.1108/INTR-08-2022-0647

Livingstone, K. M., & Srivastava, S. (2012). Up-regulating positive emotions in everyday life : Strategies, individual differences, and associations with positive emotion and well-being. Journal of Research in Personality, 46(5), 504-516. https://doi.org/10.1016/j.jrp.2012.05.009

Livingstone, S., & Helsper, E. J. (2007). Taking risks when communicating on the Internet : The role of offline social-psychological factors in young people's vulnerability to online risks. Information, Communication & Society, 10(5), 619-644. https://doi.org/10.1080/13691180701657998

Mackenzie, C. (Éd.). (2014). Vulnerability : New essays in ethics and feminist philosophy. Oxford University Press.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. Journal of the Academy of Marketing Science, 45(2), 135-155. https://doi.org/10.1007/s11747-016 0495-4

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy : Effects on Customer and Firm Performance. Journal of Marketing, 81(1), 36-58. https://doi.org/10.1509/jm.15.0497

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., Wang, Y., & Weaven, S. K. (2020). Data Privacy in Retail. Journal of Retailing, 96(4), 474-489. https://doi.org/10.1016/j.jretai.2020.08.003

Martin, M. C., & Gentry, J. W. (1997). Stuck in the Model Trap : The Effects of Beautiful Models in Ads on Female Pre-Adolescents and Adolescents. Journal of Advertising, 26(2), 19-33. https://doi.org/10.1080/00913367.1997.10673520

Omolo, N., & Mafongoya, P. L. (2019). Gender, social capital and adaptive capacity to climate variability : A case of pastoralists in arid and semi-arid regions in Kenya. International Journal of Climate Change Strategies and Management, 11(5), 744-758. https://doi.org/10.1108/IJCCSM-01-2018-0009

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR : Challenges and proposed solutions. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy001

Przybylski, A. K., & Weinstein, N. (2013). Can you connect with me now? How the presence of mobile communication technology influences face-to-face conversation quality. Journal of Social and Personal Relationships, 30(3), 237-246.

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior, 29(4), 1841-1848. https://doi.org/10.1016/j.chb.2013.02.014

Ratchford, M., & Ratchford, B. T. (2021). A cross-category analysis of dispositional drivers of technology adoption. Journal of Business Research, 127, 300-311. https://doi.org/10.1016/j.jbusres.2021.01.037

Reagle, J. (2015). Following the Joneses : FOMO and conspicuous sociality. First Monday. https://doi.org/10.5210/fm.v20i10.6064

Riegelsberger, J., & Sasse, M. A. (2010, juin 9). Ignore These At Your Peril : Ten principles for trust design. Presented at: TRUST2010: 3rd International Conference on Trust and Trustworthy Computing, Berlin, Germany. (2010). TRUST2010: 3rd International Conference on Trust and Trustworthy Computing, Berlin, Germany. https://discovery.ucl.ac.uk/id/eprint/20297/

Staksrud, E., & Milosevic, T. (2022). Social Networking Sites and Children's Social Development. In The Wiley-Blackwell Handbook of Childhood Social Development (p. 707-725). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119679028.ch38

Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm ? Computers in Human Behavior, 29(1), 40-50. https://doi.org/10.1016/j.chb.2012.05.026

Strycharz, J., & Duivenvoorde, B. B. (2021). The exploitation of vulnerability through personalised marketing communication : Are consumers protected ? Internet Policy Review, 10(4), 1-27. https://doi.org/10.14763/2021.4.1585

Varchetta, M., Fraschetti, A., Mari, E., Giannini, A. M., Varchetta, M., Fraschetti, A., Mari, E., & Giannini, A. M. (2020). Adicción a redes sociales, Miedo a perderse experiencias (FOMO) y Vulnerabilidad en línea en estudiantes universitarios. Revista Digital de Investigación en Docencia Universitaria, 14(1). https://doi.org/10.19083/ridu.2020.1187

Wang, Y., Zhu, D., Yang, Y., Lee, K., Mishra, R., Go, G., Oh, S.-H., Kim, D.-H., Cai, K., Liu, E., Pollard, S. D., Shi, S., Lee, J., Teo, K. L., Wu, Y., Lee, K.-J., & Yang, H. (2019). Magnetization switching by magnon-mediated spin torque through an antiferromagnetic insulator. Science, 366(6469), 1125-1128. https://doi.org/10.1126/science.aav8076

Wang, Z., & Yu, Q. (2015a). Privacy trust crisis of personal data in China in the era of Big Data : The survey and countermeasures. Computer Law & Security Review, 31(6), 782-792. https://doi.org/10.1016/j.clsr.2015.08.006

Wang, Z., & Yu, Q. (2015b). Privacy trust crisis of personal data in China in the era of Big Data : The survey and countermeasures. Computer Law & Security Review, 31(6), 782-792. https://doi.org/10.1016/j.clsr.2015.08.006

Warner, M., & Wang, V. (2019). Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability and information management. Journal of Information, Communication and Ethics in Society, 17(4), 375-394. https://doi.org/10.1108/JICES-07-2018-0060

Wegmann, E., Oberst, U., Stodt, B., & Brand, M. (2017). Online-specific fear of missing out and Internet-use expectancies contribute to symptoms of Internet-communication disorder. Addictive Behaviors Reports, 5, 33-42.

Wiederhold, N. P. (2017). Antifungal resistance : Current trends and future strategies to combat. Infection and Drug Resistance, 10, 249-259. https://doi.org/10.2147/IDR.S124918

Wortham, S., Mortimer, K., Lee, K., Allard, E., & White, K. D. (2011). Interviews as interactional data. Language in Society, 40(1), 39-50. https://doi.org/10.1017/S0047404510000874

Zhang, K. Z. K., Lee, M. K. O., Cheung, C. M. K., & Chen, H. (2009). Understanding the role of gender in bloggers' switching behavior. Decision Support Systems, 47(4), 540-546. https://doi.org/10.1016/j.dss.2009.05.013

Annexe

Figure 1 : Modèle de recherche

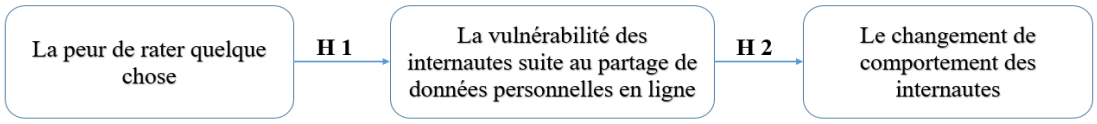

Tableau 1 : Description de l'échantillon

	Caractéristiques	**Pourcentage**
Genre	Homme	32.8%
	Femme	67.2%
Age	40 ans et moins	81.8%
	Plus de 40 ans	18.2%
Lieu de résidence	Tunisie	47.8%
	France	52.2%
Catégorie socio-professionnelle	Elèves, étudiants	50.2%
	Artisans, commerçants ou chefs d'entreprise	8.9%
	Cadres ou professions intellectuelles supérieures	22.3%
	Employés	10.1%
	Ouvriers	2.4%
	Retraité	0.3%

ISSN : 2724-7260
Volume 4 : Numéro 2

	Sans activité professionnelle	5.8%

Tableau 5 : Résultats des liens de structure

Liens de structure	**Estimate**	**S.E.**	**C.R.**	**P**	**Hypothèse**
FOMO ==> Vulnérabilité	0.156	0.051	3.057	***	Acceptée
Vulnérabilité ==> Changement de site Web	0.341	0.007	4.886	***	Acceptée