UNIVERSITÉ DU QUÉBEC À MONTRÉAL

VULNÉRABILITÉ DES CONSOMMATEURS QUÉBÉCOIS SUITE À L'APPLICATION DE LA LOI 25 DANS LE SECTEUR DE LA FINTECH

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

MAÎTRISE ÈS SCIENCES DE LA GESTION

PAR

PHANIE MANUELA MOPE MBOPDA

JANVIER 2026

REMERCIEMENTS

Ce rapport représente une phase significative de mon parcours scolaire et je souhaite exprimer ma sincère reconnaissance à tous ceux qui ont participé à la réalisation de ce mémoire de recherche. En premier lieu, je souhaite exprimer ma profonde gratitude à Mme Sandrine Prom Tep et à M. Renato Hübner Barcelos, pour leur accompagnement inestimable tout au long de la réalisation de ces travaux, leurs recommandations judicieuses et leur soutien continu tout au long de ce projet. Un sincère merci pour leur générosité, leurs principes humains et leur dévouement total à la réussite de leurs étudiants.

Je souhaite également remercier le corps enseignant de l'ESG UQAM pour leur soutien académique. Une gratitude spéciale à tous ceux qui ont consacré de leur temps pour répondre à mon enquête, car leur apport a joué un rôle déterminant dans la réalisation de cette recherche.

Je tiens à remercier mes parents pour leur soutien inconditionnel malgré la distance, leurs prières et leur amour. À Linda, ma grande sœur et meilleure amie, merci pour ton soutien moral et de m'avoir redonné de l'espoir et du sourire, de te rendre disponible et de me redonner confiance à chaque fois, merci d'exister. À l'homme de ma vie, merci pour ton amour inconditionnel, ta patience et ton soutien indéfectible. À tonton Jean Baptiste, tonton Jean Jacques, tata Julie, Rousselle, Bryan, mes amis, un énorme merci pour votre compréhension et votre engagement à ma réussite. Un merci à mes responsables de la GAR Clinique qui m'ont permis de concilier études et travail.

Merci à vous tous.

DÉDICACE

À tous les étudiants internationaux, nous pouvons
être fiers de notre parcours.

AVANT-PROPOS

Ce projet de mémoire s'inscrit dans le cadre de ma formation en Maîtrise en Sciences de Gestion option Marketing Numérique à l'ESG-UQAM. À travers cette recherche, l'objectif est d'examiner un thème pertinent et d'une grande actualité qui touche les consommateurs dans le monde de façon générale et le Québec de façon particulière : la vulnérabilité par les consommateurs du Québec dans un contexte numérique en perpétuel changement, caractérisé par l'application de la Loi 25 et ses conséquences dans le domaine des technologies financières.

Cette approche scientifique m'a permis d'allier mon intérêt pour les problématiques liées à la protection des données personnelles et ma curiosité pour les enjeux que rencontrent les consommateurs dans un environnement économique qui se complexifie davantage. Grâce à ce travail, j'ai pu consolider mes connaissances, acquérir des aptitudes d'analyse et m'impliquer dans une analyse critique des méthodes actuelles et des alternatives envisageables pour gagner la confiance des utilisateurs et diminuer leur sentiment de vulnérabilité lors de leur parcours client sur les plateformes de technologies financières. Toutefois, la principale difficulté rencontrée dans l'exécution de notre mission a été la collecte des données.

Il est important pour moi que les aboutissements de ce travail de recherche puissent non seulement aider à comprendre les perceptions et attentes des consommateurs québécois, mais également proposer des idées aux décideurs et chercheurs concernés par les problématiques liées à la confidentialité et à la gestion des données numériques.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

RÉSUMÉ

Dans un environnement où la préservation des informations privées des consommateurs en ligne est une préoccupation majeure, l'instauration de la Loi 25 au Québec impose aux entreprises exerçant sur ce territoire, en particulier celles du domaine des services financiers numériques, de nouvelles responsabilités. Ce travail de recherche examine la vulnérabilité perçue par les consommateurs québécois dans ce contexte numérique, notamment à la suite de l'adoption de la Loi 25 en septembre 2022, une loi destinée à intensifier la protection des informations privées. Cette recherche, se concentrant particulièrement sur le domaine des technologies financières (Fintech), analyse les avis des clients concernant la protection de leurs données personnelles et leur confiance aux entités de services bancaires en ligne.

En articulant notre cadre conceptuel autour des notions clés telles que la connaissance de la Loi 25 et de la protection des données, la transparence des plateformes, l'utilité perçue et la facilité d'adoption des plateformes financières, nous avons proposé et testé huit hypothèses d'étude. L'approche méthodologique se base sur une analyse quantitative utilisant une analyse de la variance dans le contexte d'un design expérimental intersujets à un facteur, comprenant six conditions qui convergent avec divers modèles de conception de bannières de sécurité.

Les divers résultats obtenus démontrent que la connaissance de la Loi 25, l'instauration des dispositifs de protection des données, le degré de transparence des plateformes de Fintech, l'utilité et la facilité d'utilisation des mesures de sécurité entre autres jouent un rôle crucial dans la diminution de la vulnérabilité ressentie par les utilisateurs. En outre, cette faille impacte directement la confiance de ces consommateurs et leur adoption des services Fintech en accord avec la Loi 25. Les résultats ont également permis de révéler l'urgence de l'application d'un modèle de conception unique pour tous afin de favoriser l'application de la Loi 25 pour toutes entreprises de services bancaires en ligne exerçant au Québec.

Ces conclusions véhiculent des contributions théoriques en dotant la littérature existante sur la perception du risque et l'acceptation des règlementations en matière de protection des données. Sur le plan managérial, elles mettent en avant la nécessité pour les entreprises Fintech d'accroître

la transparence de leurs politiques de confidentialité et d'optimiser l'expérience utilisateur des bannières de sécurité.

Mots clés : Vulnérabilité perçue, utilisateurs, Loi 25, technologies financières, design UX.

ABSTRACT

In an environment where the preservation of consumers' private information online is a major concern, the introduction of Bill 25 in Quebec imposes new responsibilities on companies operating in this territory, particularly those in the digital financial services sector. This research examines the vulnerability felt by Quebec consumers in this digital context, particularly following the adoption of Bill 25 in September 2022, a law designed to intensify the protection of private information. Focusing particularly on the field of financial technologies (Fintech), this research analyzes customers' opinions on the protection of their personal data and their trust in online banking entities.

By articulating our conceptual framework around key notions such as knowledge of Law 25 and data protection, platform transparency, perceived usefulness and ease of adoption of financial platforms, we proposed and tested eight hypotheses. The methodological approach is based on quantitative analysis using analysis of variance in the context of a single-factor between-subjects experimental design, comprising six conditions that converge with various safety banner design models.

The various results obtained demonstrate that knowledge of Law 25, the introduction of data protection measures, the level of transparency of Fintech platforms, the usefulness and ease of use of security measures, among others, play a crucial role in reducing the vulnerability felt by users. In addition, this vulnerability has a direct impact on consumers' confidence and their adoption of Fintche sercives in accordance with Law 25. The results also revealed the urgent need to apply a single design model for all, in order to promote the application of Bill 25 for all online banking companies operating in Quebec.

These findings convey theoretical contributions by endowing the existing literature on risk perception and acceptance of data protection regulations. On a managerial level, they highlight the need for fintech companies to increase the transparency of their privacy policies and optimize the user experience of security banners.

Keywords : Perceived vulnerability, users, Bill 25, financial technologies, UX design.

INTRODUCTION

Lorsque nous essayons de donner une définition exacte au concept de protection de vie privée, nous sommes la plupart du temps renvoyés à des définitions subjectives du concept du droit à la vie privée. C'est le cas de Lebrun qui propose comme définition à ce concept l'obligation pour tout être humain d'avoir droit à une vie privée et de déterminer les limites de sa vie privée qui doivent être respectées par les professionnels. (Lebrun, 2015).

La loi dans sa généralité ne présente pas une définition du concept de protection de la vie privée (Martin et Murphy, 2017), mais elle donne une description de ses objectifs afin que le consommateur[1] puisse être averti sur ses droits et les entreprises sur ses obligations concernant l'utilisation des données clients. Néanmoins, Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, définit la vie privée en ligne comme étant l'optique que l'avenir de la vie privée ne peut pas être certifié qu'en conformité aux cadres législatifs et règlementaires; au contraire, la certification de la vie privée doit devenir le mode d'opération par défaut d'une organisation (Ann Cavoukian, 2013). Autrement dit, la protection de la vie privée dépend de la législation qui encadre le concept de vie privée d'un état à un autre et aussi d'une période à une autre (Lau, 2017).

Les avancées technologiques et la propension de l'intelligence artificielle dans les domaines d'activités médicales, des transports, de la communication, etc., ont bouleversé et amélioré nos modes de vie de plusieurs manières différentes (Rowland, 2006). À l'ère des mégadonnées, l'automatisation des pratiques de collectes et de traitement des données personnelles a permis de dresser des profils plus fins des consommateurs sur la base de leur comportement en ligne et représente un moyen d'accroître significativement les performances en matière de relation client (Martin et al., 2020).

De la définition fournie par Ann Cavoukian et de l'automatisation des pratiques facilitant la réalisation des performances en matière de relation client, nous comprenons la nécessité pour les

[1] Pour des raisons de lisibilité, le masculin est employé dans ce mémoire comme forme générique er englobe toutes les personnes sans distinction de sexe.

pays de définir un cadre législatif régulant les pratiques courantes établies par les organisations et les institutions afin de définir des restrictions sur le traitement des données à caractère personnel pour les entreprises et donner du pouvoir aux consommateurs afin qu'ils aient un meilleur contrôle sur les données qu'ils laissent aux mains des entreprises (Saerens, 2019). C'est ainsi que le parlement européen a adopté en 2016 le **Règlement général sur la protection des données** (RGPD) qui est entré en vigueur en mai 2018. Cette loi est l'une des premières à être définie dans le cadre légal de protection de données à caractère personnel et son application concerne aussi bien les responsables de traitement et sous-traitants étrangers, qui traitent des données personnelles en provenance de l'Union européenne (UE). (Mission RGPD, 2023)

Il existe également la **Loi californienne sur la protection de la vie privée des consommateurs** (California Consumer Privacy Act) de 2018, entrée en vigueur le 1er janvier 2020, mais avec évolution du temps et des données a été modifié par les California Privacy Rights Acts de 2020 (CPRA), qui sont entrées en vigueur le 1er janvier 2023, avec prise d'effet au 1er juillet 2023. (Atlassian, 2023).

Au Québec, nous avons La **Loi 25** qui s'inspire du règlement général sur la protection des données (RGPD) de l'Union européenne (Tink profitabilité numérique, 2023), modernisant des dispositions législatives en matière de protection des renseignements personnels et qui apporte des modifications importantes à la Loi sur la protection des renseignements personnels dans le secteur privé (Commission accès à information du Québec, 2023). Ces modifications de la Loi 25 entrent progressivement en vigueur depuis 2022 et s'échelonnent sur une période de trois ans, soit jusqu'en 2024 (Commission accès à information du Québec, 2023).

Toutes les règlementations précédemment définies ont pour objectif principal de protéger la vie privée des consommateurs en fixant des principes à suivre par les institutions pour la collecte, l'utilisation, la divulgation, l'exactitude de la mise à jour, la conservation, la sécurité et la suppression des données personnelles (Division de l'information, de la protection de la vie privée et des archives publiques, 2018). Les renseignements personnels (renseignements enregistrés au sujet d'une personne identifiable) sont donc le point central de la protection de la vie privée. Le

Manuel sur l'Accès à l'information et la protection de la vie privée établit comme pouvant constituer des renseignements personnels une liste exhaustive d'informations notamment :

- Les renseignements personnels : le nom, l'adresse personnelle, l'adresse de courriel personnelle, le numéro de téléphone personnel, la race, l'origine nationale et ethnique, la couleur, la religion, l'âge, la date de naissance, l'orientation sexuelle, les antécédents médicaux et professionnels, etc.

- Les renseignements sur l'identité professionnelle : le nom, le titre, les coordonnées ou la désignation d'une personne qui permettent de l'identifier en liaison avec ses activités commerciales, professionnelles ou officielles.

- Les renseignements liés au service à la clientèle : le nom, l'adresse et le numéro de téléphone ou les autres coordonnées, le numéro de la transaction ou du reçu fourni, les renseignements relatifs au versement des droits, s'il y a lieu, etc.

L'entrée en application de la Loi 25 au Québec s'échelonne en trois phases et sur trois périodes (22 septembre 2022 1re phase, 22 septembre 2023 2e phase, 22 septembre 2024 3e phase) et à chaque phase, les entreprises qui font affaire au Québec sont tenues de respecter des obligations en vigueur en matière de protection des renseignements personnels (Commission d'accès à l'information, 2023). Ces responsabilités et obligations définies par le gouvernement du Québec sont toutes aussi importantes les unes que les autres, mais pour cette introduction, nous présentons de façon brève, concise et précise ce que cette Loi impose aux organismes privés et publics : il s'agit de mettre en place des politiques de confidentialité claires et de mettre à jour leur inventaire des renseignements. Ce qui signifie que toute entreprise au Québec qui collecte, traite ou communique des données numériques doit intégrer une politique de confidentialité par l'ajout d'une page dédiée compréhensible et mettre une bannière de consentement sur son site. Elles ont par conséquent l'obligation d'énumérer, expliquer et permettre aux utilisations d'effectuer des choix sur l'utilisation ou non des fichiers témoins encore appelés cookies (Leprince, 2023). Le pouvoir revient donc au consommateur.

Une étude réalisée en 2022 et publiée en mars 2023 par la société Phoenix Strategic Perspectives inc. (Phœnix SPI), mandatée par le commissariat à la protection de la vie privée du Canada dans le but de sensibiliser les Canadiens aux enjeux liés à la protection de la vie privée et de les aider à mieux comprendre a révélé que la grande majorité des Canadiens (93%) des Canadiens sont quelque peu préoccupés par la protection de leur vie privée (Commissariat à la protection de la vie privée, 2023). Sur les 1500 répondants, les groupes susceptibles de suivre l'actualité sur la protection sont représentés par 57% dans la région du Québec contre 68% vivant au Canada atlantique. 38% des répondants estiment avoir une bonne connaissance sur la façon de se protéger en 2022 contre 46% en 2020 et 2018. Par ailleurs, 4 Canadiens sur 10 estiment que les entreprises respectent leur droit à la vie privée. Dans cette même étude, il fait état du fait que les Canadiens font confiance au gouvernement et aux banques traditionnelles pour la protection de leurs renseignements personnels, mais pas aux autres organisations et aux entreprises. Cette confiance exprimée ne s'applique pas aux nouveaux acteurs du domaine financier digital car bien que les entreprises de Fintech évoluent dans le secteur financier, elles se différencient des banques classiques par leur orientation technologique, l'importance des plateformes digitales et la multitude de méthodes utilisées pour collecter et traiter les données privées des clients. Aussi, historiquement régies par des relations de confiance solides et des cadres règlementaires bien établis, les Fintech fonctionnent dans un contexte considéré comme plus neuf et dynamique, mais aussi plus imprévisible du point de vue des clients. Tandis que les banques traditionnelles jouissent d'un capital de confiance institutionnelle qui a été construit sur le long terme, les Fintech sont confrontées à un manque de légitimité perçue, surtout en ce qui concerne la protection des données et la transparence des opérations digitales.

C'est principalement cette différence qui suscite chez les consommateurs un sentiment de vulnérabilité particulier, ce qui explique l'importance d'examiner le secteur de la Fintech comme un cadre d'analyse de la protection des données, ce qui nous permet de ressortir deux concepts essentiels dans la vie privée : la confiance et la vulnérabilité perçue. Le concept de vulnérabilité perçue fait référence à la manière dont un individu perçoit sa possible exposition à des risques, son manque de contrçole ou une disparité d'information dans une relation d'échange numérique. Dans le secte de la Fintech, cette fragilité découle principalement de l'incertitude qui entoure l'utilisation, la protection et la gestion des données personnelles. Ce principe reprécente le cœur de cette

recherche car il aide à saisir comment les traits distinctifs des plateformes, les mécanismes de sauvegarde des données et la compréhension des règlementations impactent l'adoption ou la résistance aux services Fintech.

À partir des résultats présentés par le rapport Phoenix SPI qui démontrent que les Canadiens ne font pas confiance aux entreprises, notre regard se porte sur la perception de vulnérabilité du consommateur québécois. Au moment où toutes les phases de la Loi 25 ont pris effet, nous évaluons l'application de cette règlementation par les entreprises de technologies financières (Fintech) à travers les bannières de sécurité utilisées dans ce domaine d'activité.

L'écosystème des services financiers en ligne du Québec s'est rapidement imposé comme un protagoniste majeur dans le panorama financier international. En poursuivant sa progression en 2024, il continue de se développer grâce à de nouveaux produits introduits et une augmentation des partenariats. Le Québec comptabilise à ce jour 257 entreprises de technologies financières qui emploient environ 19 900 personnes au Canada et plus de 86 000 dans le monde (Rapport Fintech Québec semestriel, 2024). Secteur avec une très forte utilisation des données personnelles des utilisateurs, ces entreprises ont pour obligation d'appliquer les règles imposées par le législateur à travers la Loi 25 et par conséquent, de créer des bannières de sécurité sur leurs plateformes dans le respect des normes légale, éthique et responsable afin que l'expérience utilisateur soit le meilleur possible, que les consommateurs aient confiance quant à l'utilisation de leurs informations personnelles et favoriser ainsi l'adoption de leurs plateformes par ces utilisateurs.

Malgré les progrès apportés par la Loi 25, la manière dont les consommateurs perçoivent leur vulnérabilité sur internet reste un obstacle majeur à l'adoption des plateformes de Fintech dans leur habitude de consommation. La perception de cette vulnérabilité résulte d'un manque de confiance dans les paramètres de sécurité et d'une ignorance des dispositifs instaurés pour préserver leurs informations privées.

La littérature démontre que les individus sont soucieux de leur intimité sur les différentes plateformes (Acquisti, 2011). Malgré les pratiques des entreprises en matière de protection des renseignements, les consommateurs en ligne ont affirmé qu'ils n'ont aucun choix ou contrôle quant

au suivi et au partage de leurs renseignements personnels ou que les outils de protection de la vie privée existants ne sont pas utiles (Lau, 2017).

Dans un environnement où les plateformes Fintech se transforment en piliers de la gestion financière, saisir comment les utilisateurs et les paramètres de sécurité conçus interagissent est primordial pour créer une balance entre innovation, respect des normes règlementaires et vulnérabilité des usagers afin de favoriser l'adoption de ces plateformes par les Québécois.

Les résultats présentés dans cette étude confirment l'importance cruciale de la vulnérabilité perçue dans le lien entre les consommateurs et les plateformes de Fintech au Québec. Elle démontre que cette vulnérabilité est considérablement affectée par la transparence, la mise en œuvre des mesures de protection de données et la compréhension de la Loi 25. Ils mettent en évidence l'importance de voir la vulnérabilité perçue non comme un aspect secondaire, mais comme un facteur crucial des comportements d'adoption dans les contextes financiers numériques.

L'objectif global de cette étude vise à examiner l'impact des bannières de consentement sur la perception du sentiment d'insécurité des consommateurs et leur volonté d'adopter les services Fintech, en lien avec l'application de la Loi 25 concernant la protection des données personnelles. C'est dans ce contexte que cette recherche aspire à offrir des apports tant sur le plan théorique que managériale.

D'un point de vue managérial, notre étude offre des recommandations pratiques aux entrepriss de Fintech. Elle propose des méthodes de conception des paramètres capables d'atténuer le sentiment de vulnérabilité et d'encourager l'utilisation des services financiers numériques respectant les normes juridiques et éthiques. L'objectif théorique est de contribuer à enrichir la littérature sur la vulnérabilité perçue des consommateurs dans secteur des technologies financières sensibles, en mobilisant les modèles S-O-R et TAM pour examiner l'impact des paramètres de sécurité, de transparence et de connaissance règlementaire spécifique de la Loi 25.

est d'analyser les opinions des consommateurs du Québec concernant les mesures de sécurité numérique et les services offerts par les entreprises Fintech, conformément aux exigences récentes de la Loi 25. En d'autres termes, notre article vise à :

- QR 1 : Évaluer l'impact de la Loi 25 sur la perception de vulnérabilité des consommateurs québécois en ligne.

- QR 2 : Établir une étude comparative entre le design des bannières rattachées à la collecte et à l'utilisation des données personnelles dans le domaine de la Fintech par rapport aux autres domaines d'activité.

- QR 3 : Proposer un guide de recommandation pour un design optimal du consentement sur les plateformes en Fintech

Cette recherche, en adoptant un design expérimental à un facteur, examine dans les chapitres qui suivent les relations entre les divers concepts clés (Loi 25, vulnérabilité des consommateurs, bannières de sécurité, technologies financières) dans le but de suggérer des solutions pour allier la protection des données, le design axé sur l'utilisateur et la conformité légale des paramètres de sécurité. Il sera de ce fait présenter tout au long du chapitre 1 la littérature portant sur les concepts clés mentionnés précédemment (évolution de la Loi 25, vulnérabilité des consommateurs, marché de la Fintech au Canada / Québec, Design UX ainsi que les différents modèles théoriques). Le chapitre 2 mettra en avant le cadre conceptuel ainsi que les hypothèses de recherche soigneusement définies. Le troisième chapitre exposera par la suite la démarche de recherche en débutant par le plan expérimental, la procédure de collecte des données et une présentation des instruments de mesure établis. Le chapitre 4 va se focaliser sur la présentation et l'analyse des résultats effectués. Le chapitre 5 qui est le chapitre final proposera une discussion des résultats obtenus en lien avec les travaux littéraires, des recommandations de gestion et il va souligner les limites et les perspectives pour de probables futures recherches.

CHAPITRE 1
REVUE DE LA LITTÉRATURE

Une revue de littérature est une analyse spécifique, détaillée et critique des travaux majeurs en cours sur un sujet spécifique (Jaillet, A. et Mabilon-Bonfils, B., 2021). Elle offre la possibilité de maîtriser le domaine de recherche et d'acquérir les connaissances essentielles sur les travaux de recherche menés dans ce secteur.

Ce chapitre expose les bases théoriques sur lesquelles repose notre thème de cette recherche, qui est d'illustrer l'impact de l'application de la Loi 25 sur la vulnérabilité des consommateurs québécois dans le domaine des technologies financières. Notre revue de la littérature débute par une présentation de la Loi encadrant la protection des données, ensuite une définition du concept de vulnérabilité du consommateur, du marché de la Fintech au Canada et au Québec, et enfin une présentation de la conception du Design UX dans le secteur des Fintechs.

1.1 Évolution de la Loi encadrant la protection des données personnelles

1.1.1. La protection intégrée des renseignements par le Centre pour la Défense de l'Intérêt Public (CDIP) de 2016 à 2017

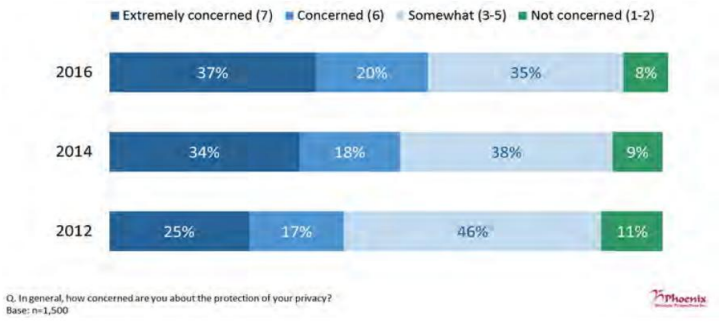
Le choix du consommateur d'utiliser les appareils dits intelligents est motivé, selon la littérature, par des considérations de popularité, de convivialité et le prix des technologies données (Kelly et al., 2013, Kim et al., 2008) malgré le risque potentiel d'utilisation abusive de ses données par les entreprises (Barth et De Jong, 2017). Néanmoins, les recherches démontrent que les consommateurs sont encore plus préoccupés par leur vie privée avec l'avènement des mégadonnées notamment par la distribution ambigüe des données et de leur utilisation par les tiers (Smith et al., 2017).

C'est fort de ce constat que le CDIP a financé la réalisation d'une étude dont le but était de relever l'intérêt des consommateurs relativement à un ensemble normalisé de paramètres de sécurités qui étaient appliqués en 2016 sur de différentes plateformes de navigation et leurs avis sur les fonctionnalités de la case relative à la protection de la vie privée (Lau, 2017). L'aboutissement de cette étude avait pour objectif de permettre aux consommateurs de faire des choix éclairés et de donner un consentement significatif en matière de confidentialité.

Les points saillants de ce rapport importants pour notre étude sont :

- 92 % des Canadiens sont préoccupés au sujet de la protection de leurs renseignements personnels (Figure 1.1).

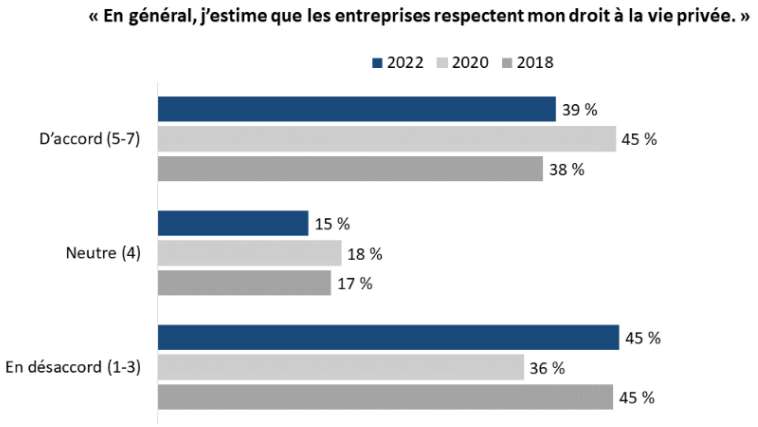
Figure 1-1: Préoccupation au sujet de la protection des renseignements personnels



Source : Commissariat à la protection de la vie privée du Canada, 2016

- Le sondage d'opinion publique a révélé que 74 % des répondants avaient l'impression que leurs renseignements personnels étaient moins protégés dans le cadre de leur vie quotidienne qu'ils l'étaient il y a 10 ans (Figure 1.2)

Figure 1-2: Opinion concernant le respect du droit à la vie privée par les entreprises



Source : Commissariat à la protection de la vie privée au Canada, 2023

- La plupart des participants aux groupes de réflexion trouvent les outils relatifs à la confidentialité difficile à comprendre ou à utiliser. Très peu de participants comprennent ou tentent même de lire les politiques de confidentialité et nombre d'entre eux ont conclu que les déclarations et les paramètres de confidentialité étaient modifiés à leur insu par les entreprises.
- Les participants ont insisté sur l'importance du droit de choisir quand ils partagent leurs renseignements et comment ceux-ci sont utilisés et divulgués à d'autres parties.
- Les participants aux grou
- pes de discussion préféraient généralement une case relative à la protection des renseignements personnels évidente, simple et facile à comprendre dotée d'un nombre limité d'options.

De ces résultats, le Commissariat à la protection de la vie privée (CPVP) au Canada a décidé que la protection intégrée des renseignements personnels sur mesure deviendra plus importante en vue de protéger la vie privée des canadiens et d'assurer qu'ils disposent de choix et de contrôles réels, notamment en matière de consentement éclairé visant la collecte, l'utilisation et la divulgation de leurs renseignements. Six recommandations ont été établies à savoir :

- La « Protection intégrée des renseignements » développée dans le présent rapport doit être prise en compte par toutes les entreprises et les organismes privés dotés d'une présence en ligne et idéalement coordonnée par une association du secteur (telle que les Normes canadiennes de Publicité ou la Network Advertising Initiative).
- Le CPVP doit publier des lignes directrices sur l'adoption et la mise en œuvre de mesures de protection de la vie privée par les services et application en ligne, l'accent étant particulièrement mis sur les organisations privées. Il doit également, de manière générale, mettre en relief la protection intégrée des renseignements personnels sur mesure, notamment : la publication de rapports et de documents de recherche, l'instauration de lignes directrices claires et d'exemples ou la création d'une norme de protection intégrée des renseignements sur mesure.
- Les exigences de protection des renseignements sur mesures doivent être inscrites dans la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) fédérale.

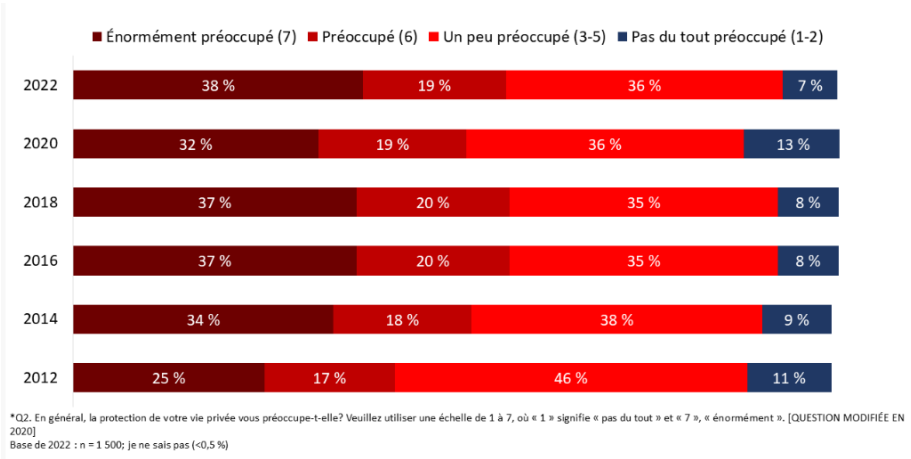
1.1.2. Commissariat à la Protection de la Vie Privée (CPVP) et perceptions des canadiens vis-à-vis de la confidentialité de leurs données.

Le CPVP est l'organisme mandaté par le gouvernement du Canada pour veiller au respect de la Loi sur la protection des renseignements personnels et pour accomplir sa mission principale qui est de protéger et promouvoir le droit à la vie privée, il effectue chaque deux ans des recherches quantitatives auprès de l'ensemble de la population afin de recueillir les renseignements dont il a besoin pour s'acquitter de sa responsabilité fondamentale de protéger le droit à la vie privée et faire rapport à cet égard.

Le but de la présente étude est de permettre au Commissariat d'analyser les préoccupations et les attitudes des Canadiens à l'égard de la protection de la vie privée, leur connaissance des institutions chargées de la protection de la vie privée et leur opinion sur la gestion des renseignements personnels. Il ressort de ce rapport que :

- La grande majorité (93 %) des répondants sont à tout le moins quelque peu préoccupés par la protection de leur vie privée (Figure 1.3). Comparativement à 2020, la proportion des Canadiens qui se disent énormément préoccupés par la protection de leur vie privée a augmenté de 6 points de pourcentage (de 32 % à 38 % en 2022).

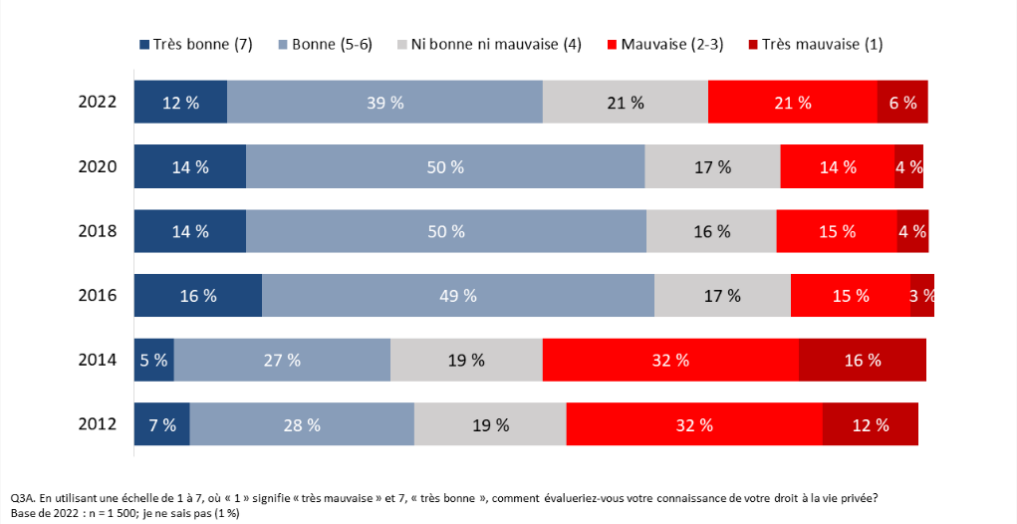
Figure 1-3: Niveau de préoccupation concernant la vie privée des consommateurs



Source : Commissariat à la Protection de la Vie privée au Canada, 2023

- Environ quatre Canadiens sur dix (39 %) estiment en général que les entreprises respectent leur droit à la vie privée. En revanche, une minorité importante de Canadiens (45 %) sont en désaccord avec cet énoncé. La confiance envers les entreprises quant au respect du droit à la protection des renseignements personnels a diminué de six points de pourcentage depuis 2020.
- La majorité des répondants font confiance au gouvernement du Canada, aux banques et aux organismes d'application de la loi pour protéger leurs renseignements personnels; mais leur confiance envers d'autres organisations est limitée (Figure 1.4).

Figure 1-4: Connaissance générale des droits en matière de vie privée



Source : Commissariat à la Protection de la Vie privée au Canada, 2023

1.1.3. Les principaux enjeux liés à la protection de la vie privée des Canadiens de 2022 à 2023

La Loi 25 est un règlement entré en vigueur à partir de septembre 2022 au Québec et qui a pour but d'apporter des modifications importantes à la Loi sur la protection des renseignements personnels dans le secteur privé tout en modernisant des dispositions législatives en matière de protection des renseignements personnels (Commission accès à information du Québec, 2023). Comme vu dans les deux études réalisées à la demande du commissariat à la protection de la vie privée au Canada, les consommateurs ne font pas confiance à leurs informations collectées et utilisées par les entreprises privées. Ce règlement vient donc dans le but de réguler la collecte et

l'utilisation des données clients dans le secteur privé au Québec, mais aussi d'accroître le sentiment de confiance des consommateurs au système mis en place.

Nous sommes rendus à la dernière phase de l'application de cette loi (septembre 2024), sa mise en application a débuté en septembre 2022 et la deuxième phase en septembre 2023. Les obligations des entreprises privées dès l'entrée en vigueur de la première phase étaient principalement de désigner des personnes responsables de la protection des renseignements personnels, publier ses informations sur le site de l'entreprise, prendre des mesures en cas d'incident de confidentialité et respecter le nouvel encadrement de la communication des données des clients (Commission accès à information du Québec, 2023).

La mise en application de la deuxième phase depuis septembre 2023, qui s'ajoute à la mort annoncée des cookies sur Chrome en 2025, est beaucoup plus contraignante pour les entreprises du secteur privé (Leprince, 2023). Il s'agit pour ces entreprises de :

- Établir des politiques et des pratiques encadrant la gouvernance des renseignements personnels et publier de l'information détaillée sur celles-ci en termes simples et clairs sur le site internet de l'entreprise ou, si elle n'a pas de site, par tout autre moyen approprié;
- Réaliser une évaluation des facteurs relatifs à la vie privée lorsque la Loi l'exige, par exemple avant de communiquer des renseignements personnels à l'extérieur du Québec;
- Respecter les nouvelles règles entourant le consentement à la collecte, à la communication ou à l'utilisation des renseignements personnels, de communication des renseignements personnels à l'extérieur du Québec, sans le consentement de la personne concernée;
- Détruire les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les anonymiser pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d'un délai de conservation prévus par une loi.

Pour pouvoir respecter ces engagements, les entreprises doivent de ce fait mettre en œuvre des politiques de gouvernances des renseignements personnels. Elles devront faire l'inventaire des

renseignements détenus par l'entreprise, évaluer leur sensibilité, le tenir à jour et préciser les rôles et responsabilités du personnel impliqué dans la protection des données privées.

Pour ce qui est de la troisième phase de l'application de cette Loi qui a pris effet en septembre 2024, à titre de personne exploitant une entreprise, il s'agissait particulièrement de répondre aux requêtes de portatibilité des informations personnelles (Commission accès à information du Québec, 2023).

1.2 La vulnérabilité du consommateur québécois en ligne

1.2.1 Définition du concept de vulnérabilité en marketing

Comprendre le concept de vulnérabilité des consommateurs selon un cadre précis permet de décrire les situations auxquelles ils sont confrontés (Hill et Sharma, 2020) et agir en établissant des stratégies organisationnelles pertinentes pour protéger la vie privée des consommateurs (Deslée, 2023). Les œuvres littéraires rédigées autour du concept de vulnérabilité du consommateur ont mis en lumière un continuum de travaux réalisés au fil des ans.

La vulnérabilité du consommateur est perçue en 1997 comme étant un aspect sociodémographique susceptible de nuire à un individu défini à priori comme désavantagé (Smith et Cooper-Martin 1997 dans Beaudaert et Nau, 2021). Baker, Gentry et Rittenberg proposent une approche marketing à ce concept et définissent la vulnérabilité comme étant un état d'impuissance causé par un déséquilibre dans les interactions sur le marché ou par la consommation de produits et de messages marketing (Baker et al., 2005). Hill et Sharma reviennent sur cette notion en 2020 et suggèrent une définition plus avancée de la vulnérabilité comme un état dans lequel les consommateurs subissent un préjudice parce que leurs accès aux ressources et leur contrôle sont restreints de manière à inhiber considérablement leur capacité à fonctionner sur le marché (Hill et Sharma, 2020). Cette définition a permis de mettre en lumière divers facteurs de l'expérience de vulnérabilité. Il est donc correct de dire que les perceptions liées à ce concept sont causées par des situations d'incertitudes et de risques, lesquelles génèrent des sentiments de craintes ou de peur (Martin et al., 2017).

1.2.2 Vulnérabilité réelle et vulnérabilité perçue

De plus en plus de recherches en marketing portent sur les enjeux de la vulnérabilité sur le comportement des consommateurs en ligne avec l'ère du Big Data, de la collecte et du traitement des données personnelles. La mise en œuvre de ce cadre conceptuel revêt une importance, car il intègre les progrès des recherches précédentes sur les diverses formes de vulnérabilité du consommateur. Les travaux de Martin et al. ont ressorti deux types de vulnérabilité : vulnérabilité perçue et vulnérabilité réelle. Ils distinguent la vulnérabilité perçue par le consommateur comme étant une réaction émotionnelle (anxiété, frustration, peur) causée par l'incertitude et le risque liés à l'accès et à l'usage des données privées, de la vulnérabilité réelle qui se manifeste en raison d'utilisations abusives des informations personnelles (Martin et al., 2017).

Les analyses menées sur le terrain auprès de 15 entreprises par Martin et al. en 2017 et les travaux de Martin et Murphy (2017) ont démontré l'existence de 4 types de vulnérabilité et de la relation intrinsèque entre les notions de violation et confiance des clients et leur conséquence sur les effets de la vulnérabilité des données clients :

- La vulnérabilité liée au risque d'accès aux données personnelles : le simple accès aux données des clients par les entreprises en ligne revient au fait que ces entreprises détiennent des dossiers numériques sur leurs clients, ce qui leur permet de transférer ces données avec des tiers. Cette vulnérabilité résulte donc des craintes du consommateur quant aux risques qui adviennent de la publication des renseignements personnels ou de leur surveillance (Deslée, 2023).
- La vulnérabilité par contagion ou vulnérabilité aux violations de données : ce type de vulnérabilité inclue le fait qu'une entreprise qui détient nos informations ou un de ses concurrents ait été victime d'une véritable faille de sécurité. À la suite d'une fuite de données dans une entreprise qui détient les informations du client, la perception de vulnérabilité augmente, tout comme lors de violations chez des concurrents proches, car ces évènements renforcent la conviction que des violations similaires sont envisageables (Martin et al., 2017).

- La vulnérabilité par débordement ou vulnérabilité au risque d'atteinte à la vie privée : elle est caractérisée par une situation dans laquelle le consommateur se sent vulnérable en raison de la perte de sécurité d'une entreprise similaire à celle qui détient ses informations personnelles (Martin et al., 2017).

- La vulnérabilité manifeste pour la vie privée : c'est un état dans lequel le consommateur subit réellement des préjudices d'une mauvaise utilisation des données personnelles. Ce type de vulnérabilité est la plus grave, car elle dépasse la simple susceptibilité pour devenir un véritable préjudice à cause des divulgations et activités frauduleuses.

1.2.3 Vulnérabilité vécue et vulnérabilité observée

Dans l'objectif de mieux comprendre les différents évènements préjudiciables pour le consommateur en ligne, les récentes recherches menées par Hill et Sharma (2020) offrent également une base conceptuelle sur la vulnérabilité : les ressources limitées et le contrôle restreint comme antécédents majeurs de la vulnérabilité des consommateurs. Tous les consommateurs vulnérables sont exposés à des dommages, car leur accès aux ressources et leur contrôle sur celles-ci sont restreints commercialement (Hill et Sharma, 2020). Afin de mieux expliquer la vulnérabilité perçue relative aux données privées à travers le cadre des ressources-contrôles, les auteurs distinguent différents types de ressources à savoir :

- Ressources individuelles : capacités psychologiques, physiologiques, caractéristiques du consommateur ainsi que ses actifs
- Ressources interpersonnelles : capital social, sentiment d'appartenance, soutien social
- Ressources structurelles : pratiques commerciales, cadres règlementaires, etc.

La catégorisation des ressources présentées ci-dessous est la même qui est utilisée pour présenter la conceptualisation du contrôle :

- Contrôle individuel : comme antécédent, nous avons des perceptions psychologiques telles que l'auto-efficacité et la confiance en soi

- Contrôle interpersonnel : on peut considérer les structures hiérarchiques sociales et les organisations religieuses comme exemples.
- Contrôle structurel : Par exemple, le contrôle effectué par les organismes et influencé par des éléments externes tels que les avancées technologiques.

Ressortir ainsi les liens dynamiques entre les ressources limitées et le contrôle restreint permet de mieux comprendre à partir de quels facteurs le sentiment de vulnérabilité se développe chez les consommateurs (Deslée, 2023). Grâce à cette recherche, deux approches ont été mises en exergue par Hill et Sharma pour identifier l'état des lieux : approche par les expérimentateurs et approche par les observateurs. La vulnérabilité vécue (approche expérimentateur) est identifiée comme une situation où des personnes ont l'impression de subir et d'identifier les facteurs qui leur procurent ce sentiment. La vulnérabilité observée quant à elle fait référence au cas où ce sont des personnes tierces telles que les décideurs politiques qui détectent et identifient la vulnérabilité chez les individus, que les individus observés aient détecté ou pas (Hill et Sharma, 2020). Ces deux méthodes d'identification se distinguent notamment par la personne qui perçoit le sentiment de vulnérabilité.

L'un des enjeux de notre recherche est de déterminer les facteurs influençant le sentiment de vulnérabilité de l'utilisateur québécois en ligne et de proposer aux entreprises des méthodes favorisant la suppression de ce sentiment afin de contribuer au développement de la confiance des utilisateurs. C'est dans ce sillage que nous utilisons le cadre conceptuel ressources-contrôle pour proposer un examen holistique de la vulnérabilité perçue (proposée par Martin et al. en 2017) par les consommateurs québécois après la mise sur pied de la Loi 25 dans le secteur de la Fintech.

Dans le contexte de notre étude, nous nous concentrons uniquement sur la vulnérabilité perçue du point de vue des consommateurs, c'est-à-dire comment ils perçoivent subjectivement leur exposition aux risques lors de l'utilisation des services Fintech. Cette recherche utilise une démarche expérimentale qui consiste à exposer les participants à divers systèmes d'information et de protection des données, dans le but d'analyser l'impact de ces stimuli sur la vulnérabilité perçue, ls perceptions connexes et les intentions d'adopter des services Fintech. Cette approche conceptuelle et méthodologique garantit une concordance directe entre l'examen de littérature, le cadre théorique suggéré et les études empiriques qui seront présentées par le suite, en mettant

l'accent sur les processus perceptifs et cognitifs qui influencent les actions des utilisateurs dans les contextes financiers numériques.

1.3 Marché de la Fintech au Canada et au Québec

Innovation financière, technologies de pointe, renouveau de l'industrie du digital, start-up ou encore PME du secteur financier, telles sont les expressions attribuées à la Fintech en 2024. La définition qui revient le plus souvent de la Fintech, contraction des mots Finance et Technologie, est qu'elle désigne l'utilisation des moyens technologiques pour développer, améliorer et offrir des produits et services financiers (Cachecho et Prom Tep, 2022). La Fintech est un domaine qui englobe une diversité de services financiers regroupés par secteurs tels que les marchés de capitaux, gestion de patrimoine et d'actifs, technologies de paiements, de prêts et d'assurance, le financement participatif pour ne citer que ceux-là.

L'essence de l'existence des Fintechs repose sur une proposition de sources d'innovations à travers divers services financiers et des solutions digitales ainsi qu'une approche plus centrée sur le client. Il revient donc aux entreprises de ce secteur d'adopter des normes de conceptions (idéation, création, réalisation de prototypes et d'affinage) de l'interface et de l'expérience utilisateur modernes afin de rendre le parcours client sur leur site web moins stressant et stimuler un comportement financier sain. Pour ce faire, la protection des données des utilisateurs par les entreprises Fintech est un enjeu véritable pour les deux parties.

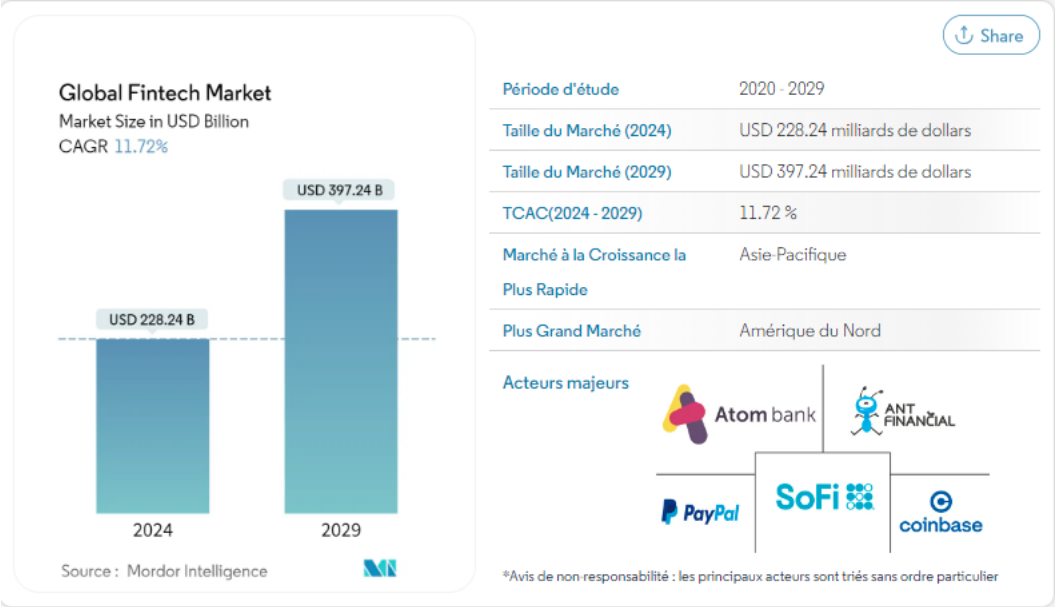
1.3.1 Présentation du marché de la Fintech au Canada

La technologie financière a connu une véritable croissance fulgurante après la crise financière mondiale de 2008/2009 qui a amplifié le besoin de solutions technologiques pour faciliter les transactions virtuelles (Selma et al., 2021). Il est indéniable que ces dernières années, de nombreuses avancées technologiques ont eu une répercussion directe ou indirecte sur les activités financières, ce qui a créé un vif engouement chez les investisseurs à la recherche de nouvelles opportunités sur le marché des technologies.

En 2015, les investissements dans les entreprises Fintech ont connu une augmentation de 75%, atteignant 22,3 milliards d'USD l'année précédente. En tout, les entreprises Fintech ont été investies avec plus de 50 milliards d'USD depuis 2010 (Skan et al., 2016).

En 2024, la valeur du marché mondial des technologies financières est de 228,24 milliards USD et il est prévu qu'elle atteigne 397,24 milliards USD d'ici 2029. (Mordor Intelligence, 2024). Le marché de la Fintech en Amérique du Nord représente le plus grand marché comme précédent dans la figure suivante.

Figure 1-5: Taille du marché mondial des technologies financières



Source : Modor Intelligence, 2024.

La carte du marché des entreprises de Fintech au Canada est définie par les entreprises de **sociétés technologiques** qui proposent des services dans le domaine des **services financiers** ou qui produisent, distribuent et gèrent elles-mêmes des produits financiers (Fitzgerald, 2019). Ce marché est passé de 12 sous catégories en 2019 pour 18 en 2024. Quelques points forts du marché des services financiers au Canada (McKinsey&Compagny, 2024):

- Le secteur bancaire canadien est vaste comparé aux autres pays de la G7 : En 2023, les revenus bancaires s'élevaient à 7,9 % du PIB, alors qu'ils étaient de 5,8 % aux États-Unis et de 5,6 % dans les autres économies développées. Avec une estimation de revenus de 136 milliards de dollars en 2022, il fait partie des dix plus importants marchés d'assurance à l'échelle mondiale.

- Le domaine des services financiers au Canada présente une forte concentration, ce qui témoigne fréquemment de l'impatience des innovateurs à faire avancer les choses. En 2022, les 5 banques les plus importantes (Banque Royale du Canada, Banque Canadienne Impériale de Commerce, Banque Toronto Dominion, Banque Scotia, Banque de Montréal) représentaient plus des trois quarts des revenus bancaires, tandis que les 6 compagnies d'assurance les plus importantes représentaient près de 50 % des revenus du domaine.
- La volonté d'adoption de nouvelles technologies représentées par un taux de pénétration des téléphones intelligents, de l'utilisation d'internet et le niveau d'éducation supérieure au Canada lui permet de se classer parmi les cinq premiers pays au monde.

Cependant, un rapport Pulse of Fintech de la firme KPMG international publié en février 2024 dévoile une faible adoption des services financiers au Canada par rapport aux autres pays économies évoluant dans le même secteur d'activité durant le deuxième semestre 2023. Les investissements dans les sociétés canadiennes spécialisées dans la technologie financière ont connu un ralentissement significatif l'année dernière, avec une baisse de moitié du nombre de transactions et une baisse de près de 30 % de leur valeur (KPMG Canada, avril 2024). Ces résultats témoignent de la diminution des investissements à l'échelle mondiale, avec une baisse de 65 % du nombre de transactions et une diminution de 73 % de leur valeur. Néanmoins, la dernière édition de Pulse of Fintech par KPMG (KPMG international, août 2024) présente de belles perspectives pour la Fintech canadienne par le fait que le Canada fait parti des pays dont les transactions d'investissements de 1 milliard de dollars et plus ont été effectuées dans le domaine de la Fintech durant le 1er semestre 2024 et dont le volume de transactions offre un signe d'optimisme pour ce marché.

1.3.2 Présentation du marché de la Fintech au Québec

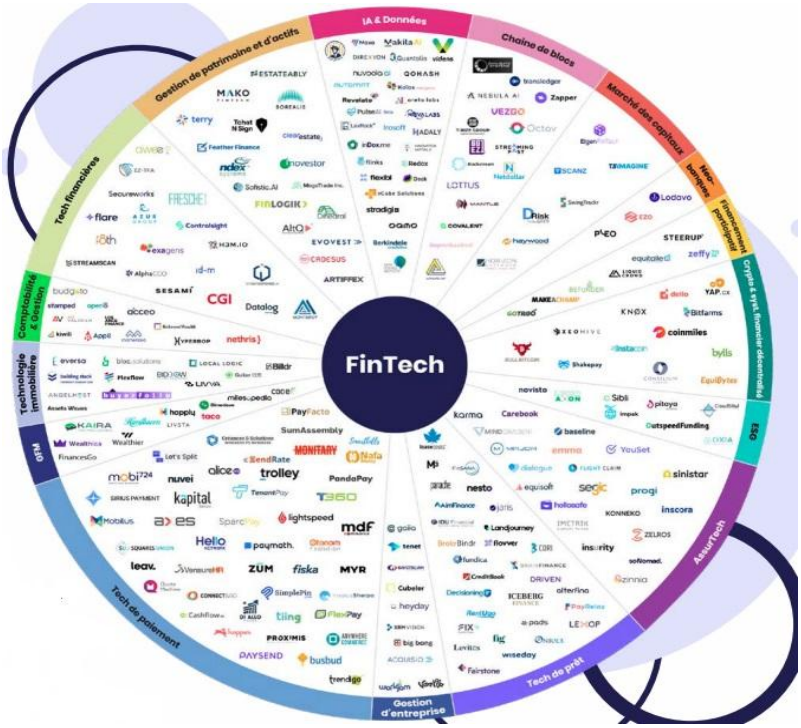
Depuis 2023, un écosystème Fintech dynamique a permis de placer le Québec parmi les régions qui connaissent la croissance la plus rapide au monde et il demeure un acteur important dans cet univers. Pendant que nous examinons les principales tendances de cet écosystème qui ont marqué le premier semestre de l'année 2024, voici présentés quelques points saillants (Rapport Québec Fintech semestriel 2024, juin 2024) :

- Ces dernières années, l'écosystème des Fintechs québécoises a connu une forte expansion, avec plus de 21 % d'entre elles ayant été créées après 2020 et 257 entreprises Fintech dont le siège social est basé au Québec.
- Le développement de Montréal en tant que centre Fintech se poursuit, avec 80 % des Fintechs implantées au Québec ayant leur siège social dans la métropole montréalaise.
- Plus de 19.900 personnes sont employées par ces 257 Fintechs au Canada, contre 86 000 personnes employées à travers le monde.
- 285,32M$ CA ont été collectés durant 8 tours de financement par les Fintechs du Québec et 10 transactions impliquant une Fintech québécoise en tant qu'acquéreur ou société acquise ont été réalisées en 2023.
- Pour marquer l'évolution de ce secteur en 2024, 63,9 millions de dollars américains ont été obtenus par six fintechs québécoises durant ce 1er semestre en plus de six accords d'acquisition impliquant des Fintechs basées au Québec ont été annoncés.
- Les secteurs phares au sein de cet écosystème sont les technologies de paiement (Paytech), les technologies de prêt (Lendtech), les IA & Données.
- Pour terminer, ces entreprises de Fintech sont composées de 60 % de petites entreprises (de 5 à 99 employés), ce qui représente environ 16 % de l'ensemble des emplois créés au Québec. Les grandes entreprises (500+ employés), quant à elles, ne représentent que 4 % de toutes les Fintechs québécoises, mais elles emploient 74 % de tous les employés des Fintechs du Québec au Canada.

Le Québec bénéficie d'un écosystème fintech dynamique, comptant actuellement 257 entreprises en activité au Québec. La création de plus de 8 % de ces entreprises entre 2023 et 2024 (à nos jours) témoigne de la croissance et de la dynamique du domaine ces dernières années. L'arrivée de nouveaux acteurs met en évidence l'attrait du Québec en tant que centre d'innovation en technologie financière, soulignant ainsi son rôle essentiel dans le paysage en constante évolution de l'industrie fintech. Le fait que de nouvelles entreprises émergent constamment, ainsi que l'augmentation de 3,6% de la main-d'œuvre entre 2023 et le 1er semestre de 2023, témoigne davantage de la dynamique entrepreneuriale du Québec, de son infrastructure et de sa capacité à attirer et à soutenir des entreprises innovantes dans le domaine de la technologie financière.

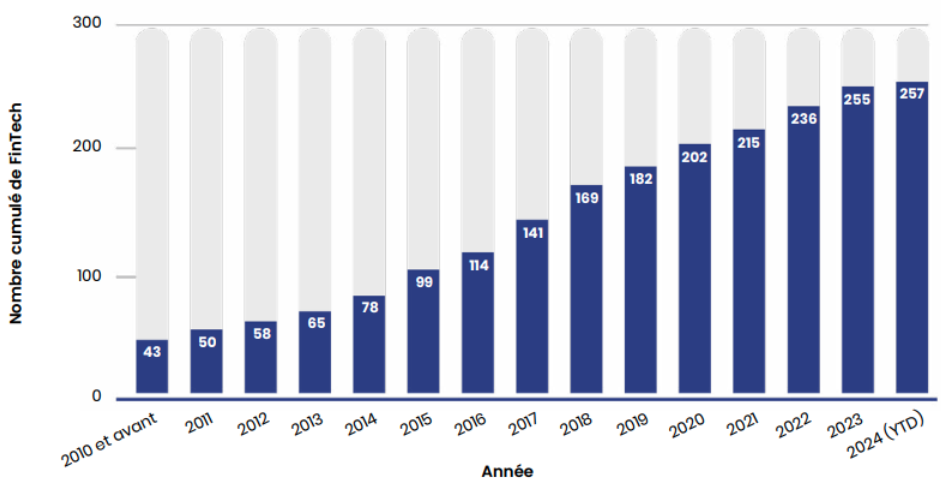
Voici présentés la carte du marché des Fintechs ayant leur siège social au Québec et le graphique de croissance des Fintechs québécoises au fil des ans.

Figure 1-6: Cartographie des Fintechs ayant leur siège social au Québec



Source : Rapport Québec Fintech semestriel 2024, juin 202

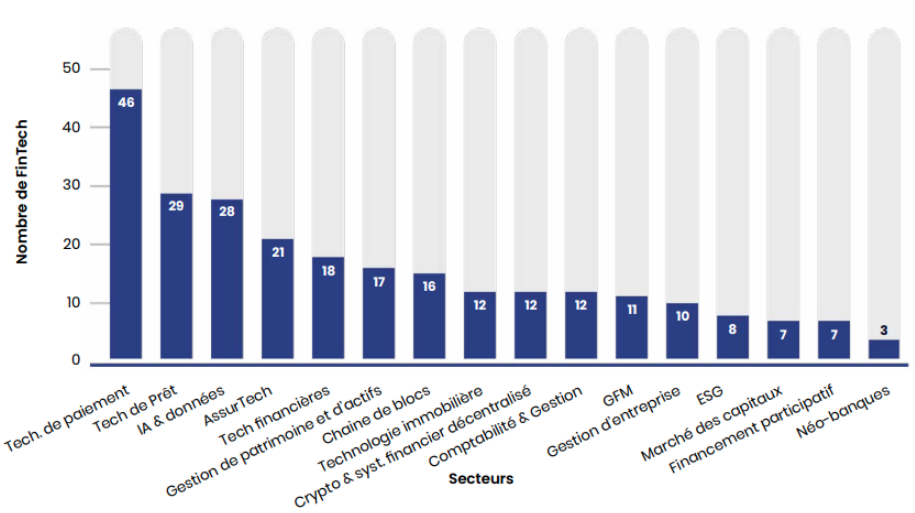
Figure 1-7: Croissance des Fintechs québécoises au fil des ans



Source : Rapport Québec Fintech Semestriel 2024, juin 2024

Comme présenté dans la figure ci-dessous, le secteur des technologies de paiement représente le secteur des Fintechs qui domine l'industrie de la Fintech au Québec, suivi de loin par les secteurs des technologies de prêt et ceux de l'IA & Données grâce à leur innovation significative et leur fort potentiel croissant.

Figure 1-8: Croissance des Fintechs québécoises par secteur



Source : Rapport Québec Fintech Semestriel 2024, 2024

1.3.3 Les enjeux de la Fintech au Québec

Aux vues des informations partagées ci-dessous, l'industrie des technologies financières au Québec se doit de comprendre comment exploiter pleinement l'épanouissement de ce secteur d'activités bien que leur développement engendre des problématiques significatives qui ont un impact sur la manière dont ces servives sont perçus et adoptés par les consommateurs. Pour ce faire, McKinsey&Company a réalisé une étude auprès des professionnels et universitaires de la Fintech qui révèle cinq secteurs où les évolutions seront cruciales pour la croissance à long terme du secteur à savoir : le comportement des consommateurs, les partenariats stratégiques, le financement, la règlementation en vigueur et les compétences dans le domaine de la Fintech.

Dans le cadre notre rapport, notre terrain d'intérêt s'établit autour des enjeux liés au comportement du consommateur et à ceux des règlementations, car ils sont directement liés aux notions de perception de vulnérabilité et de confiance vis-à-vis des plateformes numériques. Effectivement, convaincre les utilisateurs d'opter pour des plateformes Fintech et en particulier pour des segments jugés fragiles (les utilisateurs débutants ou encore les les immigrants), nécessite de limiter les inquiétudes relatives à la protection des données, à la transparence dans les opérations et au contrôle des données privées.

Au moment où chaque gouvernement adopte des lois en vue de mieux réguler la protection des données personnelles des consommateurs et donner le pouvoir à ces consommateurs, le secteur de la Fintech ne pourrait y échapper et étant un secteur qui repose essentiellement sur les innovations technologiques, il serait crucial pour chaque entreprise de respecter les lois encadrant la protection des données des consommateurs, car beaucoup d'informations sont échangées durant le parcours client sur les sites web des différentes entreprises et préconiser l'application d'un Design UX légal, responsable et éthique afin de favoriser un sentiment de confiance des utilisateurs envers les services financiers et par conséquent favoriser l'adoption de ces services. L'entrée en vigueur de la Loi 25 a donc pour but d'aborder ces inquiétitudes en intensifiant la sauvegarde des informations personnelles et en restituant aux utilisateurs une autorité renforcée sur leurs données.

Par conséquent, c'est dans un cadre juridique rigoureux que cette évolution doit se faire, tout en assurant la sécurité et la confidentialité des transactions et des informations, ainsi que l'intégrité des marchés de la Fintech au Québec, des éléments qui sont essentiels pour l'étude de la vulnérabilité perçue dans le contexte de la Loi 25.

1.4 Conception du Design UX dans le secteur des technologies financières

L'adoption par les banques et les technologies financières en matière de design et d'expérience utilisateur a été cruciale en raison de l'évolution de la technologie et des contraintes législatives encadrant la protection des données des consommateurs en ligne sans oublier la numérisation du système bancaire. Si une attention particulière est portée sur le design UX des

sites, applications ou logiciels des Fintechs, c'est grâce au contexte de plus en plus concurrentiel ajouté au fait que trop de personnes passent un temps considérable derrière leurs écrans ce qui constitue un enjeu considérable sur les volets éthique, légal et responsable de la conception UX.

1.4.1 Design légal des plateformes de Fintech.

Le Projet de *Loi C-27*, encore appelé *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, établit des règles de protection des renseignements personnels au Canada dans un contexte où les données circulent largement au-delà des frontières et où l'économie repose fortement sur l'analyse et l'échange de ces données (Parlement, 2020). Dans une même lancée et en s'inspirant particulièrement du règlement européen (Règlement général de la Protection des Données) en Europe, la *Loi 25* est adoptée au Québec dans le but de moderniser les dispositions législatives en matière de protection des renseignements personnels et apporter des modifications importantes à la *Loi* sur la protection des renseignements personnels dans le secteur privé (Commission accès à information du Québec, 2023). Toutefois, nous allons mettre un point d'honneur sur l'importance d'obtenir un consentement valide des utilisateurs par les sites ou les plateformes des entreprises privées du Québec.

- Projet de Loi C-27.

Le projet de Loi C-27 comprend la *Loi sur la protection de la vie privée des consommateurs*, la *Loi sur le Tribunal de la protection des renseignements personnels et des données* (Gouvernement du Canada, 2020) et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois.

L'objectif de ce projet de Loi est de garantir la protection de la vie privée des individus au Canada en établissant des normes fiables pour l'utilisation, la collecte et la communication des données personnelles. En pratique, cela implique que les entreprises canadiennes doivent d'abord avoir une connaissance et une compréhension approfondies des règles liées à l'application de cette Loi, puis mettre en œuvre des mécanismes rigoureux pour obtenir le consentement éclairé des utilisateurs avant de recueillir et d'utiliser leurs informations personnelles.

Le projet de loi C-27, tel qu'il est écrit, va profondément modifier le modèle d'application actuel en vertu de la LPRPDE (Loi sur la Protection des Renseignements Personnels et les Documents électroniques) en conférant au commissaire à la protection de la vie privée du Canada

(CPVP) d'importants pouvoirs d'ordonnance et le pouvoir de recommander l'imposition d'amendes. Un nouveau Tribunal de la protection des renseignements personnels et des données sera également créé afin d'entendre les appels concernant les ordonnances émises par le CPVP, ainsi que pour établir et imposer aux organisations les amendes recommandées par le CPVP. Les personnes auront aussi un droit privé d'action pour les préjudices réels subis (Cassell et al., 2020).

Cette mesure oblige de ce fait les institutions financières à gérer de manière efficace les informations personnelles des utilisateurs sur leurs différentes plateformes, tout en assurant la sécurité et l'intégrité des données, en respectant les nouvelles exigences de divulgation, d'accès et de suppression de ces données en accord avec la législation (Belky, 2023). Cela nécessite la création de protocoles de sécurité solides afin de préserver la sécurité des données des utilisateurs, tout en assurant que ces données ne sont utilisées qu'à des fins légitimes (Gouvernement, 2020).

- Retour sur la Loi 25 : Consentement éclairé

L'objectif principal de cette récente Loi provinciale est de fournir plus de droits aux consommateurs en ligne qui partagent leurs informations privées et instaurer dans le même élan un principe général de transparence (KPMG, juillet 2023). Il faut noter que la collecte des données sur le web se fait à travers : les cookies, les formulaires en ligne et les tiers. Que doit faire une entreprise afin que les consentements de ses utilisateurs soient considérés comme manifestes, libres dans un langage clair, simple et précis? Selon le rapport de la Commission d'accès à l'information, les informations dont l'entreprise doit partager lors de la collecte avec l'individu concerné sont (Commission d'accès à l'information, 2023) :

- Les buts pour lesquels ces informations sont collectées
- Les moyens par lesquels ces données sont collectées
- Les droits d'accès, de rectification et de retrait de consentement à l'utilisation des renseignements recueillis
- Les types de tiers à qui il est nécessaire de communiquer les renseignements pour les finalités définies
- La possibilité que les renseignements soient partagés à l'extérieur du Québec.

Vu les défis et le changement de paradigme qui se produisent dans le domaine du respect de la vie privée, il est primordial que les entreprises respectent les exigences de consentement envers

les clients, prospects sous peine d'amendes. Toutefois, en accordant une grande importance au consentement pour permettre la collecte de données, la Loi 25 a paradoxalement encouragé les plateformes à concevoir des design et des techniques afin d'obtenir ce consentement à tout prix. Plusieurs plateformes s'efforcent de tout faire pour échapper à la Loi. Ainsi, les sites internet et les applications offrent désormais des pop-up cookies avec des motifs sombres.

Selon Utz et al. (2019), 57,4% des bannières cookies sont élaborées de manière à ce que les utilisateurs sélectionnent les options qui ne favorisent pas la protection des données confidentielles. Malgré la règle de protection des données dès la conception et par défaut, la plupart des bannières cookies ont des paramètres par défaut qui permettent un accès intrusif aux informations personnelles (Soe et al., 2019).

1.4.2 Design éthique des plateformes de Fintech.

Depuis quelques années, nous assistons à plusieurs débats publics autour de l'éthique, entraînant la mise en place des normes incontournables par le législateur (Vuxe, 2018). Il en est de même dans le secteur du numérique avec l'application de la *Loi 25* au Québec. Après des scandales tels que celui de Facebook-Cambridge Analytica ou encore les 143 millions de clients touchés par un acte de piratage à Equifax en 2017, des normes commencent à être instaurées afin de mettre l'humain au cœur des préoccupations et lui déférer plus de pouvoirs.

Il en va de même pour le domaine du design, où des questions concernant la dimension morale des créations sont manifestées. Jusqu'à ce jour, certains concepteurs UX sont plus utilisés par les donneurs d'ordre dans le but de croître la consommaction de leur public cible, peu soucieux de l'aspect moral de leurs missions, au profit de l'attention du public ou des briefs qu'on leur fournit. Un design "Anti-éthique" qui se manifeste principalement par l'utilisation de "Dark Pattern" afin de guider les décisions du visiteur dans l'interface. Un travail réalisé sans aucun sens moral conçu pour tromper l'utilisateur (Vuxe, 2018).

- Qui sont les designers éthiques ?

Les questions autour de l'éthique dans le domaine du design des sites web, plateformes ou logiciels surviennent après des polémiques concernant les GAFAM (Google, Apple, Facebook,

Amazon, Microsoft), les géants du numérique dont le modèle économique s'appuie sur la dangerosité de l'exploitation des données personnelles (Quilliou-Rioual, mars 2023).

Le design éthique repose sur l'engagement du designer envers l'être humain et la société moderne (Usabilis, 2019). Les Designers Éthiques représentent une association qui explore les pratiques de conception numérique avec pour principales thématiques : le design persuasif, le design systémique, l'écoconception, l'accessibilité et l'inclusion (Designers Éthiques, 2024). Leurs principaux objectifs sont d'accompagner les designers au développement de produits éthiques numériques.

> *« Le design est devenu l'outil le plus puissant avec lequel l'homme forme ses outils et son environnement. » Victor Papanek, 1970,* ***Design for the real world, Human Ecology and Social change.***

De façon simple, on peut dire que l'éthique du design implique la création d'une connexion entre un produit et son utilisateur afin de favoriser des choix responsables et moraux (Nag, février 2022). Il s'agit donc de définir et de concevoir la notion de « Bonté » dans l'élaboration d'un produit qui cherche à apporter des avantages à l'utilisateur, ainsi qu'à son écosystème et à toute la société. Cependant, il n'existe pas une règle universelle qui préconise une structure de conception éthique des sites web. Nous pouvons toutefois nous servir de certains paramètres pour nous aider à définir si un design est éthique ou pas. Il s'agit de :

- L'utilisabilité : il s'agit de la capacité qu'a un utilisateur à atteindre un objectif précis en utilisant une fonction spécifique, une solution de conception ou un produit de façon efficace et satisfait. Pour ce, le système de conception doit être accessible à TOUS et avoir une grande facilité d'utilisation.
- La confidentialité : il est évident que nos informations privées ne sont plus autant « privées », mais le concepteur UX a l'obligation de les utiliser de manière appropriée.
- La persuasion : comment exercer une influence saine et non abusive sur les utilisateurs? La frontière est mince entre les facteurs tels que le temps passé en ligne, les conversions et le fait de vouloir soutirer le moindre fragment d'attention ou d'énergie du consommateur pour une utilisation maximale.

- La durabilité : l'environnement et l'écosystème dans lesquels sont conçus les produits ont un impact sur le changement et le réchauffement climatiques par exemple donc il devient crucial pour les entreprises et les concepteurs de ne plus considérer les principes de conception comme un second plan.
- La société : le designer éthique doit être conscient de l'impact de créations sur la santé mentale de l'individu auxquelles sont soumises ses créations. Il est donc nécessaire de prendre en compte ce volet dans l'exercice de ses fonctions.

- Gamification et Dark patterns

De nos jours, il est rendu impossible pour une marque de bâtir sa présence numérique sans accorder une importance particulière au Design UX (User Experience) de sa plateforme, particulièrement dans un secteur à l'affut de l'innovation comme celui de la Fintech. Cependant, les services de ce domaine dépendent des décisions financières délicates et d'une accumulation considérable des informations privées, ce qui entraine des actions relatives à la conception UX qui posent des questions éthiques et règlementaires cruciales suite à l'instauration de la Loi 25.

Au Royaume-Uni, 15 millions d'applications bancaires ont été téléchargées et près de 80 % des clients des banques utilisent les services bancaires en ligne ou mobiles au moins une fois par mois. Les sociétés financières embrassent la révolution digitale (Cordeiro and Weeves, 2016).Dans ce contexte, des méthodes de conception spécifiques comme la ludification et les dark patterns nécessitent une analyse particulière étant donné qu'elles ont le potentiel d'augmenter la vulnérabilité perçue des consommateurs ou, à l'inverse, d'aider à la diminuer en fonction de leur application.

❖ Gamification ou ludification

La ludification, plus connue sous le terme de gamification, représente un processus qui implique l'incorporation d'éléments et de mécanismes de jeu dans des champs ou des domaines qui ne sont pas ludiques, dans le but de renforcer l'implication, stimuler la motivation ou encore de favoriser les échanges (Deterding et al., 2014). La Fintech est un secteur en plein essor qui utilise différentes stratégies pour atteindre ses objectifs de développement, parmi lesquelles la

gamification. L'objectif principal de cette stratégie dans le monde des finances et de l'investissement est de rendre l'accès au financement plus accessible et de proposer des conseils en matière d'investissement, en particulier pour les individus ayant un budget limité (Maya et al., 2022). Il n'est plus obligatoire d'avoir une expertise financière pour avoir accès aux services financiers et cet aspect permet aux investisseurs novices et inexpérimentés d'être attirés par des applications financières qui leur offrent des interfaces utilisateur (UI) astucieuses et à des frais réduits.

Toutefois, lorsque la psychologie des consommateurs est exploitée dans le but de les manipuler et les inciter à faire des choses qui ne sont pas leur intérêt essentiel, la gamification se révèle contraire à l'éthique (McGonigal, 2011). Les principaux obstacles liés à la réalisation de cette pratique sont d'une part l'absence de prise en compte de ce qui constitue réellement une décision et d'une autre part le partage des informations privées (Maya et al., 2022). Les utilisateurs ont de ce fait manifesté une préoccupation grandissante due à la collecte d'informations par les structures financières, car la plupart de ces utilisateurs ont un manque criant de connaissances dans ce domaine et les conséquences des décisions prises constituent des risques financiers et éthiques d'atteinte à leur vie privée.

On ne pourrait totalement déposer toute la responsabilité du respect de l'éthique et de la confidentialité sur les entreprises financières sans considérer celle des individus qui doivent être éduqués aux usages, limites et garanties que présentent ces plateformes et logiciels avant de les utiliser afin qu'ils soient plus prudents, prennent des décisions mieux réfléchies et aient plus confiance au système. Il est donc crucial que les utilisateurs puissent exprimer leur consentement de manière explicite et complète, en étant conscients de l'ampleur de l'utilisation de leurs informations et des conditions de confidentialité du système exploité.

Au regard de la Loi 25, la gamification pose ainsi une question cruciale : comment allier implication de l'utilisateur et consentement éclairé ? Une approche responsable dans la création d'interfaces devrait permettre aux utilisateurs de manifester un accord clair, volontaire et éclairé, sans que les éléments de divertissement ne compromettent leur compréhension des termes d'utilisation ou de l'étendue de la collecte d'informations.

✓ Les « Dark Patterns »

Le terme « Dark Pattern » a été inventé par Harry Brignull en 2010 pour définir des « interfaces conçues pour inciter les utilisateurs à faire des choses qu'ils n'auraient pas faites autrement » (Kelly et Burkell, mars 2024). L'expérience utilisateur est cruciale pour influencer le comportement du consommateur afin de l'amener à souscrire à des services, s'abonner ou encore réaliser des achats en ligne. Comme toute médaille, l'UX a son revers qui est d'inciter, de manipuler et de tromper l'utilisateur à travers des techniques telles que les dark patterns, le nudging, les bannières cookies. Plusieurs études ont analysé les motifs sombres comme des méthodes de conception d'interface utilisateur trompeuses parmi lesquelles celles de Gray et al. en 2018 qui définit le concept comme une situation où un designer exploite sa compréhension du comportement humain (par exemple, la psychologie) et les préférences des utilisateurs finaux afin de mettre en place des fonctionnalités trompeuses qui ne sont pas dans l'intérêt de son utilisateur (Gray et al. 2018).

Il va sans dire que plusieurs chercheurs ont essayé de donner une définition à ce concept selon différents prismes (Marthur et al., 2019, Narayanan et al., 2020, Luguri & Strahilevitz, 2021, etc.), mais trois traits essentiels reviennent à chaque définition : (1) un paramétrage fréquent d'éléments présents dans les interfaces numériques, (2) conçu intentionnellement par un concepteur et (3) qui entraine un comportement de l'utilisateur qui va à l'encontre de ses intérêts (Lukoff er al. 2021). Les dark patterns identifiés par les professionnels de l'UX ont été identifiés par Gray et ses collaborateurs dans leurs travaux dans une typologie qui comprends cinq grandes catégories et 12 variantes parmi lesquelles :

- Le nagging (harcèlement): Cette technique est caractérisée par une redirection des attentes fonctionnelles persistantes au-delà d'une ou plusieurs échanges. On peut prendre pour exemple la mise à jour des logiciels tels que Microsoft qui interrompt votre travail par des menus avec nombreuses options sans réelle alternative pour l'utilisateur.
- L'obstruction : Le but ici est d'imposer une tâche plus difficile qu'elle ne devrait l'être dans le but de décourager de certaines actions. Nous avons pour exemple la

désinscription à des services où il devient extrêmement difficile de trouver la fonctionnalité qui permet de le faire.

- Le sneaking ou faufilage : qui essaie de dissimuler, de déguiser ou de retarder la divulgation d'informations précieuses pour l'utilisateur dans le but de faire augmenter par exemple le montant de l'offre entre le moment où ce dernier clique sur cette offre et celui où il met les informations de sa carte bancaire.
- L'interface interférence : Les talents du designer sont vraiment requis pour cette pratique, car il s'agit d'améliorer l'interface utilisateur afin de favoriser des actions précises au détriment d'autres, car les techniques utilisées vont guider l'utilisateur vers un but précis.
- Forced action : il s'agit ici d'inviter l'individu à réaliser une action spécifique afin d'accéder ou de continuer à accéder à des fonctionnalités définies.

En mettant des fonctionnalités moins accessibles ou en masquant des informations cruciales, ces différentes méthodes peuvent renforcer la perception de vulnérabilité des consommateurs et engendrer un affaiblissement de la confiance envers les plateformes Fintech. Dès lors, l'analyse des dark patterns est incluse dans cette recherche, non pas en tant qu'élément de design, mais comme un élément illustratif du sentiment de vulnérabilité et du non-respect des normes règlementaires. Leur étude aide à admettre comment des éléments d'interfaces affectent négativement la perception de sécurité et entraver l'adoption des services financiers numériques.

✓ Types et impacts observés des bannières de sécurité

➢ Types de cookies

Le gouvernement du Canada définit sur son site, pensezcybersécurité les cookies internet comme de petites données utilisées pour surveiller les actions et les informations des utilisateurs en ligne lors de leur navigation sur un site web (Gouvernement du Canada, décembre 2022). Par ailleurs, la CNIL (Commission nationale de l'informatique et des libertés) donne une définition plus détaillée du terme cookies : « *un cookie est un petit fichier informatique, un traceur, déposé et lu par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le*

type de terminal utilisé (ordinateur, Smartphone, liseuse numérique, console de jeux vidéos connectée à Internet, etc.) » (CNIL, septembre 2024). Nous pouvons dire que le cookie est un fichier informatique qui conserve nos informations privées lors de l'usage de technologies. Ces informations concernent notamment l'adresse IP de l'ordinateur, les sites internet visités, la durée de ces visites, les annonces publicitaires vues, les produits ajoutés au panier d'achats en ligne, les transactions réalisées, les configurations des sites telles que la région ou la langue, les données de géolocalisation, etc. (Audrey H., 2020). Ces cookies ont pour but d'optimiser des informations pour la publicité comportementale sur le web. Ils sont bénéfiques aussi bien pour l'utilisateur que pour l'entreprise en ligne car sans ces derniers, les clients seraient contraints de ressaisir tous les détails nécessaires à chaque visite sur le site internet.

La CNIL présente des modèles de cookie à savoir (CNIL, septembre 2024):

- Les cookies http,
- Les cookies « flash »,
- Le résultat du calcul d'empreinte dans le cas des fingerprinting (calcul d'un identifiant unique de la machine basée sur des éléments de sa configuration à des fins de traçage),
- Les pixels invisibles ou « web bugs »,
- Tout autre identifiant généré par un logiciel ou un système d'exploitation.

Des témoins et cookies se sont élaborés sur la base du principe du consentement présumé, connus sous le nom d'Opt-out, partant du postulat que le consentement du consommateur est implicite en lui offrant la possibilité de le révoquer s'il le souhaite. Plusieurs sites Web visités montrent des bannières de sécurité pour informer les utilisateurs qu'un cookie est placé sur le site et que leur navigation sur ce site revient à donner leur accord pour l'installation de ces cookies, méthode imposée à l'utilisateur.

L'accroissement des exigences règlementaires concernant la protection des informations privées a contraint les entreprises à modifier les interfaces de paramétrage du consentement des utilisateurs sur leurs plateformes. C'est dans ce cadre que les bannières de sécurité occupent une place cruciale : elles représentent le premier lien entre l'utilisateur et les réglages relatifs à la

gestion de ses données. Il en existe diverses catégories chacune illustrant un degré de variable d'adhésion aux principes de transparence, de consentement informé et de libre arbitre telles que :

- La bannière tout accepter : c'est la version la plus épurée et aussi la plus controversée des bannières. Il suffit à l'utilisateur de cliquer sur le bouton accepter pour activer tous les outils de traçage.
- La bannière accepter avec politique de confidentialité : Elle est identique à la bannière tout accepter mais offre en plus le lien vers la politique de confidentialité.
- La bannière cookies essentiels : Cette bannière offre le choix entre valider tous les cookies ou ne valider que les cookies essentiels pour le fonctionnement de la plateforme.
- La bannière accepter ou paramétrer : Elle offre deux choix visibles, accepter ou personnaliser, ses paramètres et offre à l'utilisateur de valider certains cookies à travers un panneau de configuration qui lui est proposé.
- La bannière consentement éclairé : Dans ce cas, aucun cookie optionnel n'est activé par défaut. Il est nécessaire pour l'utilisateur de choisir manuellement les types de cookies qu'il souhaite autoriser.

Les bannières cookies présentent une grande disparité tant au niveau du contenu que de la forme. Certaines mentionnent simplement que le site internet utilise des cookies sans plus de détails, tandis que d'autres offrent au visiteur la possibilité de configurer leurs paramètres de manière plus précise (Utz et al. 2019). La localisation du cookie diffère également d'un site à l'autre (en haut, en bas, à gauche, à droite de l'écran).

Soe et al., (2020) ont examiné les diverses formes que peut adopter un cookie. Selon eux, le genre de bannière peut jouer un rôle crucial. Par exemple, certains pop-up empêchent la navigation sur le site internet avant d'avoir pris une décision (blocking) ou refusent l'accès à ses services si le visiteur a refusé les cookies. Parfois, le site offre uniquement le bouton de confirmation, parfois une décision binaire (j'accepte ou je refuse) ; dans certains cas, l'utilisateur a même la possibilité de personnaliser ses paramètres (accepter ou paramétrer). Toutefois, les bannières cookies fluctuent

souvent entre une multitude ou une faible variété d'options pour configurer les caractéristiques de confidentialité (Utz et al. 2019).

De plus, la configuration peut varier de cases à (dé)sélectionner à des boutons à sélectionner à gauche ou à droite. La plupart du temps, le format et les couleurs employés sont influencés par le design du site internet. Le texte et les données évoluent également considérablement, notamment en ce qui concerne la raison de la collecte, l'explication du processus ou les motivations. De plus, il n'est pas toujours possible de trouver un lien vers des informations supplémentaires (Soe et al., 2020).

Pour fermer la fenêtre, certains cookies offrent une croix, sans pour autant indiquer s'il s'agit d'une action « Refuser » ou « Accepter » (Unmarked X), tandis que d'autres ne proposent pas de boutons de refus (No choice). Il arrive parfois que le bouton de refus ne puisse être utilisé qu'après avoir cliqué sur un lien de type « En savoir plus » (CascadeChoice). Dans quelques situations, il est nécessaire de déplacer un bouton panel d'un côté à l'autre afin de configurer les cookies, mais ils ne précisent pas quel côté correspond à « Accepter » et quel côté est « Refuser » (Sliders non labellisés). Enfin, en ce qui concerne le lexique, les plateformes ne font pas usage d'un terme analogue pour « J'accepte » ou pour l'action « Accepter » (Soe et al.2020).

Selon Soe et al. (2020), les annonces de consentement (notices de consentement) sont élaborées de manière extrêmement complexe, en particulier lorsqu'on prend en compte le nombre de clics nécessaires pour accéder à l'option de refus. En outre, la diversité des mots et des termes employés rend pratiquement impossible pour l'utilisateur de « désactiver » les patterns sombres et de reconnaître la voie qu'il souhaite suivre. Plutôt que des mots comme « Refuser » ou « Décliner », on a tendance à utiliser des expressions comme « En savoir plus » ou « Paramétrer ». Il est donc essentiel de développer et mettre en place une terminologie commune ou de concevoir un design neutre (Maindiaux, 2021).

Par ailleurs, des universitaires ont calculé qu’il faudrait lire sans relâche pendant 25 jours pour prendre connaissance de l’ensemble des politiques de confidentialités mentionnées (Gendreau, 2023). Les règlementations en vigueur dans les différents pays (RGPD en Europe et Loi 25 au Québec) obligent les entreprises à établir des bannières de cookies afin d’informer les utilisateurs

sur la collecte et l'exploitation de leurs données à travers les types de cookies laissées lors de leur navigation en ligne.

- Impacts observés de cookies

Quelques auteurs ont réalisé des études sur l'impact des cookies sur le taux de consentement de l'utilisateur à l'instar de Utz et al. (2019) et Nouwens et al. (2020) selon des critères tels que la page sur laquelle est placée la bannière, le vocabulaire utilisé, le nombre de propositions disponibles et la présence de liens (Maindiaux, 2021).

Selon Nouwens et al., (2020), le taux de consentement accroît de 22% lorsque l'onglet de refus n'est pas présent sur la première page. À contrario, lorsque l'utilisateur peut gérer ses paramètres dès la première page du site, le pourcentage de consentement est revu à la baisse (8 à 20%), peu importe le type de bannière.

Utz et al., (2019) ont analysé l'effet des critères suivant sur le consentement des utilisateurs envers les bannières de sécurité et ont eu comme résultats :

- Emplacement de la bannière : Le type de bannière placé en bas à gauche est celui qui a le plus d'interactions.
- Vocabulaire : L'utilisation des termes : « The site uses cookies » accroît les interactions et réduit les probabilités que l'utilisateur consente aux cookies que les termes : « This site collects your data ».
- Nombre de propositions disponibles : Les bannières qui ne proposent que deux options ont le pourcentage d'interactions plus élevé que celles dont l'utilisateur doit paramétrer la collecte de ses informations.
- Liens renvoyant aux politiques de confidentialité : ces derniers n'ont pas un réel impact sur le taux d'interaction

Il est à noter que ces résultats ne sont pas forcément représentatifs de toutes les populations, d'autres études peuvent présenter des résultats divergents.

1.4.3 Design responsable des plateformes de Fintech.

Avant de discuter du numérique responsable, il est important de définir préalablement ce qu'est le numérique. Le numérique désigne les technologies qui permettent de manipuler l'information en utilisant des nombres (le binaire 1 et 0) (Cohu, 2023). Le digital a profondément modifié notre manière de communiquer, de travailler, d'apprendre, de consommer des biens et des services et d'interagir avec notre environnement. Il a aussi engendré de nouvelles difficultés en ce qui concerne la préservation des données personnelles, la sécurité informatique et l'éthique.

Pendant que de nombreuses personnes passent de plus en plus de temps devant des écrans, l'impact environnemental et social des espaces numériques devient de plus en plus pressant. Il est primordial que les concepteurs d'expérience utilisateur commencent à accorder une grande importance à la durabilité environnementale dans leurs projets. Ceci assure non seulement une expérience utilisateur améliorée, mais contribue également au bien-être social et environnemental des individus et de la planète (Oliver, 2024).

✓ Vers un numérique responsable

Le numérique responsable est une approche d'amélioration constante qui cherche à réduire l'impact économique, écologique et social du numérique en s'appuyant sur trois axes de réflexion distincts (Cohu, 2023) :

- La réduction de l'empreinte (économique, sociale et environnementale) du numérique.
- La capacité du numérique à réduire l'empreinte (économique, sociale et environnementale) de l'humanité.
- La création de valeur durable / l'innovation responsable via le numérique pour réussir l'e-inclusion de tous.

- Les impacts environnementaux

Le fait que le numérique soit immatériel ne favorise pas la perception polluante de la réalité. Toutefois, en prenant du recul, nous sommes en mesure d'évaluer les conséquences que cela entraîne et de prendre des mesures pour mieux satisfaire les besoins. De nos jours, les grandes entreprises et les start-up prennent conscience des défis et perfectionnent leurs services informatiques afin de favoriser une transition vers un numérique responsable (Cohu, 2023).

La majorité des recherches abordent quatre critères environnementaux essentiels qui témoignent clairement de l'impact sur notre écosystème et qui sont aisément compréhensibles. Ce sont les matières premières non renouvelables, les émissions de gaz à effet de serre (GES), la consommation d'eau potable et la consommation de produits primaires utilisés pour la fabrication des appareils.

- Les impacts socio-économiques

L'évolution numérique n'a jamais cessé de rendre notre mode de vie plus avantageux et plus simple, au point qu'elle est devenue partie intégrante dans notre quotidien. Dans de nombreux domaines tels que la finance, la gouvernance, la santé, l'enseignement, etc., la technologie est devenue un outil de développement puissant (Parlement européen. Commission du développement, 2018). Paradoxalement, la technologie omniprésente suscite un véritable espoir pour l'avenir, mais suscite également certaines craintes chez la population telles que :

- **La protection des données et la sécurité**
- **L'impact sur la santé mentale** : d'une part, l'avènement de nouvelles technologies facilite l'accès aux soins en offrant des ressources comme les applications de méditation, des plateformes de thérapie et de soutien en ligne ou encore en permettant des consultations à distance sous forme de télémédecine. D'autre part, il est bien connu que les notifications régulières, les algorithmes de recommandation et la collecte de données personnelles peuvent engendrer des niveaux de stress élevés et des complexes pouvant altérer l'estime de soi.
- **Le rapport au travail** : La mise en place du numérique responsable pose des interrogations essentielles concernant la répartition des dépenses et des profits. L'externalisation des coûts environnementaux de la production d'appareils électroniques vers les pays en

développement est fréquente. Les normes environnementales sont moins rigoureuses et les employés sont souvent exposés à des conditions de travail dangereuses. En outre, les bénéfices économiques du numérique sont souvent monopolisés par une élite technologique, tandis que les conséquences sociales, comme la perte d'emplois dans les industries traditionnelles, sont assumées par les salariés.

✓ Pour un UX socialement durable

En général, la durabilité vise à prolonger et à améliorer la vie sur Terre, en entraînant des modifications écologiques, sociales et économiques. Cela implique de diminuer les déchets, de préserver les ressources naturelles et de préserver la planète sur le plan écologique. Dans le domaine social, la durabilité se réfère à la promotion de la responsabilité sociale et de l'égalité des chances. Économiquement, cela implique de préserver et d'améliorer l'accessibilité pour tous en ce qui concerne la facilité d'utilisation, les coûts et la disponibilité (Oliver, 2024).

Selon Miles Oliver (2024), l'UX socialement durable se focalise sur les conséquences sociales et économiques de la conception. Les aspects et les méthodes les plus efficaces que les concepteurs des plateformes de Fintech doivent appliquer comprennent une:

- **Conception inclusive et accessible** : Comme évoqué précédemment, les utilisateurs accordent une grande importance aux conceptions inclusives et axées sur l'équité, car elles contribuent à la durabilité sociale. Cela implique la création d'interfaces accessibles à tous, peu importe leurs compétences, ce qui peut englober une conception adaptée aux handicaps et aux limitations physiques, cognitifs et économiques.
- **Conception éthique** : La durabilité sociale de cette conception implique de respecter les utilisateurs tout en préservant des normes éthiques. Cela peut englober des aspects tels que l'obtention d'un consentement éclairé pour l'exploitation des données et la préservation de la sécurité et de la confidentialité des utilisateurs.
- **Conception centrée sur l'humain** : Il est essentiel de mettre l'accent sur la conception socialement durable en créant des interfaces axées sur l'utilisateur, ce qui implique qu'elles accordent la priorité aux besoins de l'utilisateur. Il est essentiel de

réaliser des études afin d'acquérir une compréhension approfondie des différents besoins des utilisateurs et des différentes perspectives.

- **L'automatisation :** La durabilité sociale implique également de permettre aux individus de s'autocontrôler. Grâce à l'UX, il s'agit de créer des interfaces personnalisables et d'accorder aux utilisateurs davantage de pouvoir sur leurs expériences en ligne.

1.5 Les modèles théoriques S-O-R, TAM et UTAUT

Dans le but de mieux saisir les processus psychologiques et comportementaux liés au sentiment de vulnérabilité et à l'adoption des plateformes de Fintech québécoises dans le cadre de la Loi 25, il est judicieux de faire appel à des théories vérifiées dans le domaine des sciences de l'information et du comportement du consommateur. Deux modèles se révèlent particulièrement instructifs à ce sujet : le modèle Stimulus – Organisme – Réponse (S-O-R) de Mehrabian et Russel qui aide à comprendre comment les éléments liés à la transparence ou à la sécurité affectent les états internes des personnes et leurs réactions comportementales ainsi que le Technology Acceptance Model (TAM), qui explique les facteurs influençant l'acceptation des technologies basée sur leur utilité perçue et leur facilité d'utilisation. L'introduction de ces modèles fournira une base conceptuelle pour l'examen des résultats empiriques à venir.

1.5.1 Le modèle S-O-R

Ce modèle a été présenté pour la première fois pas Merhabian et Russel en 1974 (Kumar et Rani, 2024) et il constitue un socle théorique pour confirmer le cadre intégré suggéré par les travaux de recherche actuels. Dans le contexte de leurs travaux en psychologie environnementale, Mehrabian et Russell (1974) ont permis de démontrer que lorsqu'il est confronté à tout environnement (Stimuli), l'individu répond par une réaction affective (Organisme) et par la suite par une réaction comportementale (Résultat) (Lemoine, 2012).

Conformément au modèle SOR, on distingue deux principales classes de facteurs qui influencent les réponses comportementales (Megzari et Dahab, 2025). D'une part, les facteurs externes, plus connus sous le nom de facteurs situationnels, qui sont déclenchés par des stimuli extérieurs et d'autre part, les facteurs internes. Parmi les éléments externes figurent les

caractéristiques du site internet (utilitaires et hédoniques), les offres promotionnelles, la performance de navigation sur la plateforme, les modèles de conception des bannières de sécurité, le design d'un site web, etc. Par ailleurs, les facteurs internes propres à chaque individu sont associés aux stimuli internes comme : l'utilité perçue, les caractéristiques du consommateur, l'attente de performance, l'influence culturelle, etc. Par conséquent, les stimuli sont considérés comme un ensemble d'attributs qui ont un effet significatif sur les perceptions des consommateurs (Mollen et Wilson, 2010). Dans notre cadre d'études, nous proposons les concepts d'utilité perçue, facilité d'utilisation, influence normative et attente de performance comme des stimuli internes et le type de bannière de sécurité comme un stimulus externe.

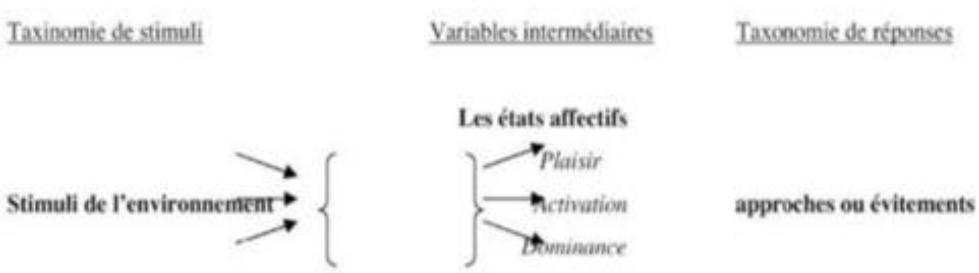
Comme dit précédemment, l'Organisme illustre les réactions émotionnelles qui surgissent face aux stimulations de l'environnement présent (Kumar et Rani, 2024). En d'autres termes, l'item Organisme du cadre SOR représente l'état cognitif et affectif transitoire des clients faisant suite à une succession d'activités psychologiques, révélant les mécanismes qui interviennent entre les stimuli et les réactions des clients (Amina et Smail, 2022). Dans le contexte numérique actuel, la notion de vulnérabilité des consommateurs est essentielle pour construire des relations durables et mutuellement rentables avec les utilisateurs. En règle général, le sentiment de vulnérabilité dénote une situation de fragilité à partir de laquelle l'intégrité d'un individu peut être compromise, amoindrie ou encore perturbée (Liendle M, 2012). En marketing, ce concept est caractérisé par une situation d'impuissance résultant d'un déséquilibre dans les échanges commerciaux ou de la consommation de produits et de communications marketing (Deslée A, 2023). Il existe diverses formes contextualisées de vulnérabilité dans le domaine du marketing parmi lesquelles la vulnérabilité perçue sur laquelle est centrée notre étude. À cet égard, ce rapport prétend que les variables liées aux stimuli ont un effet sur la vulnérabilité du consommateur qui constitue notre principal organisme.

Suite à une série d'activités cognitives ou psychologiques, l'organisme va déclencher des réactions comportementales sous forme de validation des clients ou de comportement d'évitement, qu'elles soient externes ou internes, face aux stimuli provenant de l'extérieur (Amina et Smail, 2022). De ce fait, la troisième composante (Réponse) qui constitue l'élément de réaction finale des consommateurs du cadre SOR est représentée par l'adoption des plateformes de Fintech dans notre cadre d'analyse. Les résultats de ce rapport devraient fournir des données pertinentes aux

professionnels en orientant la mise en place des stratégies destinées à optimiser l'adoption et l'acceptation des plateformes de technologies financières.

La figure 1-9 nous présente comment les consommateurs réagissent en fonction des trois phases énumérées.

Figure 1-9 : Modèle SOR de Mehabian et Russell (1974)



Source : Zghal et Aouinti, 2010

1.5.2 Le modèle TAM

Diverses disciplines se concentrent sur les problématiques cruciales d'acceptation et d'utilisation de technologies dans un environnement ou celle-ci est largement répandue et employée par une vaste partie de la population telles que les disciplines de la sociologie, de la psychologie et des systèmes d'information (Christine Dufour, 2022). Il existe par conséquent une multitude de perspectives pour examiner l'acceptation et l'utilisation des technologies :

- Selon la théorie de la diffusion des innovations qui cherche à expliquer comment une innovation technologique évolue de son état d'invention à une utilisation (ou non-utilisation) généralisée.
- Par le biais de méthodologies théoriques visant à déchiffrer la psychologie de l'acceptation par un utilisateur. Cette acceptation est vue dans ce cadre comme la conséquence d'un processus psychologique de l'utilisateur qui effectue des choix concernant une technologie.

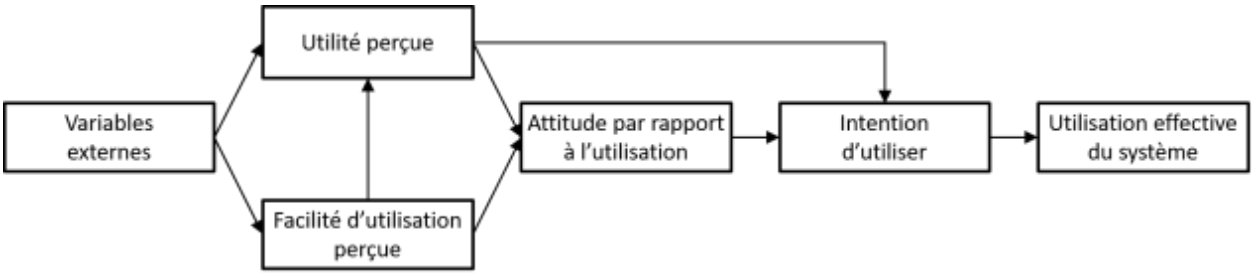
- Par l'intermédiaire des approches théoriques pour la conception des technologies « acceptables », démarches qui visent à influencer le développement des technologies avant leur déploiement.

Le modèle d'acceptation technologique, plus connu sous l'acronyme TAM (Technology Acceptance Model), développé en 1989 par Fred Davis, naît à partir de la Théorie de l'action raisonnée proposée par Fishbein et Ajzen en 1975 (Huu Binh, 2014). Ce modèle est considéré l'une des théories les plus influentes et populaires dans le domaine des recherches empiriques, car il a démontré sa capacité à prévoir l'intention comportementale et le comportement d'adoption des technologies au fil du temps (Kumar et Rani, 2024).

L'un des impacts fondamentaux de cette étude est l'élaboration de deux échelles de mesure validées empiriquement et méthodologiquement. Ces échelles pourront être utilisées pour l'évaluation, dans un contexte spécifique, de l'utilité perçue et de la facilité d'utilisation perçue d'une technologie. Il prend en compte la question des motivations qui poussent une personne à accepter ou refuser l'utilisation d'une technologie quelconque. Cette acceptation a permis d'identifier deux facteurs : **l'utilité perçue** et la **facilité d'utilisation** comme variables déterminantes sur l'**attitude** du consommateur envers l'adoption d'une technologie et par conséquent sur l'**intention** d'utiliser cette technologie (Huu Binh, 2014). L'utilité perçue correspond à la perception d'une personne quant à l'amélioration de sa performance au travail grâce à l'utilisation d'un système et la perception de la facilité d'utilisation correspond au degré où une personne considère que l'utilisation d'un système ne demanderait pas beaucoup d'efforts (Davis, 1993).

L'utilité perçue a servi à anticiper le comportement des usagers face au M-banking (Deb et Lomo-David, 2014). Selon Buabeng-Andoh (2018), l'utilité perçue joue un rôle crucial dans la prédiction des intentions de la clientèle. L'étude des intentions de comportement par Susilo et son équipe a révélé qu'une attitude se construit lorsqu'un individu fait face à un phénomène (Susilo *et al.*, 2019). Selon la littérature, l'utilité perçue exerce une influence notable sur l'attitude du consommateur (Liu et al., 2021).

Figure 1-10 : Modèle TAM de Davis et al., 1989



Source : SI &Management, 2023

1.5.3 Le modèle UTAUT

Malgré que le modèle TAM soit efficace pour prévoir des comportements d'adoption de technologies, il était indispensable pour les chercheurs d'élargir le modèle, car il présentait des explications comportementales restreintes (Kumar et Rani, 2024). Ainsi, les chercheurs ont incorporé le TAM dans la théorie UTAUT afin d'optimiser la précision du modèle de recherche.

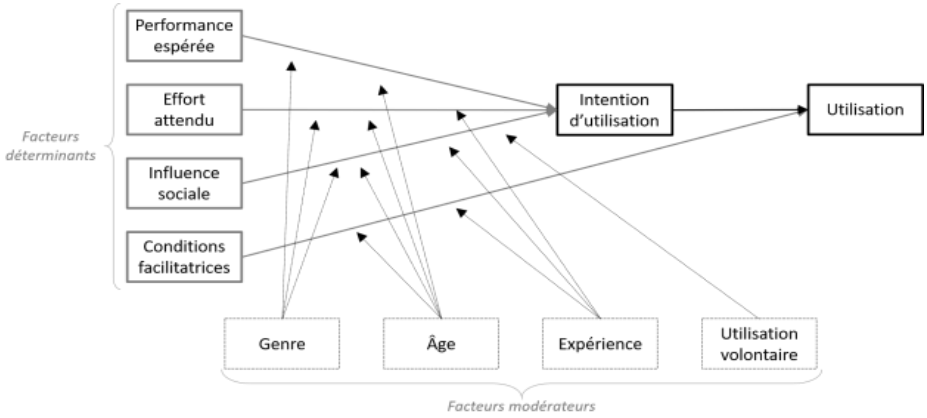
De nombreuses recherches ont été menées sur l'UTAUT et les conclusions actuelles s'accordent à dire que cet outil est fiable pour analyser les processus d'intégration et pour anticiper les comportements intentionnels (Blut et al., 2022). Les facteurs de ce modèle soulignent les liens entre la technologie, la cognition et les comportements sociaux.

La théorie Unifiée de l'Acceptation et de l'usage des technologies, proposée en 2003 par Venkatesh et al. est essentiellement établie à partir des 8 théories de l'acceptation des technologies déjà existantes dans le but d'unifier toutes ces théories et obtenir un modèle unique et compréhensif à savoir (Kouakou, 2017) :

- La théorie de l'action raisonnée (TAR) (Ajzen et Fishbein, 1975),
- Le modèle d'acceptation de la technologie (TAM) (Davis et al, 1989),
- La théorie du comportement planifiée (TCP) (Ajzen, 1991),
- La théorie du comportement interpersonnel (Triandis, 1980),
- Le modèle de l'utilisation du PC (MPCU) (Thompson et al, 1991),
- La théorie de la diffusion des innovations (DI) (Rogers, 1983),
- Le modèle de la motivation (Davis et al, 1992)
- Et la théorie cognitive sociale (TCS) (Bandura, 1989 ; Compeau et Higgins,1995).

Selon l'UTAUT, la réelle utilisation d'une technologie dépend de l'intention d'utilisation, qui est liée à des facteurs d'utilisation clés à savoir : la performance attendue, l'effort attendu, l'influence sociale et les conditions de facilitation (Venkatesh et al., 2003). De plus, ce modèle ajoute de nouvelles catégories de variables appelées modératrices, ce qui entraîne une variation de l'influence des variables déterminantes sur l'intention d'utilisation. Il y a plusieurs critères à prendre en compte : le genre, l'âge, l'expérience d'usage et la nature obligatoire ou volontaire (Kouakou, 2017). Toutefois, l'élément sur lequel nous allons poser une attention particulière est l'item attente de performance.

Figure 1-11: Schématisation des facteurs liés à l'acceptation et à l'utilisation des technologies du modèle UTAUT (Venkatesh et al.)



Source : Christine Dufour, 2022.

Le tableau ci-dessous permet de présenter l'étalonnage des notions visitées dans cette partie ainsi que les critères de sélection des plateformes des entreprises faisant partie de notre base d'études :

Tableau 1-1: Opérationnalisation des critères de sélection

Notions	Définition	Opérationnalisation avec les critères de sélection des plateformes

Loi encadrant la protection des données privées au Québec	Après évaluation des questions autour de la protection des données des utilisateurs, le gouvernement du Québec a adopté en 2021 la Loi 25, qui apporte des modifications significatives aux Lois sur la protection des renseignements personnels dans le secteur privé (CAI, 2024).	Les entreprises privées doivent : • Établir une liste des informations privées qu'elles détiennent. • Mise à jour de la politique de confidentialité et la rendre accessible et claire pour tous. • Implémentation des mesures visant à garantir la sécurité des données qu'elles possèdent.
Vulnérabilité des consommateurs en ligne	État dans lequel les consommateurs subissent un préjudice parce que leurs accès aux ressources et leur contrôle sont restreints de manière à inhiber considérablement leur capacité à fonctionner sur le marché. (Hill et Sharma, 2020)	• Vulnérabilité perçue et vulnérabilité réelle de Martin et al., (2017). • Vulnérabilité vécue et vulnérabilité observée de Hill and Sharma, (2020).
Marché de la Fintech	Utilisation des moyens technologiques pour développer, améliorer et offrir des services financiers. (Cachecho et Prom Tep, 2022)	• Le marché Fintech de l'Amérique du Nord représente le plus grand au monde. • 257 entreprises de Fintech évoluent au Québec dont 80% ont leur siège à Montréal. • Le Québec emploie 19.900 personnes au Canada et plus de 86.000 dans le monde.
Design responsable	• Conception inclusive et accessible des paramètres de sécurité • Conception centrée sur l'humain • Automatisation • Respect des normes éthiques	• Présence de bannières de sécurité • Type de consentement (éclairé, pas de consentement, consentement forcé) • Types de bannières de sécurité (validation ou refus des cookies avec

Design légal	Loi sur la protection des renseignements personnels dans le secteur privé, respect des règles entourant le consentement du consommateur en ligne à la collecte, la communication et à l'utilisation de ses renseignements personnels.	un clic, validation des cookies avec un clic et refus (paramétrage) avec au moins deux clics, obligation de validation des cookies)
Design éthique	Informer les utilisateurs en des termes clairs et simples sur le site internet de l'entreprise des actions prises et des conséquences qui en découlent en évitant toute manipulation frauduleuse pour obtenir un consentement éclairé vis-à-vis de la gestion des informations personnelles de l'utilisateur.	
Modèle S-O-R	Représente la combinaison des entrées ou Stimuli (S), des processus ou Organisme (O) et de la sortie ou Résultat (R) qui permet de démontrer l'impact des incitations environnementales sur l'état interne des personnes et leurs réactions cognitives.	• Conformité des plateformes • Influence normative • Adoption des plateformes de Fintech
Modèle TAM	Cadre conceptuel qui vise à expliquer comment les individus adoptent et utilisent les technologies.	• Conformité des plateformes • Influence normative • Adoption des plateformes de Fintech
Modèle UTAUT	Modèle intégrateur qui permet d'expliquer les variations dans le comportement d'acceptation et d'utilisation des technologies	• Conformité des plateformes • Influence normative • Adoption des plateformes de Fintech

Source : créé par l'auteur

CHAPITRE 2
CADRE CONCEPTUEL

Dans un environnement aux évolutions numériques fulgurant, la Loi 25 adoptée par le gouvernement québécois a représenté un changement significatif dans la règlementation entourant la gestion des données personnelles des utilisateurs, notamment dans le domaine de la Fintech, un secteur qui se démarque par l'utilisation de technologies novatrices pour offrir des services financiers à leur clientèle. L'objectif de cette Loi est de renforcer la préservation des informations privées tout en encourageant l'innovation technologique.

Tout au long du chapitre précédent, nous avons apporté un cadre théorique aux différents concepts sur lesquels repose notre recherche. Le présent chapitre a pour objectifs de présenter les hypothèses sur lesquelles nous avons établi notre étude ainsi que son cadre conceptuel.

2.1 Hypothèses de recherches définies

Les hypothèses de recherche sont des suppositions faites sur la base de données collectées durant des recherches empiriques et visant à mettre en liaison des variables. Cette section est divisée en quatre sous-sections dont trois sont une revue des variables présentées dans le chapitre précédent (connaissance de la Loi 25, vulnérabilité perçue et Design UX) et la quatrième section qui fait l'état des lieux de l'utilisation du cadre théorique Stimuli-Organisme-Réponse (SOR) pour étudier les différents concepts présentés.

2.1.1 Influence normative

- Connaissance de la Loi 25 et vulnérabilité des consommateurs.

Le sondage réalisé en 2022 par le Commissariat à la protection de la vie privée du Canada (CPVPV, 2023) a contribué à la présentation des enjeux en relation avec la protection de la vie privée des Canadiens, et ce par région. Les différents résultats présentés ont permis de déterminer dans quelle mesure la population québécoise connait et comprend ses droits en matière de protection de la vie privée et les enjeux de cette dernière par rapport aux populations des autres régions. Il en découle que :

- Sur les six Canadiens sur dix qui affirment suivre l'actualité sur les questions en rapport avec la protection des données, 57% de Québécois sont plus enclins à suivre d'assez près l'actualité sur la gestion de leurs données personnelles contre 68% de personnes vivant au Canada atlantique.
- Entre 2020 et 2022, la proportion de Canadiens qui se préoccupent de la protection de leur vie privée en ligne a gagné 6 pour cent quittant de 32% à 38% et le niveau de préoccupation est plus marqué au Québec. Nous avons un résultat de 43% de répondants québécois extrêmement préoccupés contre 29% de la Colombie-Britannique.
- Toutefois, sur 51% de canadiens qui estiment avoir une connaissance générale de leurs droits en matière de vie privée (13 points de moins qu'en 2020), le Québec est la région qui a le pourcentage est le plus élevé avec 61% de répondants contre 48% à l'Ontario, 53% dans les prairies et 39% en Colombie-Britannique

Par ailleurs, l'un des changements importants qu'apporte la Loi 25 est l'obligation pour les entreprises d'informer et publier les politiques de confidentialité mises en place sur leurs sites, informer et publier également les conditions d'utilisation de ces sites web afin que l'utilisateur donne un consentement éclairé et juste sur la gestion de ses données privées. Le gouvernement du Québec a jugé nécessaire que les consommateurs en ligne québécois prennent connaissance de leurs droits afin qu'ils aient plus confiance aux entreprises privées. Aux vues de ces informations, nous pouvons poser cette hypothèse :

H1 : Plus la connaissance de la Loi 25 est grande, plus faible est le sentiment de vulnérabilité des utilisateurs face à l'utilisation de leurs informations personnelles en ligne.

- Protection des données personnelles et vulnérabilité des consommateurs.

La garantie du respect de la sécurité et de la confidentialité des utilisateurs des services de technologies financières ainsi que la prise en considération de la sécurité de leurs données privées sont des éléments importants dans la perception du sentiment de vulnérabilité des consommateurs en ligne (Cachecho et Prom Tep, 2022). Les dispositions de la Loi 25 ont apporté des changements significatifs à la protection de la vie privée dans l'environnement numérique québécois. Les

nouveaux règlements renforcent notamment les pouvoirs de la Commission d'accès à l'information et les mesures de confidentialité et de transparence des ministères, des organismes publics québécois et des entreprises. Elles contribuent aussi à renforcer la responsabilité des organisations soumises à la Loi et à donner aux citoyens et aux citoyens du Québec un meilleur contrôle sur leurs informations personnelles (Commission accès à l'information, 2023). On peut donc dire que le gouvernement du Québec donne le pouvoir total au consommateur en ligne sur la gestion de ses données personnelles et met un point d'honneur sur la gestion en toute sécurité de ces données.

Par ailleurs, la vulnérabilité associée au risque d'accès aux données personnelles, celle qui fait l'objet de notre étude, est perçue comme étant : le simple accès aux données des clients par les entreprises en ligne revient au fait que ces entreprises détiennent des dossiers numériques sur leurs clients, ce qui leur permet de transférer ces données avec des tiers. Cette vulnérabilité résulte donc des craintes du consommateur quant aux risques qui adviennent de la publication des renseignements personnels ou de leur surveillance (Deslée, 2023). La Loi 25 a donc trouvé important que les consommateurs en ligne puissent savoir dans quels buts ils donnent l'autorisation à toute entreprise d'utiliser leurs données et comment ces données seront utilisées, durant quelle période afin de diminuer ce sentiment de vulnérabilité chez les utilisateurs.

Il est à noter que la majorité des répondants à une étude du gouvernement du Canada ont mentionné avoir confiance à la gestion de leurs données par le gouvernent, mais pas aux entreprises privées (Commissariat à la protection de la vie privée au Canada, mars 2023). Vu l'importance accordée par ce nouveau règlement sur la perception de la vulnérabilité et la prise en charge des risques liés à la vie privée, nous pouvons poser cette hypothèse :

H2 : L'adoption des mesures de protection des données a un effet positif sur la réduction du sentiment de vulnérabilité par les utilisateurs dans le secteur de la Fintech.

2.1.2 Les stimuli : les attributs

- Stimulus externe : le modèle de conception de la bannière de sécurité

Parmi les stimuli externes présentés par le cadre SOR de Mehrabian et Russel en 1974 figurent les caractéristiques du site internet (utilitaires et hédoniques), telles que les modèles de

conception des bannières de sécurité (Mollen et Wilson, 2010). La conception des bannières de sécurité est un élément crucial dans le milieu digital et peut servir à la fois de nudge ou de manipulation (Clara M., 2021). Des recherches effectuées indiquent que la façon dont les structures exposent les options de consentement sur leur plateforme en ligne peut affecter la perception de confiance, de contrôle et le sentiment de sécurité des utilisateurs (Utz et al., 2019). En utilisant cette variable comme stimulus externe, le modèle SOR confirme son aptitude à décrire les réactions émotionnelles et comportementales des consommateurs en ligne et par conséquent sa capacité à analyser le sentiment de vulnérabilité.

H3 : Le type de bannière de sécurité conçu par les entreprises dans le secteur de la Fintech a un effet positif sur la réduction du sentiment de vulnérabilité perçu par les utilisateurs.

- Transparence des entreprises de Fintech

Il n'est plus à débattre sur l'importance de la collecte et de l'utilisation des données clients comme moyen essentiel pour améliorer les résultats marketing d'une organisation, mais cette mesure ne doit pas passer par l'augmentation du niveau d'anxiété et de vulnérabilité des clients qui, pour se défendre, utilisent des stratagèmes à leur portée (Marcus & Davis, 2014). À travers des manipulations expérimentales effectuées auprès des clients de 15 entreprises, Martin et compagnie confirme les effets négatifs au sentiment de vulnérabilité sur les performances de l'entreprise (Martin et al., 2017).

L'étude de terrain réalisée auprès des consommateurs réels des entreprises de trois secteurs différents pour tester les pratiques de transparence et de contrôle à partir des politiques de confidentialité au moment de l'exécution de l'étude (en 2017) a révélé les résultats suivants sur les différents types de vulnérabilité (accès, violation, débordement et manifeste) (Martin et al., 2017).

Parmi les participants de l'étude 3, 10 % ont affirmé qu'ils auraient davantage tendance à fabriquer leurs informations personnelles, 23 % auraient une tendance plus prononcée à parler négativement et 22 % affirment qu'ils vont changer de fournisseur si une entreprise accède simplement à leurs données personnelles. Ces perceptions ont un impact négatif sur la performance sur l'ensemble du continuum. Selon un autre rapport effectué sur la vulnérabilité des clients créée

par 414 violations de la sécurité des données qui ont affecté 261 sociétés cotées en bourse par les mêmes auteurs, il est observé qu'une véritable violation des données diminue la valeur des actions de l'entreprise cible de −0,29 % et celle de son plus proche rival de −0,17 %.

Par ailleurs, le sondage obtenu par le commissariat à la protection de la vie privée des Canadiens démontre que 65% des Canadiens hésitent à communiquer leurs renseignements personnels dans divers scénarios (27% pour le Québec et 36% pour la Colombie-Britannique), 75% des répondants dont 58 % au Québec contre 46 % au Canada atlantique et 44 % en Ontario ont pris des mesures pour protéger leur vie privée en ligne (refuser de fournir les informations privées, ajuster les paramètres de sécurité, supprimer ou arrêter d'utiliser un compte, etc.).

Pour rappel, les points clés qu'apporte la Loi 25 sont la transparence totale dans la gestion des données des utilisateurs et leur consentement éclairé. Effectivement, cette Loi apporte de nouvelles obligations en termes de transparence des organisations dans la collecte et l'utilisation des données des utilisateurs. De ce fait, ces organisations doivent fournir, au moment de la collecte des renseignements personnels, des informations telles que : les objectifs de la collecte, les moyens, les droits d'accès des utilisateurs et de rectification, le droit des personnes concernées de retirer leur consentement, etc. (CAI, 2023). Néanmoins, une grande majorité des Canadiens se disent que les entreprises surveillent leurs activités en ligne ou sur les téléphones intelligents (34% des répondants québécois, 53% venant de l'Ontario, 50% de la Colombie-Britannique) et 87% des répondants à l'étude ont mentionné le fait d'être préoccupés par la façon dont les entreprises gèrent leurs données privées en ligne (CPVPC, 2020).

Les entreprises privées exerçant au Québec ont pour obligation d'établir des politiques et des pratiques encadrant la gouvernance des renseignements personnels et publier en détail ces politiques en termes simples et clairs sur le site web de leurs entreprises ou, si elles n'ont pas de site, par tout autre moyen approprié (CAI, 2023). Selon Deslée (2023), les chartes de confidentialité ne sont toujours pas suffisamment efficaces pour informer les consommateurs sur les différentes méthodes de collecte et d'utilisation des données personnelles. La lisibilité et la compréhension de ces politiques ne semblent pas avoir changé depuis près de vingt ans, alors que des travaux anticipés ont déjà montré l'existence de contraintes imposées au consommateur (Gauzente, 2003). Les limites énoncées dans les politiques de confidentialité témoignent d'un manque de clarté. Les

recherches menées par Portes et ses collègues en 2017 offrent une meilleure compréhension de la transparence, qui est conceptualisée à partir de trois aspects : la clarté (clarté, pertinence et accessibilité en temps réel des informations), l'objectivité (pour ne pas perturber la prise de décision) et l'ouverture (permettant la communication, la participation et la collaboration avec l'entreprise) (Portes et al., 2017).

De ce fait, la transparence dans l'utilisation des données est un élément pouvant avoir un impact sur la vulnérabilité des données et par conséquent sur l'adoption des paramètres de sécurité. Motivées par les arguments énumérés précédemment, nous pouvons formuler l'hypothèse suivante :

H4 : La transparence dans les modes de collecte et d'utilisation des données privées des entreprises de Fintech réduit favorablement le sentiment de la vulnérabilité des consommateurs.

- Utilité perçue et facilité d'utilisation perçue

La notion d'utilité perçue se rapporte à la manière dont les utilisateurs évaluent l'efficacité des services de paiement Fintech sur mobile et elle constitue un élément crucial qui a un impact direct sur les intentions comportementales des clients (Kumar et Rani, 2024). Dans le même ordre d'idées, Deb et Lomo-David (2014), ajoute que ce concept a été employé pour anticiper le comportement des utilisateurs en ce qui concerne les services bancaires en ligne. De plus, la littérature a démontré que l'utilité perçue influence considérablement l'attitude des consommateurs (Liu et al., 2021). Une recherche réalisée auprès de 174 participants a démontré que l'utilité aide à booster la productivité, à optimiser l'efficacité, à perfectionner les performances, etc. Ainsi, les sociétés de commerce mobilisées peuvent optimiser l'efficacité du système en améliorant la perception des clients (Susilo et al., 2019).

De ce fait, plus les mesures introduites par la Loi 25 au travers des paramètres de sécurité sont perçues utiles comme moyen d'amélioration de la protection des utilisateurs, plus la possibilité d'adoption des technologies financières est importante d'où l'hypothèse :

H5 : L'utilité perçue des paramètres de sécurité a un effet positif sur la réduction du sentiment de vulnérabilité sur les plateformes de technologies financières.

Les recherches effectuées par Singh et al. en 2020, Nguyen et al. en 2022 et Humida et al. en 2022 ont rapporté l'existence d'un lien substantiel entre l'utilité et l'intention comportementale et entre la facilité d'utilisation et l'intention comportementale (Kumar et Rani, 2024). La facilité d'utilisation peut être réalisée de plusieurs façons, allant d'une intégration sans heurts à une personnalisation à chaque phase. Ce qui importe est qu'en fin de compte, toutes ces démarches doivent avoir pour objectif de concevoir un produit final que les utilisateurs peuvent manier de façon indépendante, avec le moins d'interruptions et de supervision possible (Anthony S, 2024).

De plus, les participants à une étude réalisée par le Centre pour la Défense de l'Intérêt Public en 2017 dans le but d'examiner l'intérêt du consommateur canadien relativement aux paramètres de sécurité présents sur les différents sites web ont affirmé que les outils de protection sont difficiles à comprendre et à utiliser. Aussi, très peu de participants tentent de lire les politiques de confidentialité (tout comme les répondants au sondage réalisé par le CPVPC) et le volume d'utilisation des sites web et applications rend la gestion des paramètres de sécurité compliquée ce qui a un impact direct sur la perception du sentiment de vulnérabilité lors du parcours client (Lau, 2017). Il serait donc nécessaire que la conception des paramètres de sécurité telle promulguée par la Loi 25 soit facile d'utilisation pour tous les membres de la communauté québécoise.

En nous basant sur ces arguments, nous avons pu poser l'argument suivant :

H6 : Plus les paramètres de sécurité sont faciles d'utilisation, moins le consommateur en ligne se sent vulnérable sur les plateformes de technologies financières.

- Attente de performance

L'attente de performance se préoccupe du degré dans lequel un individu suppose que l'application d'un système lui permettra d'obtenir des avantages. Aussi, la littérature précise que dès l'instant où les utilisateurs possèdent une auto-efficacité élevée sur un sujet ou un domaine en particulier, leur performance est supérieure à leur attente (Kumar et Rani, 2024). Il est ajouté que, plus une personne est persuadée de la performance d'un produit, plus forte sera son intention d'utiliser ce produit.

Dans le domaine des technologies financières, l'attente de performance se manifeste par la certitude que l'usage des plateformes numériques, en particulier celles qui respectent les

règlementations telles que la Loi 25, offre une meilleure protection des données privées, une plus grande transparence ou une amélioration de l'efficacité transactionnelle. Lorsque les utilisateurs constatent que ces plateformes satisfont leurs exigences en termes de sécurité, de protection de la vie privée ou de contrôle de leurs informations, leur volonté d'adopter ces plateformes est renforcée.

Dans le cadre de notre recherche, nous opérationnalisons l'attente de performance à travers la variable efficacité perçue de la Loi 25 : les utilisateurs déterminent si cette Loi, qui renforce les exigences de consentement, de transparence et de paramétrage, a un apport significatif sur la réduction du sentiment de vulnérabilité en ligne.

C'est pourquoi l'hypothèse suivante a été formulée :

H7 : Plus l'utilisateur est convaincu de la performance des bannières de sécurité, plus faible sera son sentiment de vulnérabilité.

2.1.3 De l'organisme à la réponse

Afin d'identifier les éléments qui influencent l'adoption des technologies et mesurer le sentiment de vulnérabilité des consommateurs en ligne dans un contexte post Loi 25, nous avons décidé de prendre en compte les aspects essentiels tels que la perception d'utilité et la facilité d'utilisation à travers la théorie TAM ; les attentes en termes de performance et les conditions facilitantes grâce à la théorie UTAUT et le modèle S-O-R nous permettront de couvrir les réactions émotionnelles et comportementales aux stimuli liés à la protection des données. Ces modèles sont fréquemment utilisés dans la recherche en marketing pour expliquer les conséquences de l'environnement des sites web sur les réactions des utilisateurs (Lemoine, 2012), car elles se ressemblent sur la manière dont les individus perçoivent des déterminants basés sur la technologie ainsi que sur des facteurs contextuels plus larges (Kumar et Rani, 2024).

Aussi, réduire la vulnérabilité des consommateurs sur les plateformes ou sites web a pour objectif de redonner à ces utilisateurs une maîtrise du contrôle de leurs données sur le web, ce qui pourrait contribuer à l'adoption des mesures de protection des informations. Puis que ce modèle préconise l'existence d'un lien entre le sentiment de sécurité perçu (organisme) et l'adoption des plateformes de Fintech (réponse), l'hypothèse suivante a été établie :

H8 : Le sentiment de vulnérabilité perçue par les consommateurs en ligne au Québec a un effet sur l'adoption des Fintechs conformes à la Loi 25.

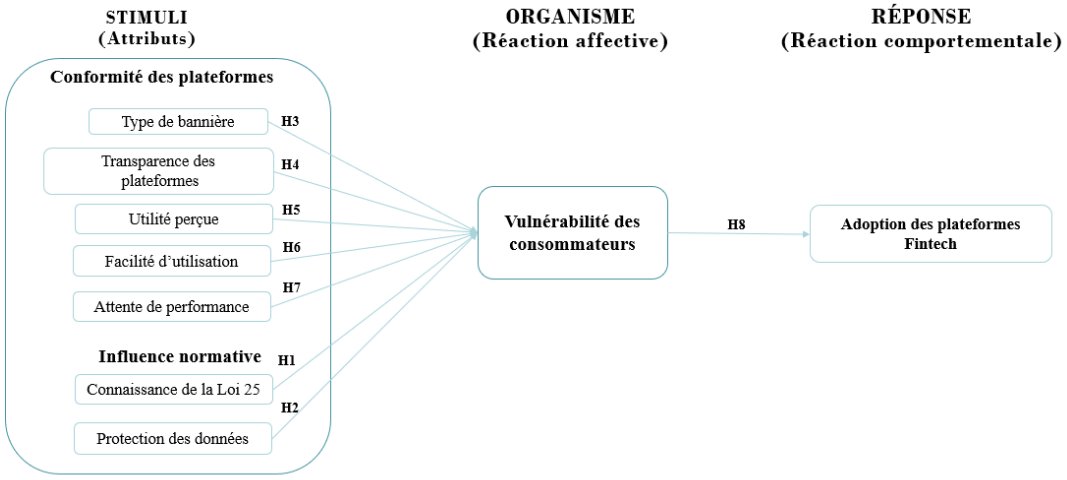
À partir de l'analyse des différents modèles précédemment présentés, cet article inclut donc le concept de SOR qui s'ajoute à la recherche sur les intentions comportementales des clients lorsqu'ils adoptent les Fintechs. Dans notre cadre de recherche, ce modèle sert de modèle pour démontrer les liaisons des facteurs **design des paramètres de sécurité, connaissance de la Loi 25, utilité perçue, facilité d'utilisation perçue** et **risque perçu** comme principaux stimuli sur les **attitudes** et les **intentions comportementales** (organisme) des utilisateurs face à l'adoption des bannières de sécurité proposées par les plateformes dans le secteur de la Fintech.

Même si le modèle suggéré met l'accent particulièrement sur l'impact du type de bannière sur le sentiment de vulnérabilité perçu, il est important de noter que cette variable manipulée a la possibilité d'affecter d'autres éléments du modèle comme la perception de la transparence des plateformes ou encore l'adoption des mesures de protection des données. Ces potentielles corrélations ne sont pas examinées dans notre étude mais elles représetent des prolongations théoriques significatives.

2.2 Opérationnalisation de notre cadre d'étude

Notre cadre conceptuel a pour objectif de présenter les liens entre l'adoption des plateformes et sites web Fintech depuis la mise en place des règlements apportés par la Loi 25 et la perception de vulnérabilité des consommateurs québécois dans le domaine de la Fintech québécoise. Pour comprendre les dynamiques d'acceptation des technologies financières et les effets de cette adoption sur le sentiment de sécurité ou de vulnérabilité des consommateurs, nous utilisons trois modèles théoriques fondamentaux : TAM (Technology Acceptance Model) à travers la facilité d'utilisation et l'utilité perçue des bannières de sécurité, UTAUT (Unified Theory of Acceptance and Use of Technology) à travers l'attente de performance des paramètres de sécurité et enfin le modèle S-O-R (Stimulus-Organism-Response).

Figure 2-1: Cadre conceptuel



Source : créer par l'auteur.

CHAPITRE 3
MÉTHODOLOGIE

La méthodologie est un élément crucial de toute recherche, car elle détermine les méthodes et les ressources employées pour traiter les interrogations de recherche et atteindre les buts établis. Notre recherche s'appuie sur un design expérimental *between subject* à six conditions et un éventail de modèles de conception de bannières de protection de données utilisés dans le secteur de la technologie financière au Québec.

3.1 Design de recherche

Dans les analyses réalisées précédemment, il est établi que la vulnérabilité des consommateurs dépend de leurs propres perceptions (Baker et al. 2005 ; Hill et Sharma, 2020). L'objectif de notre étude étant d'approfondir des connaissances sur un thème en identifiant, sur la base des suppositions de recherche, le lien entre les facteurs causals et le résultat anticipé comme le préconise Malhotra (Malhotra, 2011), nous utilisons le design de recherche de type causal parmi les différents types de design de recherche présentés par la littérature (exploratoire, descriptif et causal. La méthode utilisée est par conséquent l'expérimentation.

Notre étude mesure d'une part l'impact du numérique et de la politique à travers l'application de la Loi 25 sur la vie des utilisateurs. Ayant un intérêt public allant au-delà d'un site web ou d'une plateforme, notre recherche n'est pas juste à caractère marketing. Nous nous intéressons à l'apport de la Loi 25 sur la vulnérabilité des consommateurs et sur les mesures de protection des données appliquées par les entreprises de finances technologiques sur leurs plateformes. Plus précisément, elle examine la pertinence de réalisation des différents modèles de conception des bannières de sécurité présentes sur les sites web des entreprises évoluant au Québec de façon générale, et des Fintechs en particulier et le comportement d'adoption de ces dernières. Pour ce faire, après avoir établi un aperçu des différents spécimens des paramètres de sécurités auxquels les entreprises ont recours, nous avons créé 6 bannières de sécurité fictives pour une entreprise X dont le nom est Atlas.

La présente recherche a été menée en suivant un plan expérimental unifactoriel complètement aléatoire à 6 conditions (6*1). Les six conditions sont liées aux six bannières de sécurité créées, une condition représentant un groupe d'études. En recherche expérimentale, deux modèles de manipulation de variables sont couramment utilisés. Le design between-subjects dans lequel chaque participant ou groupe de participants est soumis à une condition unique contrairement au design within-subject où chaque condition implique la participation de tous les participants (Malhotra, 2011). Notre cas d'études utilise le modèle *between-subjects*, ce qui signifie que chaque bannière de sécurité fictive créée représente une équipe distincte les unes des autres. Ainsi, nous nous sommes servis du Rapport Fintech Québec 2023 et du Rapport Fintech Québec Semestriel 2024 pour faire un recensement des paramètres de sécurité auxquels ont recours les entreprises de technologies financières. Cette action a permis de faciliter la détection de diverses mesures de protection des données des utilisateurs et de produire des modèles de conception représentatifs du marché.

Comme indiqué dans les travaux littéraires, les conceptions des paramètres de protection des données personnelles par les entreprises évoluant au Québec doivent répondre aux exigences légale, éthique et responsable. Comme le recommande la Loi 25, les bannières de sécurité doivent présenter de manière détaillée les politiques et pratiques encadrant la gouvernance des informations personnelles des utilisateurs, réaliser une évaluation des facteurs relatifs à la vie privée et détruire les renseignements personnels lorsque la finalité de leur collecte est atteinte (Commission accès à l'information du Québec, 2023). Pour ce qui est du volet éthique, il met en lumière l'aspect du consentement éclairé prôné par la Loi 25. Il est demandé aux designers UX de concevoir des interfaces claires, sincères et respectueuses des utilisateurs. Il est primordial d'éclairer les usagers sur les décisions qu'ils prennent et des répercussions qui en résultent, d'encourager une perspective éthique de l'expérience client qui souligne les besoins et la confiance des usagers, tout en prévenant toute fraude. Par cette obligation, on considère que le consentement de l'utilisateur est éclairé lorsque l'entreprise lui fournit, dans un langage clair, tous les renseignements nécessaires avant son approbation sur l'utilisation de ses données. Le volet responsable des modèles de conception des bannières apporte une approche de réduction de l'empreinte économique, sociale et environnementale du numérique. Il est recommandé aux designers UX d'intégrer une conception inclusive et accessible des paramètres de sécurité et une conception centrée sur l'humain. Ceci nécessite l'élaboration d'interfaces pour tous, simples et claires et indépendamment de leurs

aptitudes, incluant une conception adaptée aux handicaps et aux contraintes physiques, mentales et financières. Par ailleurs, l'interface doit, dès sa page d'accueil, présenter les paramètres avec toutes les informations essentielles à une prise de décision claire et consentie du consommateur.

Après la collecte des modèles de bannières de sécurité utilisés par les concepteurs UX au Québec, nous avons réalisé ces six bannières qui représentent chacune un groupe d'études afin de mesurer les réactions face à la bannière présentée. Pour ce faire, nous avons les bannières ci-dessous qui représentent chaque type de bannière : la bannière tout accepter, la bannière accepter avec politique de confidentialité, la bannière accepter les cookies essentiels, la bannière sans paramètre de confidentialité, la bannière accepter ou paramétrer et la bannière consentement libre.

Figure 3-1: Bannière tout accepter

Figure 3-2: Bannière accepter avec politique de confidentialité

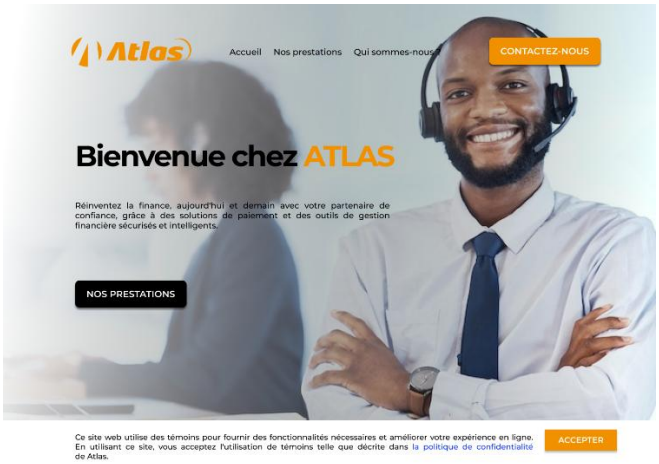


Figure 3-3: Bannière accepter les cookies essentiels

Figure 3-4 : Bannière sans paramètre de confidentialité

Figure 3-5: Bannière accepter ou paramétrer

Figure 3-6: Bannière consentement libre

3.2 Sélection des bannières de sécurité

Notre collecte de données est effectuée en deux phases. La première phase consiste à réaliser des captures d'écran des pages d'accueil des sites web des entreprises de Fintech québécoises en ligne versus les captures d'écran des pages d'accueil des autres secteurs d'activité afin de présenter ce qui est fait en termes de respect des mesures de protection des données. Cette phase s'est tenue d'avril à septembre 2024 dans le but de recueillir les données actualisées du rapport Fintech Québec semestriel 2024. Il convient de noter que cette période de collecte des données précède l'application intégrale de la troisième phase obligatoire de la Loi 25 qui exige, depuis septembre 2024, des critères plus stricts concernant le consentement explicite et la transparence liée à l'utilisation des données privées des utilisateurs. Ainsi, il faut traduire certains procédés observés durant cette étape, tels que l'absence de bannières de sécurité sur des plateformes Fintech, conformément au cadre règlementaire qui était en transition.

Par la suite, un questionnaire est réalisé en ligne avec la plateforme Qualtrics qui permet de regrouper les différentes expérimentations en un sondage et de configurer ce dernier de telle sorte que les différentes bannières sont présentées automatiquement et une fois qu'un stimulus à une bannière a atteint le quota requis de répondants (50), celui-ci n'est plus présenté. Cette étape s'est tenue de novembre 2024 à février 2025.

Les résultats présentés dans ce rapport d'étude sont établis sur la base de 264 captures d'écran des plateformes d'entreprises évoluant au Québec aussi bien dans le secteur de la Fintech québécoise (130 captures) que dans les autres secteurs (134 captures) que ces soit épicerie, automobile, cosmétique, cabinets de conseil, ameublement, etc., afin de discerner ce qui est conçu

comme paramètres de sécurité par nos entreprises et jusqu'à quel point ces paramètres respectent l'utilisateur sur les volets légal, responsable et éthique.

Il est important de rappeler que lors de ces captures d'écran, une catégorie de bannières de sécurité a été formée, la catégorie '' sans bannière de sécurité'' car comprend des entreprises n'offrant aucun paramètre ou procédé explicite d'accord concernant l'utilisation des données personnelles. Cette classification représente des pratiques constatées avant l'application intégrale de la Loi 25. Actuellement, ces actions enfreignent les obligations juridiques prévues par cette loi, ce qui donne à ce groupe une dimension analytique spécifique, surtout pour mettre en évidence les différences entre les pratiques antérieures et les normes règlementaires actuelles.

3.2.1 Caractéristiques de notre échantillon

- Critères de sélection des plateformes

Les deux critères primordiaux de notre échantillon sont : être une entreprise qui évolue au Québec et avoir un site internet qui représente le volet numérique de vos différentes activités.

Après cette 1re étape, nous avons navigué sur le net afin d'obtenir le maximum d'informations sur les différents types de bannières de sécurité effectués dans le domaine de la Fintech versus les autres domaines afin de pouvoir ressortir un aperçu des meilleures pratiques.

Un total de 134 captures d'écran de bannières de sécurité a été pris pour représenter notre banque d'informations des entreprises de cosmétiques (L'Oréal), d'ameublement (Meubles Foliot, Leon's, tec.), d'épiceries (Metro, IGA, Super C, Provigo, Costco, etc.), automobiles (Volvo, Ford, Hyundai, GMC, etc.), magasinage (JD, Patagonia, Jean bleu, the North Face, HM, La baie d'Hudson, etc.), restaurant (Piazetta, Toi et Moi Café), Enseignement (Université de Montréal, Université de Sherbrooke, etc.), entreprise de services et de conseil (REMAX, PWC, Tourisme Monstréal, etc.).

Notre base de données des entreprises de Fintech est établie à partir du rapport semestriel Fintech Québec 2024 publié en juin 2024 qui résume les activités du marché de la Fintech au Québec de janvier à juin 2024, car le critère Fintech basé au Québec est essentiel aux fins de notre étude. Sur les 257 Fintechs basées au Québec, notre échantillon d'étude est de 130 entreprises qui

évoluent dans ce secteur. Pour les entreprises de Fintech, nous avons tenu à avoir un ensemble représentatif du marché de toutes les industries de la Fintech du Québec, raison pour laquelle nous avons établi une sélection selon chaque secteur d'activité à savoir :

- Tech financière (18) parmi lesquels : CGI, SESAMI, H3M.IO, , Alpha CCO, Datalog, Exagens, F8TH, Secureworks, Streamscan
- Gestion de patrimoine et d'actifs (17) parmi lesquels : CROESUS, Evovest, Fimlogik, Terry, AltQArtiffex
- IA et données (28) parmi lesquels : Winston AI, Pulse AI, Quantolio, Berkindale
- Chaine de blocs (16) parmi lesquels : Covalent, Nebula AI, Octav, Zapper, Lottus, Zapper, Covalent, Streaming Fast
- Marché des capitaux (7) parmi lesquels : Scanz, Haywood, Horizon, Tsimagine, Swingtrackr
- Banque alternative ou Néo banque (3) : Pleo, Lodavo, Ezo
- Financement participatif (7) : Zeffy, Makeachamp, Equitalle
- Crypto et système financier décentralisé (12) parmi lesquels : Bitfarms, coinmiles, Dello, InstaCoin, Knox, Shakepay, Yap.cx, Bylls, BullBitcoin
- ESG (8) parmi lesquels : IMPAK, Novisto, Sibli, Cloudsibyl.
- Assurtech (21) parmi lesquels : Equisoft, Insurity, Emma, Sinistar, Dialogue, Flight Claim, Major, Zinnia, Inscore
- Tech prêts (29) parmi lesquels : Brain finance, Aim Finance, Alterfina, CreditBook, Iceberg Finance, Nesto, FIG, Flovver, Landjourney, Pads, PayRelax
- Tech de paiement (46) parmi lesquels : Lightspeed Montreal, Mobilus, Cashflow, Digitech Payments, Nethris, Proximis, Trolley, Di Allo, Mobi724, T365, MDF Commerce, Tenant Pay.
- GFM (11) : LIVSTA, CODE F, Wealthica
- Technologie immobilière (12) parmi lesquels : Livya, Billdr, Bloc.solutions, Eversa, Local Logic.
- Gestion d'entreprise (10) parmi lesquels : Acquisio, Cubeler, Tenet, Big Bang.
- Comptabilité et gestion (12) parmi lesquels : Kiwili, Stamped, App8.

- Corpus des entreprises retenues

➢ Types de paramètres de sécurité

Avant de présenter les différents paramètres de sécurité qui feront l'objet de notre analyse, il est important de rappeler que l'un des objectifs de cette étude est de promouvoir le respect des volets légal, responsable et éthique des différents paramètres de sécurité en général par les concepteurs UX. Vu l'impact du type de bannière sur le consentement de l'utilisateur, il est nécessaire d'établir une comparaison des différents modèles utilisés par les entreprises de secteurs divers, mais plus précisément celles exerçant dans le domaine de la Fintech.

L'analyse des différentes bannières de sécurité conçues par les entreprises de notre étude nous a permis de dégager cinq principaux types de paramètres de sécurité à savoir :

- **La bannière de sécurité de type consentement à choix unique** <<tout accepter >> : Ce type de bannière présente généralement un texte assez bref de ce qui sera fait avec les cookies et n'offre qu'une seule option à l'utilisateur qui est d'accepter (ou autoriser) que ses données soient utilisées par l'entreprise. On peut dire que le consentement de l'utilisateur est forcé dans ce genre de situation. Exemple :

Figure 3-7: Exemple de bannières de type choix unique << accepter >>

Source : site de l'entreprise H3M.IO

- **La bannière de sécurité de type consentement unique << Accepter >> avec possibilité de consultation de la politique de confidentialité** : tout comme la bannière précédente, celle-ci a un message bref pour dire ce qui est fait des témoins

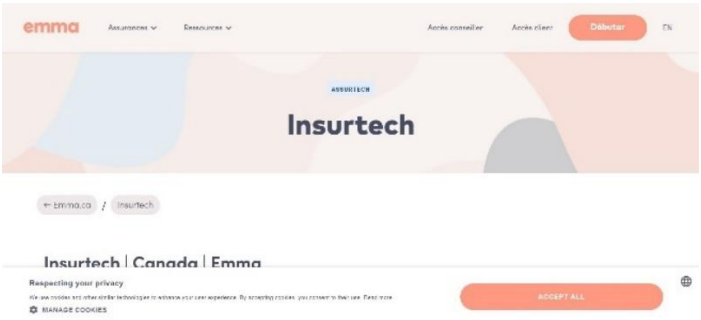
et oblige le consentement de l'utilisateur, mais en plus elle donne la possibilité aux utilisateurs de lire la politique de confidentialité définie sur 3 à 4 pages en cliquant sur le lien. Exemple :

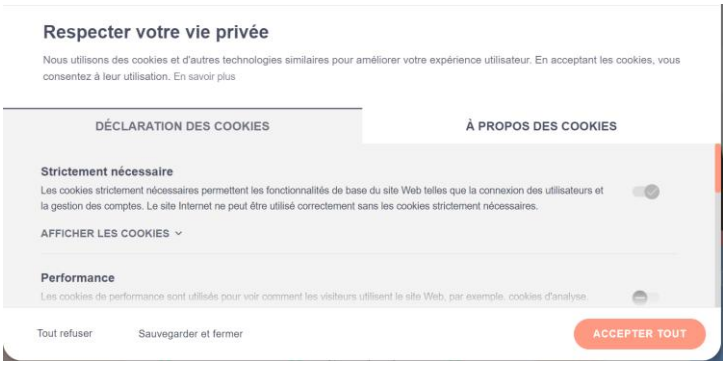
Figure 3-8: La bannière de sécurité de type consentement unique << accepter >> avec politique de confidentialité.

Source : site de l'entreprise BRAINFINANCE

- **La bannière de sécurité de type <<autoriser les cookies ou configurer >>** : la particularité de ce type de paramètre de sécurité est qu'il donne le choix à l'utilisateur de valider le type de cookies qu'il permet à l'entreprise d'utiliser pour améliorer l'expérience client. Il est important de noter que, malgré que l'utilisateur a le choix de sélectionner sur des cookies après plus d'un clic, les cookies dits nécessaires ou essentiels sont automatiquement validés durant la conception de ces paramètres. Exemple :

Figure 3 - 1 : bannières de sécurité de type configurer : <<autoriser les cookies ou configurer >>

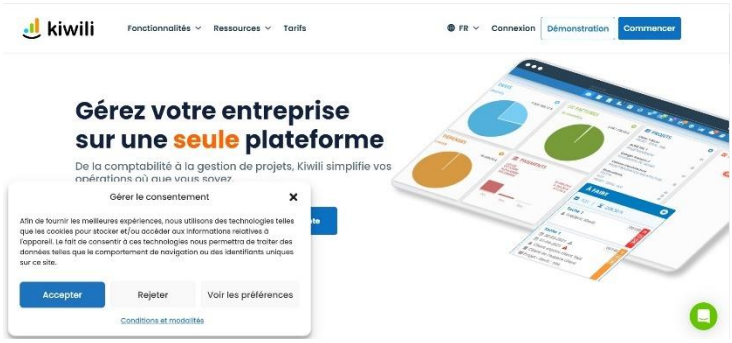




Source : site de l'entreprise EMMA

- **La bannière de sécurité de type consentement libre : <<autoriser, rejeter ou configurer les cookies >>** : Ce type de paramètre permet à l'utilisateur de gérer son consentement dès la présentation des paramètres de sécurité sans avoir à cliquer sur un lien de direction. En effet, l'utilisateur a le choix de refuser que toutes sortes de cookies soient stockés sur son appareil durant sa navigation sur le site, d'accepter tous les cookies ou encore d'émettre des préférences. Le consentement de l'utilisateur dans ce cas n'est pas forcé. Exemple :

Figure 3-9: La bannière de sécurité consentement libre : <<autoriser, rejeter ou configurer les cookies >>

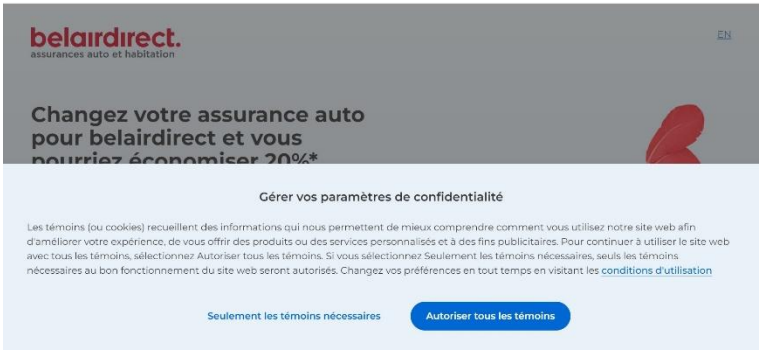


Source : site de l'entreprise KIWILI

- **La bannière de sécurité de type cookies essentiels : <<autoriser tous les cookies ou autoriser les cookies essentiels >>** : La seule différence qu'apporte ce modèle de

paramètres est que l'utilisateur a la possibilité de ne choisir que les cookies essentiels au fonctionnement du site web.

Figure 3-10: Bannière de sécurité de type cookies essentiels : <<autoriser tous les cookies ou autoriser les cookies essentiels >>



Source : site de l'entreprise BELAIRDIRECT

Il est à noter que ce ne sont pas toutes les entreprises qui ont conçu des bannières de sécurité, donc un sixième groupe appartient à ces entreprises qui jugent que ce n'est pas nécessaire de permettre aux utilisateurs d'établir ou pas des directives concernant l'utilisation de leurs données personnelles par les entreprises. Le sixième groupe est nommé : sans bannière de sécurité.

3.3 Sélection des participants

Le processus d'échantillonnage en design causal relève d'un certain nombre d'étapes parmi lesquelles déterminer des relations de cause à effet et optimiser les variables (Malhotra, 2010). Des deux méthodes d'enquêtes qu'offre ce design entre le test de marché et l'expérimentation (Malhotra, 2010), nous utilisons la méthode expérimentale.

L'élaboration de notre échantillon a commencé par l'identification de la population à analyser. Cette étude vise de ce fait les individus âgés de 18 ans et plus vivant au Québec qui utilisent les appareils intelligents au moment de l'étude. Aussi, ils doivent utiliser un des services de technologies financières (paiements en ligne, cryptomonnaie, gestion des finances personnelles, services bancaires en ligne, etc.).

La méthode non probabiliste boule de neige, technique la plus répandue pour les sondages en ligne, a été choisie dans notre cadre d'étude. Les répondants sont recrutés parmi les réseaux de connaissances de la chercheuse. Cette méthode implique une élaboration graduelle de l'échantillon en se basant sur les références recueillies des premiers participants (Malhotra, 2011). Le questionnaire est diffusé sur les pages WhatsApp, Facebook, LinkedIn de la chercheuse et par la suite, les contacts initiaux vont partager les différents sondages sur leur page par la suite.

La taille de notre échantillon est de 300 répondants repartie entre les six groupes, pour un minimum de 50 individus par groupe. Il est essentiel de préciser qu'un répondant a le choix de participer à une expérimentation ou de refuser de prendre part à cette recherche. La récompense est un tirage de deux cartes cadeaux Winners d'une valeur de 50$ chacune.

3.4 Questionnaire

L'outil de mesure recommandé par Malhotra (2010) selon notre design causal est un questionnaire. Ainsi, nous avons pu avoir une approche quantitative du phénomène grâce aux données collectées, qui ont par la suite été pondérées pour généraliser plus facilement nos résultats (Malhotra, 2010). Cet auteur a également défini le questionnaire comme étant une série de questions formalisées destinées à obtenir des informations sur un sujet auprès des répondants à une étude (Malhotra, 2011). Pour mesurer la vulnérabilité perçue par les consommateurs québécois durant leurs parcours en ligne, nous nous sommes basés sur des échelles de mesure et items qui existent dans la littérature à travers les travaux de Ho *et al.*, 2023, Gordon Bruner (1954), Hill et Sharma, 2020, Fred Davis 1989, 2020, Martin et al, 2017, Venkatesh et al., 2003 et bien d'autres. Les types de questions mis en avant dans ce questionnaire sont les questions à choix multiples et les questions à échelle et dans le but de standardiser les questions à échelle, les variables ont été évaluées à l'aide d'une échelle de Likert à 7 points, allant de 1 (pas du tout d'accord) à 7 (totalement en accord). Nous utilisons des questions de l'échelle de mesure de Likert pour mesurer nos différents concepts clés et établir le degré d'accord de nos répondants (Sarsted et Mooi, 2019).

D'Astous (2019) préconise, avant la collecte de données, de réaliser la soumission du questionnaire révisé à quelques personnes de la cible. Dans un premier ordre, nous avons effectué six questionnaires à partir de l'outil de sondage Google Forms portant chacun sur chaque type de

bannière de sécurité à étudier. Mais par la suite et considérant l'amélioration des outils de sondage, l'utilisation du logiciel Qualtrics nous a été recommandée. Ce dernier nous a permis de regrouper les six différents questionnaires en un seul sondage d'enquête tout en configurant de tel en sorte que les différentes bannières soient présentées automatiquement et une fois qu'un stimulus à une bannière a atteint le quota requis de répondants (50), celui-ci n'est plus présenté. Le Québec étant une province dont la langue officielle est le français, le sondage est établi en langue française.

Notre formulaire d'enquête commence par une page introductive qui englobe les sections suivantes : l'identification de l'étudiant responsable de la recherche, le but général, les procédures pour les participants, les avantages et les risques, l'anonymat et la confidentialité, la participation volontaire, la compensation financière, les droits des répondants, les remerciements puis les signatures de l'étudiant et de la direction responsable du projet (Annexe A). Le consentement du répondant étant primordial avant toute étude, une page de consentement suit la page d'identification où les répondants ont le droit de cliquer sur « j'accepte» ou « je refuse» à la déclaration suivante: «J'accepte volontairement de participer à cette étude. Je peux me retirer en tout temps sans préjudice d'aucune sorte.». Si l'option refusée était choisie, le questionnaire ne sera pas considéré pour comme valable pour notre examen.

Par la suite, le sondage comprend des questions filtres qui permettent de recruter des individus qui répondent essentiellement à notre population d'études. Il s'agit des questions : « Quel âge avez-vous? », «Résidez-vous dans la province du Québec? » « À quelle fréquence utilisez-vous les appareils connectés par jour », « À quelle fréquence utilisez-vous les services bancaires par semaine (paiements en ligne, prêts numériques, gestion financière via applications, cryptomonnaie, assurance, etc.)? ». Les réponses éliminatoires sont respectivement : « moins de 18 ans et plus de 65 ans », « Non », « Je n'utilise pas d'appareils connectés » et « Je n'utilise pas de services Fintech ».

Ensuite s'en vient la partie la plus cruciale de l'enquête à savoir la mise en situation projective de la bannière fictive présentée. Cette partie analyse particulièrement le comportement des utilisateurs face à la bannière de sécurité, l'utilité, la facilité d'utilisation des bannières de sécurité ainsi que le consentement et les perceptions psychologiques à l'utilisation des autres. S'en suivent les questions relatives à la connaissance de la Loi 25, à l'analyse de la perception de la vulnérabilité

des utilisateurs face aux services Fintech, et enfin des questions relatives à l'analyse des variables individuelles affectant la vulnérabilité des consommateurs.

Le questionnaire se concluait par des interrogations concernant des informations sociodémographiques comme le genre et le statut professionnel. Finalement, une dernière interrogation était formulée afin de solliciter l'inscription d'une adresse courriel permettant de communiquer avec le répondant s'il recevait la carte cadeau. Il était possible pour les participants d'y répondre ou non, sans que cela ait un impact sur leurs réponses au questionnaire.

3.5 Échelles de mesure utlisées

Pour évaluer de façon précise les différentes variables de cette recherche, nous avons choisi des échelles de mesure qui ont été validées dans la littérature. Ces échelles sont majoritairement issues d'études précédentes dans les domaines de psychologie sociale, du comportement des consommateurs et de l'adoption des technologies. Elles ont été minutieusement sélectionnées pour leur validité conceptuelle, leur fiabilité statistique et leur adéquation avec notre contexte de recherche.

Les échelles de mesure présentées dans le tableau 3-1 sont les versions originales rédigées en anglais. Dans le cadre de cette étude, elles ont été traduites par la suite en français par le biais d'une démarche de traduction inverse (back-traduction) visant à garantir une équivalence conceptuelle et sémantique entre les éléments originaux et leur déclinaison française. Cet ajustement linguistique a permis d'assurer une meilleure compréhension des termes par les participants tout en préservant l'intégrité des échelles originales.

Tableau 3-1: Échelles originales au questionnaire

Variables	Types d'échelles	Item (Version originale)	Source
Attitude to the Ad (General)	Intervalle - Likert	1. I paid close attention to the ad. 2. I fully concentrated upon the ad. 3. I was deeply engrossed in the ad.	Kim and Lakshmanan (2015)

Attitude toward the Ad (Meaningfulness)	Intervalle - Likert	1. The ad was meaningful to me. 2. The ad was appropriate for me. 3. The ad was useful to me 4. The ad was valuable to me.	Lehnert, Till, and Ospina (2014)
Attitude toward the Ad (Vividness)	Intervalle - likert	1. not specific / specific 2. not concrete / concrete 3. not detailed / detailed	Kim and Lakshmanan (2015)
Argument strength	Intervalle - Likert	1. not very persuasive / Very persuasive 2. not at all informative / very informative 3. Made me think of _____ in the exact same way / Made me think of _____ in a completely different way.	Yeh and Jewell (2015)
Reactance (intrusiveness)	Intervalle - Likert	1. The _____ is disturbing. 2. The _____ is interfering. 3. The _____ is intrusive. 4. The _____ is forced upon me. 5. The _____ is unwelcomed. 6. I want to resist the _____. 7. I want to dismiss the content of this _____.	Bleier and Eisenbeiss (2015).

Affective response to the ad (Vulnerability)	Intervalle - Likert	1. Exposed 2. Unprotected 3. Susceptible 4. Unsafe 5. Vulnerable	Aguirre et al. (2015)
Privacy of Response	Intervalle - Likert	1. It is my impression that my responses will be shared with everyone else here today. (r) 2. It is my understanding that my responses will be made public. (r) 3. It is my impression that my responses will be kept anonymous and confidential.	Green and Peloza (2014).

Source : Bruner, G.C (2017). Marketing Scales Handbook.

Les outils de mesure employés dans cette recherche sont cohérents avec les variables identifiées dans le cadre conceptuel. Chaque variable est évaluée en utilisant des échelles dérivées de la littérature, ajustées et traduites pour le contexte québécois.

Afin de s'assurer de la transparence méthodologique ainsi que d'une concordance entre les divers modèles conceptuels et les outils de mesure, le tableau ci-dessous illustre la relation entre les variables employées dans ce projet de recherche et les échelles déployées pour leur mesure. Cette explication a pour but de clarifier le rapport entre chaque variable théorique et les questions présentes dans notre questionnaire, ce qui facilitera l'analyse des résultats.

Tableau 3-2: Correspondance entre les variables du modèle et les échelles

Variables du cadre conceptuel	**Échelles adaptées**	**Échelles originales (Source)**	**Auteurs**	**Type d'échelles**
Connaissance de la Loi 25	Taux d'information, Familiarité avec la Loi 25	Échelle élaborée pour notre étude	Moi-même	Intervalle - Likert
Protection des données (Consentement)	Perception du contrôle, consentement éclairé	Reactance (intrusiveness)	Bleier and Eisenbeiss (2015).	Intervalle - Likert
Transparence des plateformes	Clarté, Pertinence, Transparence perçue	Attitude to the Ad vividness, Argument strength	Yeh and Jewell (2015), Kim and Lakshmanan (2015)	Intervalle - Likert
Utilité perçue des paramètres	Utilité perçue, Attitude face à la sécurité	Modèle TAM, Attitude to the Ad general, Attitude to the Ad Meaningfull	Davis (1989), Lehnert, Till, and Ospina (2014), Kim and Lakshmanan (2015)	Intervalle - Likert

Facilité d'utilisation	Facilité d'utilisation des paramètres	Modèle TAM	Davis (1989) – TAM, Venkatesh et al. (2003) – UTAUT	Intervalle - Likert
Attente de performance.	Efficacité perçue de la Loi 25	Modèle UTAUT	Venkatesh et al. (2003) – UTAUT	Intervalle - Likert
Perception de la vulnérabilité	Perception psychologique, résignation	Reactance (intrusiveness), Affective response to the ad (Vulnerability)	Martin et al., 2017, Aguirre et al. (2015), Bleier and Eisenbeiss (2015).	Intervalle - Likert
Adoption des Fintech	Confiance dans les Fintech, expérience passée, fréquence d'utilisation	Échelle élaborée pour notre étude	Venkatesh et al. (2003)	Intervalle - Likert

Source : auteur

3.6 Considérations éthiques de notre recherche

Avant la réalisation du prétest de cette étude, toutes les procédures ont été ajustées pour répondre aux critères du comité d'éthique de notre établissement d'enseignement (ESG UQAM), à qui un protocole a été présenté et validé en 2024. En effet, le comité d'éthique de la recherche pour les projets étudiants impliquant des êtres humains (CERPÉ plurifacultaire) a pour mandat de procéder à l'approbation éthique initiale et de manière continue des projets de recherche soumis par les étudiants des facultés et écoles telles que la faculté des sciences de la gestion (ESG UQAM). Ce comité est le responsable du respect des normes éthiques afin que les étudiants mènent leurs

travaux de manière responsable. Il s'assure également de la protection des individus impliqués dans les recherches pour qu'ils soient traités avec respect. Dans cette optique, le CERPÉ plurifacultaire s'aligne sur ces principes directeurs :

- Le respect des personnes
- La préoccupation pour le bien-être
- La justice.

Notre recherche porte sur le sentiment de vulnérabilité des consommateurs québécois suite à l'application de la Loi 25 dans le contexte des plateformes Fintech. L'ensemble des principes essentiels d'éthique la concernant impliquant des humains ont été observés, y compris le respect de la dignité, de l'autonomie, de la confidentialité et de l'intégrité des personnes. Toutes les données ont été réunies grâce à un questionnaire en ligne anonyme et autoadministré, distribué à un échantillon adulte. Avant de commencer le questionnaire, les participants ont été renseignés sur le sujet d'étude, ses buts et sur les droits des répondants, y compris celui de retirer à tout moment sans avoir à justifier leur décision.

En outre, nous avons assuré la confidentialité des réponses durant tout le processus et les informations ont été conservées sur un serveur sécurisé. Il n'y a pas eu d'analyse individuelle et les résultats sont uniquement présentés de manière globale. Il n'y avait aucun risque prévu lié à la participation. Les bénéfices escomptés sont avant tout d'ordre scientifique, en particulier concernant la détermination des impacts des bannières de sécurités créées par les concepteurs UX sur le sentiment de vulnérabilité des utilisateurs dans le contexte des technologies financières.

3.7 Prétest

Malhotra définit le prétest comme étant l'examen du questionnaire sur de petits groupes de participants pour détecter des problèmes potentiels (Malhotra, 2011). Avant la diffusion définitive du questionnaire, un test préliminaire a été effectué sur 66 personnes pour garantir la clarté, l'adéquation et la fiabilité des échelles de mesure qui ont été traduites et ajustées au contexte de notre étude. Cette démarche méthodique indispensable a aidé à détecter des problèmes d'embranchements entre les questions et certaines mises à jour qui n'avaient pas été correctement

enregistrées lors de la validation du sondage. Par la suite, une étude des coefficients de l'alpha de Cronbach a été réalisée sur les réponses obtenues lors du prétest. Ce coefficient sert à évaluer la solidité interne des échelles employées, c'est-à-dire le niveau auquel les éléments constituant une même variable mesurent effectivement un concept partagé.

Le tableau suivant présente toutes les modifications effectuées sur le formulaire suite à la réalisation du prétest.

Tableau 3-3: Ajustements au prétest.

Questions	**Variables**	**Types de modification**		
		Conserver	**Ajuster**	**Supprimer**
Questions filtres	Consentement à l'étude		✓	
	Lieu de résidence	✓		
	Âge	✓		
	Fréquence d'utilisation d'appareils connectés	✓		
	Fréquence d'utilisation de services bancaires en ligne	✓		
Mise en situation projective	Action prioritaire		✓	
	Attitude		✓	
	Utilité		✓	

	Clarté et pertinence		✓	
	Contrôle des données		✓	
	Consentement aux données	✓		
	Résignation	✓		
	Utilisation des données			
Connaissance de la Loi 25 et réactions face aux politiques de confidentialité.	Perception de la Loi 25	✓		
	Lecture des paramètres	✓		
Perception de la vulnérabilité dans les services bancaires en ligne.	Facilité d'utilisation des paramètres	✓		
	Crainte d'utilisation des services bancaires	✓		
	Confiance aux entreprises de service bancaire en ligne	✓		
	Relation entre Loi 25 et vulnérabilité perçue	✓		
	Transparence des entreprises de Fintech		✓	
	Expériences passées		✓	

Variables individuelles	Connaissances des outils de protection	✓		
	Connaissances de la protection des données			✓
	Mesures d'acceptation			✓
	Stratégies palliatives			✓
	Durée de résidence au Québec			✓
	Genre	✓		
	Région de résidence	✓		
	Statut professionnel	✓		

Nous avons dû totalement supprimer plusieurs questions dans le but de conserver les variables les pertinentes de notre rapport et aussi, le questionnaire était jugé beaucoup trop long par les répondants qui constituaient notre population d'étude. De ce fait, nous nous sommes focalisés sur les variables liées à l'utilité, à l'attente de performance et à la facilité d'utilisation des paramètres de sécurité, à la connaissance de la Loi 25 et à la protection des données, à la transparence des plateformes de Fintech et à la vulnérabilité des consommateurs.

Par ailleurs, nous avons apporté des adaptations à la question Action prioritaire, car au départ c'était un ensemble de 6 questionnaires qui avaient été créés, mais ils ont été regroupés en un sondage unique. De ce fait, nous sommes quittés de quatre ou cinq réponses pour cet item qui représentaient chacune une bannière fictive précise à 8 réponses pour l'ensemble des mesures de protection projetées. Il est important de souligner que cette interrogation était cruciale, car elle

visait à vérifier si le participant avait effectivement lu la publication. Le participant devait donc sélectionner parmi ces huit réponses en précisant, d'après lui-même, quel passage résumait le mieux son action sur la page d'accueil qu'il venait de consulter. Les réponses à choix sont les suivantes :

- Refuser l'utilisation des cookies (je refuse)
- Valider le consentement des cookies (je suis d'accord)
- Modifier le paramétrage des cookies (modifier mes préférences)
- Lire la politique de confidentialité (Politique de confidentialité)
- Contacter l'entreprise pour ses différents services (contactez-nous)
- Consulter les prestations proposées (nos prestations)
- Valider les cookies essentiels
- Quitter le site faute de paramètres

Afin de simplifier la compréhension de cette partie aux répondants lors du sondage, une projection individuelle d'une page spéciale a été faite pour attirer leur attention sur la page d'accueil qui devait suivre et se présentait ainsi :

ATTENTION

Prenez le temps de consulter cette page d'accueil fictive du site web Atlas.

Considérez que cette page d'accueil vous est présentée lorsque vous accédez sur le site web de l'entreprise Atlas.

La question sur le lieu de résidence (résidez-vous au Québec) fait partie des questions filtres, car la Loi 25, étant une Loi qui ne s'applique qu'au Québec, ne permettait l'intervention que des résidents de cette partie du Québec. Ceci a amélioré notre précision concernant les caractéristiques de la population d'études. En outre, les questions sur les fréquences d'utilisation des appareils connectés et des services bancaires sont nécessaires parmi les questions filtres, car il serait presque impossible d'avoir eu à consulter des paramètres de sécurité sur une plateforme si on n'utilise pas les appareils connectés.

Au final, il y'a des questions qui ont dû être ajustées afin que le sondage soit simple et clair à la compréhension des répondants et d'autres ont été déplacées afin que les questions d'un même thème soient réunies en un bloc.

Nous avons effectué une analyse du coefficient alpha de Cronbach, également connu sous le nom d'indice alpha de Cronbach, qui est une méthode utilisée pour juger l'uniformité des résultats

(Cronbach, 1951). Pour être exactes, il est nécessaire que les composantes évaluant une variable présentent une cohérence interne. De 0 à 1, l'alpha de Cronbach peut varier. Plus le coefficient est proche de 1, plus la méthode de mesure est jugée fidèle. Selon Malhotra (2011), un coefficient de 0,6 ou supérieur témoigne d'une cohérence interne satisfaisante.

3.7.1 Échelle sur l'attitude face aux paramètres (Attitude to the Ad : General)

L'échelle sur l'attitude de l'utilisateur envers les paramètres de sécurité a été inspirée de l'échelle sur l'attitude face à une publicité proposée par Kim and Lakshmanan en 2015. Pour évaluer le degré d'attention et d'absorption d'un individu face à une publicité, on se sert de trois éléments Likert en sept points (Kim and Lakshmanan, 2015). L'échelle est générale puisque les déclarations ne spécifient pas quel aspect de la publicité a suscité l'intérêt. De plus, étant donné la formulation d'un critère spécifique, l'échelle pourrait servir de mesure de l'implication de l'utilisateur lorsqu'il se retrouve en face des paramètres de sécurité sur un site ou une plateforme. L'alpha de Cronbach de l'attitude est égal à .954 ce qui signifie que la mesure est fidèle.

Tableau 3-4: Échelle sur l'attitude

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Attitude face aux paramètres	• Je suis attentif (ve) face aux paramètres de sécurités présentées	.954
	• Je suis concentré (e) sur les paramètres de sécurité présentés	
	• Je consulte en détail ce qui m'est proposé comme choix de consentement	

3.7.2 Échelle sur l'utilité des paramètres (Attitude to the Ad : Meaningfull)

L'échelle d'origine, définie par Lenhnert et al. en 2014, est composée de quatre questions de types Likert et détermine dans quelle mesure une personne considère qu'une publicité spécifique

lui est appropriée et bénéfique. Dans notre cas, elle a été adaptée à 3 items et son alpha de Cronbach est de .903.

Tableau 3-5: Échelle sur l'utilité

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Utilité des paramètres	• La bannière de sécurité présentée est significative pour moi	.903
	• La bannière de sécurité présentée est utile pour moi	
	• La bannière de sécurité présentée est valable pour moi	

3.7.3 Échelle sur la clarté et la pertinence des bannières (Attitude to the Ad : Vividness)

Cette échelle comprend quatre différentiels sémantiques répartis en sept points, conçus pour évaluer la clarté et l'intensité visuelles d'une publicité spécifique (Kim and Lakshmanan, 2015). Cette échelle est tout aussi valide comme le présente son alpha de Cronbach (.799) dans le tableau 3.4.

Tableau 3-6: Échelle sur la clarté et la pertinence.

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Clarté et pertinence de la bannière	• L'annonce est concrète	.799
	• L'annonce est utile	
	• L'annonce est détaillée	
	• L'annonce est explicite	

3.7.4 Échelle sur le contrôle des données (Argument strength).

L'échelle qui mesure le contrôle des données est empruntée de Yeh et Jewell (2015). Nous l'avons choisie, car elle permet de mesurer à quel point les utilisateurs pensent que les paramètres

de protection définis sur le site leur sont persuasifs et apportent une valeur ajoutée sur le sujet. Elle est évaluée sur la base de trois items et comme les autres échelles, c'est le type Likert qui est utilisé. Son alpha de cronbach est de .886.

Tableau 3-7: Échelle sur le contrôle des données.

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Contrôle des données	• Les paramètres sont persuasifs	.886
	• Les paramètres sont informatifs	
	• Les paramètres m'ont donné un aperçu différent de mon consentement	

3.7.5 Échelle sur le consentement.

Inspirée de l'échelle sur la résignation de Bleir et Eisenbeis (2015), l'échelle sur le consentement évalue le niveau de résistance d'un client face à un objet précis qu'il considère qu'il lui a été imposé et l'accent est mis sur la liberté de décision des utilisateurs. L'échelle contient 7 items de type Likert, mais nous l'avons réduite à 3 et adapter les questions pour mesurer le consentement des utilisateurs face à la bannière de sécurité présentée. Son alpha de cronbach est de .226.

Tableau 3-8: Échelle sur le consentement

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Consentement	• Je considère que mon consentement est juste	.226
	• Je considère être satisfait de mon choix de consentement	
	• Je considère que mon consentement est forcé, car il n'est pas possible de refuser.	

3.7.6 Échelle sur la résignation (Reactance : intrusiveness).

Créée par Bleir et Eisenbeis (2015), l'échelle sur la résignation évalue le niveau de résistance d'un client face à un objet précis qu'il considère qu'il lui a été imposé et l'accent est mis sur la nature inadaptée de l'objet. L'échelle de base contient 7 items de type Likert, mais nous l'avons réduite à 3 dans notre cas d'analyse pour mesurer le consentement des utilisateurs face à la bannière de sécurité présentée. Son alpha de cronbach est de .953.

Tableau 3-9: Échelle sur la résignation

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Résignation	• Je me sens impuissant face aux paramètres de sécurité du site	.953
	• Les paramètres du site sont intrusifs	
	• Les paramètres du site me sont imposés	

3.7.7 Échelle sur les perceptions psychologiques (Affective Response to the Ad).

L'échelle sur les perceptions psychologiques permet d'évaluer le degré d'exposition et de sentiment d'un individu face à une publicité, on emploie cinq indicateurs Likert en sept points (Aguirre et al., 2015). Elle est utilisée quand l'accent est mis sur le ressenti psychologique de l'utilisateur face à une page d'accueil. Son alpha de Cronbach est de .681.

Tableau 3-10: Échelle sur les perceptions psychologiques

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Perceptions psychologiques	• Je me sens exposé (e) sur cette page d'accueil	.681
	• Je me sens vulnérable sur cette page d'accueil	
	• Je me sens protégée sur cette page d'accueil	
	• Je me sens susceptible vis-à-vis de cette page d'accueil	

3.7.8 Échelle sur l'utilisation à long terme (Privacy of response).

Mesurer l'utilisation à long terme revient à mesurer la croyance d'une personne que ses informations sur un thème spécifique demeureront privées ou publiques à partir d'items de type Likert. Son alpha de Cronbach est défini dans le tableau 3.9.

Tableau 3-11: Échelle sur l'utilisation à long terme.

Échelle adaptée	**Items adaptés**	**Alpha de cronbach α**
Utilisation à long terme	• J'ai l'impression que mes informations seront rendues publiques à travers ce site.	-1,834
	• J'ai l'impression que ces informations resteront anonymes et confidentielles sur ce site.	

3.8 Analyse du prétest

Notre formulaire d'enquête a été prétesté auprès de 66 individus pour estimer le temps de réponse, relever les questions mal comprises et de possibles problèmes d'embranchement, tout problème pouvant nuire à la collecte des données (D'Astous, 2019).

Après avoir présenté une analyse sur la fiabilité des diverses échelles de mesure de notre étude et la procédure de réalisation de notre prétest, nous établissons l'analyse statistique de notre prétest. Dès lors, nous avons eu recours à l'analyse factorielle en composantes principales basée sur la méthode par Oblimin directe pour limiter le nombre d'items par variable pour notre questionnaire final (Hair et al., 1998). Cette méthode d'analyse est l'une des plus populaires en données multivariées et elle évalue la validité des résultats en se basant sur la validité convergente qui correspond à la corrélation entre les éléments d'une variable et la validité discriminante qui représente l'absence de relation entre les items d'une variable et ceux d'une autre (Godin-Bergeron, 2017). Nous avons précédemment utilisé l'alpha de Cronbach pour déterminer la fiabilité de l'échelle et le test de Bartelett qui va suivre, révèle la dépendance des items (Malhotra, 2011).

Pour que le test de corrélation (test de Bartelett) soit différent de la matrice d'identité et puisse offrir une justification de l'emploi de l'analyse factorielle, il doit être significatif donc avoir un p

≤ 0,050 (Stewart, 1981). L'évaluation des corrélations entre les éléments a été réalisée grâce au test de Kaiser Mayer Olkin (KMO). Lorsque l'indice de KMO varie entre 0 et 1, il fournit plus d'informations à la matrice de corrélation (Malhotra, 2011). Il est recommandé que le résultat dépasse 0,5 afin d'être qualifié de satisfaisant. Plus l'indice du KMO est élevé, plus l'analyse factorielle est pertinente.

3.8.1 Analyse statistique de l'échelle sur l'attitude de l'utilisateur.

L'échelle sur l'attitude des utilisateurs vis-à-vis des paramètres de sécurité a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les trois items que comprend cette échelle.

Comme présentés dans le tableau 3.11, les résultats pour cette analyse que révèlent l'alpha de Cronbach est de 0.954 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, une bonne qualité suffisante de la corrélation entre les items est démontrée par un indice KMO = 0.731. Le pourcentage total de la variance cumulée suggère que 91,6% des items contribuent à la variance de la variable.

Tableau 3-12: Analyse statistique échelle sur l'attitude

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
Attitude face aux paramètres	• Je suis attentif (ve) face aux paramètres de sécurités présentés	.954	<.001	.731	91.662
	• Je suis concentré (e) sur les paramètres de sécurité présentés				
	• Je consulte en détail ce qui m'est proposé comme choix de consentement				

3.8.2 Analyse statistique de l'échelle sur l'utilité des paramètres de sécurité.

L'échelle sur l'utilité des paramètres de sécurité a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les trois items que comprend cette échelle.

Comme présentés dans le tableau 3.12, les résultats pour cette analyse révèlent que l'alpha de Cronbach est de 0.903 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, une bonne qualité suffisante de la corrélation entre les items est démontrée par un indice KMO = 0.648. Le pourcentage total de la variance cumulée suggère que 84,6% des items contribuent à la variance de la variable.

Tableau 3-13: Analyse statistique échelle sur l'utilité

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
Utilité perçue des paramètres	• La bannière de sécurité présentée est significative pour moi	.903	<.001	.648	84,6%
	• La bannière de sécurité présentée est utile pour moi				
	• La bannière de sécurité présentée est valable pour moi				

3.8.3 Analyse statistique de l'échelle sur la clarté et la pertinence des paramètres de sécurité.

Les échelles sur la clarté et la pertinence des paramètres de sécurité ont été mesurées sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les quatre items que comprend cette échelle.

Comme présentés dans le tableau 3.13, les résultats pour cette analyse que révèlent l'alpha de Cronbach est de 0.799 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, la qualité suffisante de la corrélation entre les items est démontrée par un

indice KMO = 0.520. Le pourcentage total de la variance cumulée suggère que 94,6% des items contribuent à la variance de la variable.

Tableau 3-14: Analyse statistique échelle sur la clarté et la pertinence.

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
Clarté et pertinence de la bannière	• L'annonce est concrète • L'annonce est utile • L'annonce est détaillée • L'annonce est explicite	.799	<.001	.520	94,6%

3.8.4 Analyse statistique de l'échelle sur le contrôle des données.

L'échelle sur le contrôle des données a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les trois items que comprend cette échelle.

Comme présentés dans le tableau 3.14, les résultats pour cette analyse révèlent que l'alpha de Cronbach est de 0.799 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, la qualité suffisante de la corrélation entre les items est démontrée par un indice KMO = 0.683. Le pourcentage total de la variance cumulée suggère que 81,5% des items contribuent à la variance de la variable.

Tableau 3-15: Analyse statistique échelle sur le contrôle des données.

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
	• Les paramètres sont persuasifs				

Contrôle des données	• Les paramètres sont informatifs • Les paramètres m'ont donné un aperçu différent de mon consentement	.886	<.001	.683	81,5%

3.8.5 Analyse statistique de l'échelle sur le consentement .

L'échelle sur le consentement à l'utilisation de nos données a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les trois items que comprend cette échelle.

L'item : Je considère que mon consentement est forcé, car il n'est pas possible de refuser a été supprimé, car lors du calcul du KMO, le résultat était faible (KMO = .470 et α = .226) et la qualité de représentation de cet item était négatif avec un résultat de la matrice des composantes = -,421 ce qui rendait la valeur de l'échelle sur le consentement faible.

Après suppression de l'item : Je considère que mon consentement est forcé, car il n'est pas possible de refuser et comme présentés dans le tableau 3.15, les résultats révèlent que l'alpha de Cronbach est de 0.975 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, la qualité suffisante de la corrélation entre les items est démontrée par un indice KMO = 0.683. Le pourcentage total de la variance cumulée suggère que 81,5% des items contribuent à la variance de la variable.

Tableau 3-16: Analyse statistique échelle sur le consentement à l'utilisation des données.

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
Consentement	• Je considère que mon consentement est juste • Je considère être satisfait de mon choix de consentement	.975	<.001	.500	97,8%

3.8.6 Analyse statistique de l'échelle sur la résignation.

L'échelle sur la résignation à l'utilisation de nos données a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les trois items que comprend cette échelle.

Comme présentés dans le tableau 3.16, les résultats pour cette analyse révèlent que l'alpha de Cronbach est de 0.953 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, la qualité suffisante de la corrélation entre les items est démontrée par un indice KMO = 0.776. Le pourcentage total de la variance cumulée suggère que 91,3% des items contribuent à la variance de la variable.

Tableau 3-17: Analyse statistique échelle sur la résignation à l'utilisation des données.

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
Résignation	• Je me sens impuissant face aux paramètres de sécurité du site	.953	<.001	.776	91.3%
	• Les paramètres du site sont intrusifs				
	• Les paramètres du site me sont imposés				

3.8.7 Analyse statistique de l'échelle sur la perception psychologique.

L'échelle sur la résignation à l'utilisation de nos données a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les quatre items que comprend cette échelle.

Comme présentés dans le tableau 3.17, les résultats de cette analyse révèlent que l'alpha de Cronbach est de 0.681 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, la qualité suffisante de la corrélation entre les items est démontrée par un

indice KMO = 0.500. Le pourcentage total de la variance cumulée suggère que 98.7% des items contribuent à la variance de la variable.

Tableau 3-18: Analyse statistique échelle sur la perception psychologique.

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**
Perceptions psychologiques	• Je me sens exposé (e) sur cette page d'accueil	.681	<.001	.500	98.709
	• Je me sens vulnérable sur cette page d'accueil				
	• Je me sens protégée sur cette page d'accueil				
	• Je me sens susceptible vis-à-vis de cette page d'accueil				

3.8.8 Analyse statistique de l'échelle sur l'utilisation des données à long terme.

L'échelle sur l'utilisation des données à long terme a été mesurée sur une échelle de type Likert à 7 points allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord) pour les quatre items que comprend cette échelle.

Comme présentés dans le tableau 3.18, les résultats de cette analyse révèlent que l'alpha de Cronbach est de 0.740 avec un test de Bartelett significatif qui est <.001. Ces données montrent donc que la matrice de corrélation ne constitue pas une matrice identité et les items sont corrélés entre eux. Par ailleurs, la qualité suffisante de la corrélation entre les items est démontrée par un indice KMO = 0.500. Le pourcentage total de la variance cumulée suggère que 74% des items contribuent à la variance de la variable.

Tableau 3-19: Analyse statistique échelle sur l'utilisation des données à long terme.

Échelles adaptées	**Items adaptés**	**Alpha de cronbach**	**Test de Bartelett**	**Indice KMO**	**% de la variance**

Utilisation à long terme	• J'ai l'impression que mes informations seront rendues publiques à travers ce site. • J'ai l'impression que les informations resteront anonymes et confidentielles sur ce site.	.740	<.001	.500	74%

3.8.9 Tests multivariés.

Une analyse multivariée a été effectuée sur les échelles présentées précédemment. L'analyse multivariée de la variance plus connue sous l'abréviation MANOVA est définie comme étant une méthode qui permet de comparer les moyennes de population multivariées de différents groupes et est généralement employée lorsqu'il existe deux variables dépendantes ou encore plus (*SPSS Statistics Subscription - Early Access*, 2021). Afin d'évaluer la signification statistique des divergences de moyenne, on effectue principalement une comparaison entre la variance et la covariance des différentes variables à partir de notre seuil de signification (noté α) qui est égale à 0.05.

On se sert du lambda de Wilks et du tracé de Pillai pour vérifier s'il existe une différence entre ces moyennes des groupes de sujets identifiés sur une combinaison de variables dépendantes (vecteurs de moyennes) (Zuccaro, 2023). De ce fait, si $p \leq \alpha$: les différences entre les moyennes sont statistiquement significatives et si $p > \alpha$: les différences entre certaines moyennes ne sont pas statistiquement significatives (Minitab, 2024).

Tableau 3-20: Tests multivariés

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel	Paramètre Paramètre	Puissance observée[d]
Constante	Trace de Pillai	,998	2697,634[b]	8,000	44,000	<,001	,998	21581,069	1,000
	Lambda de Wilks	,002	2697,634[b]	8,000	44,000	<,001	,998	21581,069	1,000
	Trace de Hotelling	490,479	2697,634[b]	8,000	44,000	<,001	,998	21581,069	1,000
	Plus grande racine de Roy	490,479	2697,634[b]	8,000	44,000	<,001	,998	21581,069	1,000
Sondage	Trace de Pillai	1,527	3,627	32,000	188,000	<,001	,382	116,048	1,000
	Lambda de Wilks	,129	3,800	32,000	163,859	<,001	,401	109,499	1,000

Source : créé par l'auteur.

À partir des résultats présentés dans le tableau 3.19, nous pouvons affirmer que l'hypothèse nulle est rejetée donc il y'a une relation significative entre le type de sondage ou de bannière présentée et les variables dépendantes, car SIG < α. Et nous pouvons également conclure qu'à partir du tracé de Pillai, 38,2% de la variation de la variabilité observée dans les variables dépendantes s'explique par le type de sondage auquel le répondant fait face et ce pourcentage est de 40,1% selon le lambda de Wilks.

CHAPITRE 4 :
RÉSULTATS

Ce chapitre dévoile les principaux résultats des analyses portant sur la vulnérabilité perçue des consommateurs québécois en ligne suite à l'application de la Loi 25 dans le contexte des services de technologies financières. Les analyses et résultats de l'étude des modèles de conception des bannières utilisés dans le secteur de la Fintech québécoise seront exposés d'abord, puis s'en suivront les résultats du sondage appliqués à notre échantillon d'études.

4.1 Analyse des paramètres de sécurité réalisés dans le secteur de la Fintech Vs les autres secteurs au Québec

4.1.1 Analyse des paramètres de sécurité conçus par les entreprises au Québec.

Un total de 134 captures d'écran de paramètres de sécurité d'entreprises (tous secteurs confondus) exerçant au Québec ont été effectuées. Nous nous sommes arrêtés à ce nombre d'entreprises, car nous étions arrivés à une saturation d'information et de types de paramètres de sécurité existante.

De ces captures, nous avons pu obtenir ces critères :

- **Tout accepter** : les entreprises qui mettent en pratique ce type de paramètres représentent 29,8% de notre échantillon d'étude donc à peine 4 entreprises sur 134 ne donnent pas la possibilité aux utilisateurs d'émettre des choix au niveau du consentement sur l'utilisation de leurs informations personnelles par les plateformes.
- **Accepter ou configurer** : le pourcentage d'utilisation de ce type de paramètres équivaut à 34,3% de la taille de notre échantillon pour 46 entreprises. Ce modèle de bannière est celui qui est le plus utilisé par les concepteurs des sites web des entreprises au Québec. Le consentement est partiel dans ce cas d'espèce.
- **Consentement libre** : Ce modèle vient en deuxième position après le modèle accepter avec possibilité de configuration. 41 entreprises mettent en pratique ce type de paramètres de sécurité, ce qui décrit 30,7% de notre population d'étude. Pour rappel, ce type de

consentement est celui qui offre un meilleur choix en termes de consentement d'utilisation de ses données personnelles.

- **Accepter avec politique de confidentialité** : pas très différente du modèle de bannière tout accepter, cette bannière est utilisée par 24 entreprises de notre population pour un pourcentage représentatif de 17,9%.
- **Cookies essentiels** : 6 entreprises de notre échantillon utilisent ce type de bannière, ce qui équivaut à 4,5% de notre population.
- **Pas de paramètres** : parmi les entreprises sélectionnées, 13 n'ont pas de paramètres de sécurité. Ce nombre en pourcentage est de 9,7%.

4.1.2 Analyse des bannières de sécurité utilisées par les Fintechs au Québec

Sur les 257 entreprises évoluant dans le secteur de la Fintech au Québec, nous avons réalisé l'étude de 130 bannières de sécurité établies dans ce secteur d'activité. Il en résulte que :

- 7 entreprises de Fintech sur 130 utilisent la bannière de sécurité **Tout accepter** : les entreprises qui mettent en pratique ce type de paramètres représentent donc 5,38% de notre échantillon d'étude.
- Pour ce qui de la bannière **Accepter ou configurer,** les analyses sont égales à celles de la bannière de sécurité **Tout accepter,** car le pourcentage d'utilisation de ce type de paramètres équivaut à 5,38% de la taille de notre échantillon pour 07 entreprises.
- Le modèle de bannière **Consentement libre** vient en deuxième position, car représente 16,15% des modèles utilisés par les Fintechs de notre étude. Juste 21 entreprises Fintech mettent en pratique ce type de paramètres de sécurité qui semble être le modèle le plus recommandé en termes de meilleures pratiques vu qu'il permet aux utilisateurs d'avoir un consentement éclairé sur l'utilisation et la gestion de ses données personnelles.
- Le modèle de bannière **Accepter avec politique de confidentialité** est celui qui est moins utilisé par les concepteurs des sites web des Fintechs québécoises. Le consentement est partiel dans ce cas d'espèce. Cette bannière est utilisée par 03 entreprises de notre population pour un pourcentage représentatif de 2,30%.
- Le paramètre de sécurité Cookies essentiels est utilisé par deux entreprises Fintech de notre échantillon pour un pourcentage de 1,53% de notre population d'étude.

- 90 des 130 entreprises Fintech étudiées n'ont pas de paramètre de sécurité, elles représentent le taux le plus élevé qui est de 69,23%.

4.1.3 Discussion sur les bannières de sécurité conçues

L'examen comparatif des paramètres de sécurité indique des différences marquées entre les entreprises Fintech et les autres domaines d'activités au Québec concernant la conception des bannières de sécurité. De manière significative, les entreprises Fintech démontrent un taux considérable d'absence de mesures de sécurité visibles sur leurs plateformes en ligne (69,23%) comparativement aux autres sociétés analysées (9,7%). Cette absence notoire, qui va à l'encontre des principes de transparence et de consentement éclairé imposés par la Loi 25, soulève d'importantes questions relatives à la protection des données privées dans le secteur des technologies financières. De même, les entreprises Fintech sont moins représentées dans les modèles de bannières jugées les plus respectueuses des droits des utilisateurs, comme celles proposant un consentement libre (16,15% pour les Fintechs comparativement à 30,7% dans l'échantillon global) ou encore celles proposant l'option accepter ou configurer (5,4% contre 34,3%). Ces résultats indiquent que les plateformes Fintech ont tendance à minimiser les options de configuration personnalisée des cookies ou à exclure entièrement ces dispositifs, ce qui pourrait accentuer le sentiment de vulnérabilité des utilisateurs.

À contrario, les modèles des bannières les plus courants dans les autres acteurs d'activité (accepter ou configurer, consentement libre) démontrent un plus grand désir d'intégrer l'utilisateur au processus décisionnel concernant l'utilisation de ses données. Ces méthodes sont davantage en accord avec les principes de consentement explicite, de transparence et de personnalisation soulignés dans le cadre réglementaire du Québec.

En fin de compte, cette différence sectorielle dans la création des interfaces de consentement pourrait partiellement justifier les résultats que nous avons constatés dans notre étude sur la perception du sentiment de vulnérabilité du consommateur québécois en ligne. Il serait donc bénéfique pour les entreprises de Fintech d'adopter des pratiques les plus transparentes et interactives dans le but de consolider la confiance numérique et de mieux répondre aux exigences imposées par la Loi 25.

4.2 Analyse de notre population d'étude

4.2.1 Représentativité de l'échantillon

La collecte des données a été effectuée de décembre 2024 à février 2025 à travers l'outil de sondage Qualtrics et un partage des affiches de recrutements. Dans un premier temps, nous avons transmis un lien de participation via notre réseau social WhatsApp, puis sur notre page et sur les différents groupes Facebook auxquels nous appartenons. Des publications ont également été faites sur notre page LinkedIn. Afin d'accélérer la collecte des données, nous avons partagé et collé des affiches de recrutement au sein de l'UQAM dans un second temps.

À partir de mes publications d'origine, des republications ont été faites par notre répertoire et tous ces partages nous ont permis d'obtenir 384 réponses au sondage. Les 4 premières réponses ont été supprimées, car elles étaient relatives à un prétest du sondage et les données étaient invalides. Par la suite, un groupe de questions ont été supprimées, car, à partir des questions filtres, si le répondant avait plus de 65 ans, ne résidait pas au Québec ou n'utilisait pas de services bancaires en ligne, il était automatiquement dirigé à la fin du questionnaire et sa participation invalide. Pour finir, le dernier lot de réponses supprimé correspondait au lot dont les répondants n'avaient pas fini de compléter leurs questionnaires et elles correspondaient à environ à 50% des réponses supprimées.

Par conséquent, cette recherche se base sur un échantillon définitif de 300 personnes, en raison de 50 participants par bannière de sécurité fictive présentée tels que c'est configuré dans le logiciel Qualtrics. Les données obtenues ont été extraites de Qualtrics pour des analyses statistiques menées sur le logiciel SPSS.

4.2.2 Profil sociodémographique de la population

Nous établissons des questions sociodémographiques dans le but d'axer et de segmenter les participants à l'étude en fonction des attributs sociaux ou démographiques (Barthelot, 2015). L'analyse de la représentativité de l'échantillon a permis d'évaluer si les attributs sociodémographiques des participants reflétaient ceux de la population visée. De ce fait, les profils mis en avant dans notre étude sont le genre, l'âge de la population d'étude et leurs profils selon les différentes bannières de sécurité utilisées dans notre étude comme le reflète le tableau 4.1.

Tableau 4-1: Profil sociodémographique des répondants

Variables	Modalités	Fréquence	Pourcentage	Acc. avec politique	Acc. ou paramétrer	Acc. tout	Cons. éclairé	Cookies essentiels	Sans bannière
Genre	Masculin	150	50	22	25	37	24	20	22
	Féminin	137	45,7	28	25	9	25	25	25
	Non binaire	1	0,3	0	0	1	0	0	0
	Autre	5	1,7	0	0	2	0	3	0
	Je préfère ne pas répondre	7	2,3	0	0	1	1	2	3
Total	**Effectif**	**300**	**100,0**	**50**	**50**	**50**	**50**	**50**	**50**
Âge	18-23 ans	45	15	7	15	4	7	6	6
	24-29 ans	84	28	12	24	12	15	12	19
	30-35 ans	82	27,3	18	10	12	17	14	11
	36-41 ans	50	16,7	8	7	14	5	10	6
	42-47 ans	20	6,7	5	1	4	3	2	5
	48-53 ans	12	4,0	0	3	1	1	6	1
	54-59 ans	7	2,3	0	0	3	2	0	2
Total	**Effectif**	**300**	**100,0**	**50**	**50**	**50**	**50**	**50**	**50**

Source : créé par l'auteur

À travers le tableau 4.1, nous constatons que notre population d'études est majoritairement constituée du genre masculin à 50 %, suivi de 45,7% par le genre féminin. Cet échantillon reflète la population québécoise de 2024, qui est relativement homogène entre 50,27 % d'hommes et 49,72 % de femmes (Statistique Canada, 2024). Le tableau nous permet également d'avoir un aperçu de la répartition des répondants à travers les différents sondages par genre et par âge. La présentation de la bannière de sécurité au répondant étant faite aléatoirement par l'outil de sondage Qualtrics, on ne pourrait établir un rapport entre le type de bannière et la représentation de la population.

La tranche d'âge comptant le plus grand nombre de participants est celle des individus âgés de 24 et 29 ans (84 répondants), suivie de près par la tranche d'âge de 30-35 ans (82 personnes) et la troisième tranche d'âge présente sur le podium est celle de 36 à 40 ans qui représente 50 personnes de la population d'études.

4.2.3 Profil d'utilisation des appareils connectés et des services bancaires en ligne

Afin de déterminer la fréquence d'utilisation des services bancaires en ligne des Québécois en ligne ainsi que leur fréquence d'interaction avec les appareils connectés et déterminer les différents profils d'utilisateurs (occasionnel, régulier, abusif), nous avons établi le tableau 4.2 qui donne un aperçu des modalités d'utilisation des appareils connectés et des services en ligne par tranche d'âge et par fréquence.

Cette étude permet de réaliser que les utilisateurs des services fintechs de notre population peuvent être considérés majoritairement comme des consommateurs réguliers, car 128 individus sur 300 ont recours aux services financiers 3 à 5 fois par semaine. Pour ce qui est de l'usage des appareils connectés, la modalité toute la journée remporte la première place avec un pourcentage de 68,7%, ce qui traduit une population addicte aux appareils connectés. Les répondants situés dans l'échelle d'âge entre (24-29 ans) et (30-34 ans) étant ceux les plus représentés dans notre échantillon, il est normal que leur pourcentage soit plus élevé dans chacune de ces deux analyses.

Tableau 4-2 : Profil d'utilisation des appareils connectés et services financiers en ligne

Variables	Modalités	Fréquence	18-23 ans	24- 29 ans	30–35 ans	36-41 ans	42-47 ans	48-53 ans	54-59 ans
Appareils connectés	1-5 fois	**20** **6.7%**	10%	40%	15%	5%	20%	10%	0%
	6-10 fois	**46** **15.3%**	17,4%	23,9%	19,6%	23,9%	6,5%	6,5%	2,2%
	11-12 fois	**28** **9,3%**	10,7%	32,1%	28,6%	7,1%	7,1%	7,1%	7,1%
	Toute la journée	**206** **68,7%**	15,5%	27,2%	30,1%	17,5%	5,3%	1,9%	1,9%
Total	**Effectif**	**300**	**15%**	**28%**	**27,3%**	**16,7%**	**6,7%**	**4%**	**2,3%**
Services financiers en ligne	0-2 fois	**74** **24,7%**	12,2%	37,8%	27%	10,8%	8,1%	2,7%	14,3%
	3-5 fois	**128** **42,7%**	12,5%	32%	24,2%	18%	7,8%	5,5%	0%
	6-8 fois	**54** **18%**	20,4%	24,1%	42,1%	16,7%	3,7%	3,7%	57,1%
	9-11 fois	**19**	21,1%	0%	40%	21,1%	10,5%	0%	14,3%

		6,3%							
	Plus de 12 fois	**25** **8,3%**	20%	8%	27,3%	24%	0%	4%	14,3%
Total	**Effectif**	**300**	**15%**	**28%**	**27,3%**	**16,7%**	**6,7%**	**4%**	**2,3%**

Source : créé par l'auteur

Les deux graphiques ci-dessous représentent les statistiques descriptives des fréquences d'utilisation des appareils connectés et des services financiers de notre population d'études afin d'avoir un meilleur visuel.

Figure 4-1 : Graphique de présentation des fréquences d'utilisation des services bancaires en ligne.

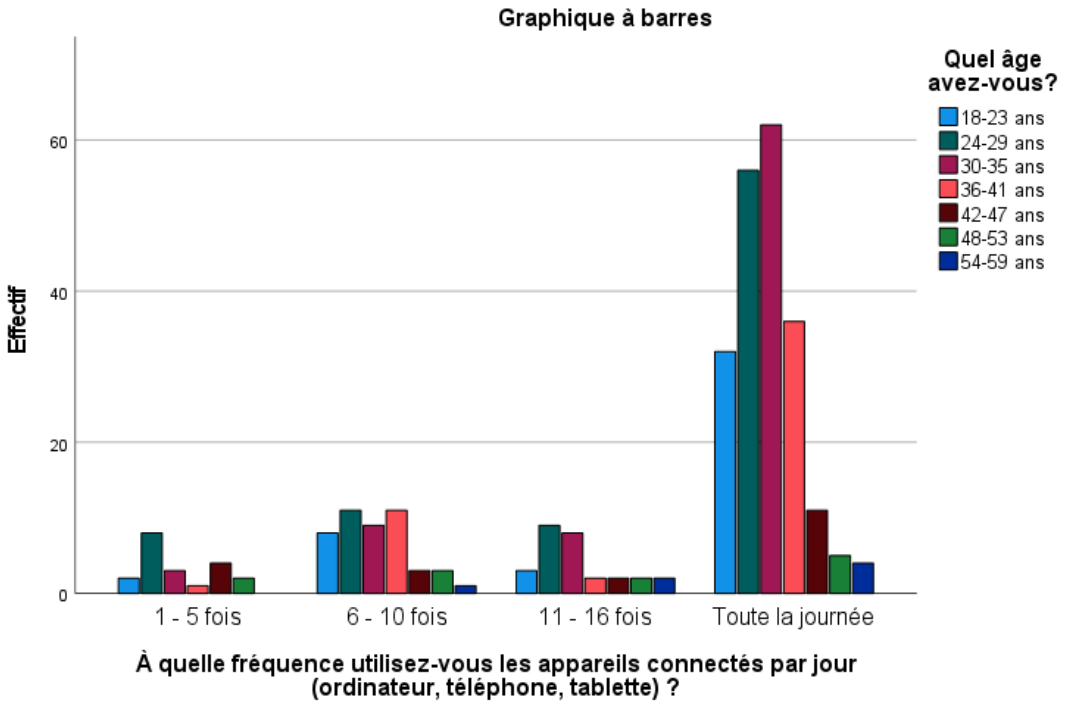
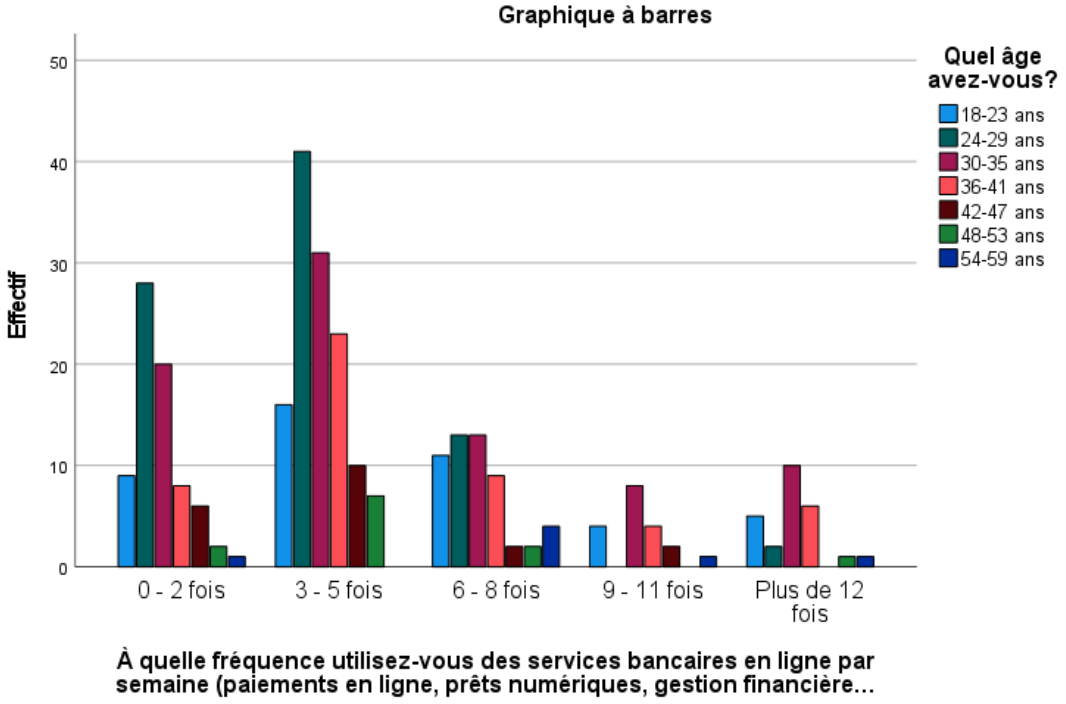


Figure 4-2 : Graphique de présentation des fréquences d'utilisation des appareils connectés en ligne.

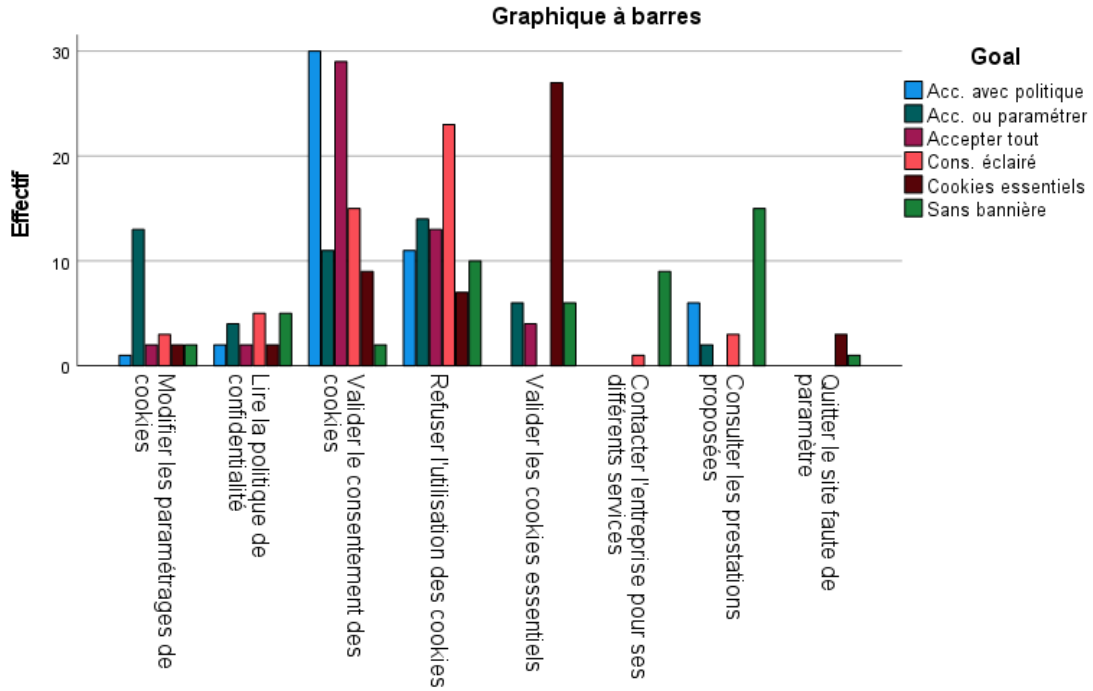


4.3 Tests descriptifs

Pour terminer avec l'examen des échelles de mesure de notre étude, nous présentons les résultats des analyses descriptives. Cela nécessite de déterminer la moyenne et l'écart type de chacune des échelles de mesure en se basant sur les nouvelles moyennes. La moyenne des variables est déterminée sur une échelle allant de 1 (pas du tout d'accord) à 7 (tout à fait d'accord).

Le graphique à barres de l'action prioritaire est également présenté pour avoir un meilleur visuel des variables descriptives de ces paramètres. Il en ressort que lorsque le choix est donné l'utilisateur de valide, de refuser ou de paramétrer ses bannières de sécurité, l'action prioritaire qui est la pus requise est refuser l'utilisation des cookies. En outre, nous pouvons relever que la présence ou l'absence de paramètres ne constitue pas un réel frein pour un utilisateur d'utiliser une plateforme tel que constater au travers de l'analyse de l'action quitter le site faute de paramètres.

Figure 4-3 : Graphique à barres action prioritaire



L'un des concepts clés que notre étude cherche à mesurer est la connaissance de la Loi 25. De ce fait, une analyse du niveau de connaissance de la Loi 25 par notre population a été effectuée et il en résulte que les parts sont presque égales. 152 personnes avaient déjà entendu parler de cette

Loi contre 148. Ce résultat peut être légitime dans la mesure où la Loi 25 a été établie récemment par le gouvernement, donc le degré de connaissance ne peut être similaire à une Loi présente depuis plusieurs années.

Tableau 4-3 : Analyses de la moyenne de connaissance de la Loi 25

Avez-vous déjà entendu parler de la Loi 25 régissant la vie privée des consommateurs québécois en ligne?

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	OUI	152	50,7	50,7	50,7
	NON	148	49,3	49,3	100,0
	Total	300	100,0	100,0	

4.4 Prémisses au test des hypothèses

Cette partie est cruciale pour notre rapport, car elle présente essentiellement toutes les analyses statistiques réalisées pour tester nos hypothèses de recherche. La technique de statistique inférentielle utilisée dans notre cas est l'analyse multivariée de la covariance (MANCOVA). Comme tous les tests de la famille ANOVA, Mancova permet de tester simultanément les effets d'une ou plusieurs variables indépendantes sur deux ou plusieurs variables dépendantes (Malhotra, 2011). La spécificité de Mancova est qu'elle est requise lorsque nous sommes en présence de plus d'une variable dépendante (Cassandra G, 2017). Cette dernière représente la variable à expliquer tandis que la variable indépendante (le facteur) représente la variable explicative. Ce facteur se compose de plusieurs éléments ou niveaux, chacun correspondant aux diverses catégories de la variable. Ces différents éléments constituent des groupes ou des échantillons de personnes.

Toutefois, il est impératif de s'assurer que les prémisses du test d'analyse de la MANCOVA sont respectées. Tout comme les autres tests d'hypothèses, il est nécessaire de vérifier certaines conditions préalables avant d'entamer l'analyse proprement dite (Éric Y. et Martine P., 2023). Ces conditions sont :

- L'indépendance des groupes ou échantillon aléatoire,
- La normalité des variables dépendantes,

- L’égalité des variances
- Absence de multicolinéarité
- Relation entre les variables dépendantes et les covariables

Effectivement, la fiabilité des conclusions dépend de plusieurs critères statistiques, y compris la normalité des variables dépendantes, l'uniformité des matrices de covariance entre les groupes, l'absence de multicolinéarité parmi les variables dépendantes, et l'indépendance des observations. Enfreindre ces suppositions pourrait mettre en péril la solidité des conclusions et provoquer des distorsions dans l'analyse.

4.4.1 Indépendance des groupes

Comme indiqué dans le chapitre consacré à la méthodologie, cette condition a été respectée grâce à l'approche sélectionnée pour la collecte de données. Effectivement, la méthode de sélection appelée « échantillonnage par boule de neige » a été utilisée pour distribuer les questionnaires aux participants. Cette sélection est effectuée de manière aléatoire, ce qui entraîne une variance de l'échantillon d’étude (Malhotra, 2011). Chaque groupe a donc subi un traitement unique et aucune relation n’existe entre les observations au sein d’un même groupe ni celles des différents groupes d’études.

4.4.2 Test de normalité

Il est possible de vérifier l’hypothèse de normalité de distribution en utilisant des mesures de forme et pour cela, nous avons recours aux tests d’asymétrie et d’aplatissement. Quand la distribution est normale, les donn.es se répartissent de manière symétrique autour du centre de la distribution, ce qui confère à la courbe une forme semblable à celle d’une cloche. Ainsi, la moyenne, la médiane et le mode sont identiques (Malhotra, 2011). Au cas contraire, on parle d’asymétrie (skewness) qui se réfère à la situation où la courbe est plus importante dans une direction que dans l’autre (Cassandra G, 2017). Son coefficient varie entre -0.5 et 0.5 (Daghfous, 2006). Le test d’aplatissement, appelé Kurtosis, évalue la platitude de la courbe (Hopkins et Weels, 1990). Selon Daghfous, le coefficient d’aplatissement varie entre -1 et 1, car une distribution normale correspond à une valeur de 0.

Tableau 4-4: Test de normalité des distributions

Variables	Test d'asymétrie (Skewness)	Test d'aplatissement (Kurtosis)
Attitude	-.633	-.199
Utilité	-.854	.504
Clarté	-.632	.096
Pertinence	-.478	.017
Consentement	-.142	-.617
Perception	.177	.694
Résignation	-.574	.099
Facilité d'usage	-.572	.187
Transparence plateforme	-.430	-.439
Efficacité Loi 25	-.694	.880
Confiance Fintech	-.418	-.467

Les résultats présentés dans ce tableau montrent que les variables attitude, utilité, clarté et résignation, facilité d'usage et efficacité Loi 25 ne respectent pas le coefficient d'asymétrie puisqu'elles ne sont pas comprises entre -0.5 et 0.5. Par contre, toutes ces valeurs respectent le test

de Kurtosis, car elles sont toutes comprises entre -1 et 1. Pour s'assurer de la normalité des distributions, on peut également analyser l'histogramme des différentes courbes (annexe B).

Les différentes courbes présentées montrent une légère divergence par rapport à celle de la distribution normale. Cependant, même si les tests de symétrie et d'aplatissement ne confirment pas l'hypothèse, on peut observer que les distributions adhèrent néanmoins à une courbe normale. En effet, l'analyse de la variance n'est généralement pas très réceptive aux variations des distributions lorsque l'échantillon est volumineux, comme c'est le cas dans cette recherche (Malhotra, 2011). Donc, il est possible d'effectuer une analyse de la variance.

4.4.3 Homogénéité des variances

On peut confirmer cette prémisse en observant le diagramme en boîte ou encore en effectuant le test de Levene qui est proposé dans les options ANOVA (Éric Y. et Martine P., 2023). Toutefois, il est essentiel d'effectuer ce test lorsque les groupes sont de taille différente (Malhotra, 2011). Si les groupes ont des tailles identiques, on peut ignorer cette hypothèse. Étant donné que nos six groupes d'études sont de groupe identique (50), nous pouvons de ce fait passer outre cette hypothèse.

4.4.4 Absence de multicolinéarité :

Le concept de multicolinéarité est établi pour définir la relation entre deux ou plusieurs variables indépendantes ou covariables. Pour examiner cette prémisse, nous utilisons le facteur d'inflation de la variance, connu en anglais sous l'acronyme VIF (Variance Inflation Factor). Une valeur proche de 1 indique qu'il n'y a pas de corrélation. Le tableau suivant présente les résultats de l'analyse effectuée.

Tableau 4-5 : Test de multicolinéarité

Variables	**Statistiques de colinéarité**	
	Tolérance	VIF

Perception	.672	1.488
résignation	.672	1.488

Par ailleurs, en effectuant le test de corrélation de Pearson, on obtient r = .573. Ces résultats prouvent que le test de multicolinéarité est respecté, car pour le test de VIF nous avons des résultats qui se rapprochent du chiffre 1 et un R<0.8. Ce qui signifie que les covariables analysées ne sont pas corrélées les unes des autres.

4.4.5 Relation entre les variables dépendantes et les covariables :

Nous devons en effet tester si les droites de régression sont homogènes. Pour comprendre cette condition, visualisons la création d'un nuage de point qui inclut la covariable et les valeurs associées à la variable dépendante pour tous les groupes formés par la variable catégorielle. Si nous observons une corrélation positive linéaire entre la variable dépendante pour un groupe et la covariable, nous souhaitons que cette tendance se maintienne pour tous les autres groupes (Éric Y. et Martine P., 2023).

Avant de présenter les résultats de cette analyse, il faut apporter un éclairci sur la covariance. On dit que deux variables covarient ensemble lorsque l'écart à la moyenne d'une variable est associé à un écart dans la même direction ou dans une direction opposée de l'autre pour le même sujet. Plus ce pattern est répandu dans l'ensemble des données, plus il apparaît que les deux variables entretiennent une association mutuelle. En d'autres termes, deux variables sont en covariance lorsqu'il semble que la fluctuation de l'une autour de sa moyenne a un impact sur la façon dont l'autre variable varie autour de sa moyenne. Ainsi, la covariance représente une mesure de la variance commune entre deux variables (Éric Y. et Martine P., 2023).

L'estimation de la covariance est directement liée à l'évaluation du lien linéaire entre deux variables continues. Si la covariance est positive, cela signifie qu'il existe une relation linéaire positive entre les variables. À l'inverse, si la covariance est négative, la relation linéaire entre ces

deux variables est également négative. L'évaluation de la puissance et de la direction de la relation entre deux variables se fait au moyen du coefficient de Pearson (r) (Éric Y. et Martine P., 2023).

Les nuages de points présentés en ANNEXE C illustrent une tendance linéaire entre les variables indépendantes et dépendantes dans chaque graphique, mettant en évidence une ligne droite discernable. Par ailleurs , le tableau de corrélation de Pearson révèle des $r \neq 0$ et des $p < 0.05$. Nous pouvons conclure que la condition d'homogénéité des droites de régression est respectée.

4.5 Tests des hypothèses

Cette partie vise à analyser, via des études statistiques, l'effet des diverses variables indépendantes sur la vulnérabilité des utilisateurs québécois dans le cadre de la Loi 25, leur rôle dans l'adoption des services Fintech en accord avec ladite Loi et pour finir répondre aux hypothèses de recherche préalablement définies.

4.5.1 **Hypothèse 1 :** Le type de bannière de bannière de sécurité conçu par les entreprises dans le secteur de la Fintech a un effet positif sur la réduction du sentiment de vulnérabilité perçu par les utilisateurs .

L'objectif de notre étude de recherche étant de comprendre et de démontrer l'impact de l'application de la Loi 25 sur la vulnérabilité des consommateurs québécois à travers le type de bannières de publicité présentée, nous apportons ces analyses complémentaires afin d'établir une relation statistique des variables type de bannière (goal) et sentiment de vulnérabilité

Comme toutes les analyses effectuées précédemment, nous commençons par le test de Box qui a déterminé que le coefficient de signification est égal à <0.001 et inférieur à la P-value 0.05, par conséquent nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-6 : Test des égalités des matrices de covariance Bannière et vulnérabilité

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	41,117
F	2,694
df1	15
df2	472780,028
Sig.	<,001

Nous allons de ce fait utiliser les résultats de la statistique de Pillai's Trace qui est plus robuste que les trois autres statistiques lorsque nous sommes en présence d'une violation de l'hypothèse d'égalité des matrices de covariance.

Tableau 4-7: Tests multivariés Relation entre type de bannière et vulnérabilité

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,389	92,459[b]	2,000	290,000	<,001	,389
	Lambda de Wilks	,611	92,459[b]	2,000	290,000	<,001	,389
	Trace de Hotelling	,638	92,459[b]	2,000	290,000	<,001	,389
	Plus grande racine de Roy	,638	92,459[b]	2,000	290,000	<,001	,389
A_ge	Trace de Pillai	,001	,184[b]	2,000	290,000	,832	,001
	Lambda de Wilks	,999	,184[b]	2,000	290,000	,832	,001
	Trace de Hotelling	,001	,184[b]	2,000	290,000	,832	,001
	Plus grande racine de Roy	,001	,184[b]	2,000	290,000	,832	,001
Genre	Trace de Pillai	,012	1,747[b]	2,000	290,000	,176	,012
	Lambda de Wilks	,988	1,747[b]	2,000	290,000	,176	,012
	Trace de Hotelling	,012	1,747[b]	2,000	290,000	,176	,012
	Plus grande racine de Roy	,012	1,747[b]	2,000	290,000	,176	,012
R_gion	Trace de Pillai	,008	1,164[b]	2,000	290,000	,314	,008
	Lambda de Wilks	,992	1,164[b]	2,000	290,000	,314	,008
	Trace de Hotelling	,008	1,164[b]	2,000	290,000	,314	,008
	Plus grande racine de Roy	,008	1,164[b]	2,000	290,000	,314	,008
Goal	Trace de Pillai	,120	3,720	10,000	582,000	<,001	,060
	Lambda de Wilks	,883	3,708[b]	10,000	580,000	<,001	,060
	Trace de Hotelling	,128	3,696	10,000	578,000	<,001	,060
	Plus grande racine de Roy	,069	4,022[c]	5,000	291,000	,002	,065

Les résultats de cette analyse montrent à suffisance que le facteur goal qui représente les différents types de bannière de sécurité a un impact statistiquement significatif sur la vulnérabilité des utilisateurs avec un coefficient de signification égal à <.001 et une distribution F de 3.720. Les covariables âge, genre et région n'ont aucun effet sur la vulnérabilité.

Analysons ensemble le tableau des tests des effets intersujets pour pouvoir répondre à notre hypothèse de recherche.

Tableau 4-8: Tests des effets intersujets Relation entre type de bannière et vulnérabilité

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	24,162[a]	8	3,020	2,504	,012	,064
	RESIGNATION	33,343[b]	8	4,168	2,506	,012	,064
Constante	PERCEPTION	201,234	1	201,234	166,828	<,001	,364
	RESIGNATION	201,548	1	201,548	121,171	<,001	,294
A_ge	PERCEPTION	,326	1	,326	,270	,604	,001
	RESIGNATION	,003	1	,003	,002	,966	,000
Genre	PERCEPTION	,061	1	,061	,050	,823	,000
	RESIGNATION	3,194	1	3,194	1,920	,167	,007
R_gion	PERCEPTION	2,492	1	2,492	2,066	,152	,007
	RESIGNATION	,278	1	,278	,167	,683	,001
Goal	PERCEPTION	21,750	5	4,350	3,606	,004	,058
	RESIGNATION	29,096	5	5,819	3,498	,004	,057
Erreur	PERCEPTION	351,016	291	1,206			
	RESIGNATION	484,029	291	1,663			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

Les résultats du tableau des tests des effets intersujets démontrent que la variable indépendante a des effets globaux statistiquement significatifs sur les variables dépendantes avec un coefficient de signification égal à 0.004. Par la suite, les covariables région, genre et âge n'ont pas d'effet sur les variables dépendantes de vulnérabilité avec des coefficients de signification supérieurs à 0.50.

Au regard de l'interprétation des résultats obtenus, nous pouvons conclure que le type de bannière de publicité a un effet significatif sur la vulnérabilité des consommateurs québécois. Toutefois, ces analyses ne nous permettent pas de garantir des différences significatives entre les bannières de sécurité. De ce fait nous allons établir une analyse des moyennes des variables ainsi qu'une analyse Post hoc pour mieux comprendre ces différences.

Au vu du tableau présenté des moyennes des variables, les variables Attitude, Utilité, Clarté, Pertinence et Résignation sont plus pertinentes selon les répondants de notre étude que les autres échelles de mesure tout type de bannière de sécurité confondu. La variable utilité est celle qui obtient la plus haute moyenne, suivie de la variable clarté et de la variable Attitude. La variable Perception est celle qui est jugée la moins pertinente selon le calcul des moyennes et avant elle la variable Utilisation à long terme.

Tableau 4-9 : Moyenne des variables

Récapitulatif des observations

Goal		ATTITUDE	UTILITÉ	CLARTÉ	PERTINENCE	CONSENTEMENT	PERCEPTION	RESIGNATION	FacilitéUsage	ConfianceFintech	EfficacitéLoi25	Transparence Fintech
Acc. avec politique	N	50	50	50	50	50	50	50	50	50	50	50
	Moyenne	4,5400	4,7933	4,5267	4,2667	3,9450	3,5600	4,6133	4,4733	4,1700	4,6400	3,7100
	Ecart type	1,54581	1,22500	1,39010	1,68359	1,40815	1,08628	1,20911	1,33008	1,81156	1,13407	1,46416
Acc. ou paramétrer	N	50	50	50	50	50	50	50	50	50	50	50
	Moyenne	4,7000	4,4933	4,2800	4,5800	3,6550	3,8750	4,0400	4,4733	4,4000	4,3200	3,7800
	Ecart type	1,53604	1,24766	,95324	,95668	1,15826	,76474	,99805	1,20673	1,31320	1,45602	1,49884
Accepter tout	N	50	50	50	50	50	50	50	50	50	50	50
	Moyenne	4,9133	5,1600	4,9467	4,8267	4,6700	4,2650	4,8133	4,4000	4,0200	4,5600	3,8200
	Ecart type	1,53243	1,11319	1,39867	1,17849	1,43342	1,28711	1,17255	1,29012	1,80972	1,37262	1,80916
Cons. éclairé	N	50	50	50	50	50	50	50	50	50	50	50
	Moyenne	4,4533	4,8400	4,8000	4,5333	4,2500	3,8100	4,0533	4,3800	4,6600	4,6300	4,0400
	Ecart type	1,43136	1,54925	1,46617	1,46152	1,42678	1,14905	1,46827	1,35528	1,53011	1,32021	1,31258
Cookies essentiels	N	50	50	50	50	50	50	50	50	50	50	50
	Moyenne	4,3800	4,8333	4,6133	4,4667	4,3400	4,1450	4,7000	4,2600	4,0900	4,3900	3,9900
	Ecart type	1,41102	1,32352	1,24423	1,22336	1,58336	1,22900	1,26751	1,28534	1,39493	1,16185	1,48973
Sans bannière	N	50	50	50	50	50	50	50	50	50	50	50
	Moyenne	4,2467	3,9200	4,0733	3,9933	3,8900	3,5600	4,2067	4,4733	4,5200	4,6100	4,3000
	Ecart type	1,76873	1,61843	1,66093	1,41018	1,49161	,98400	1,53551	1,30600	1,57778	1,18791	1,19523
Total	N	300	300	300	300	300	300	300	300	300	300	300
	Moyenne	4,5389	4,6733	4,5400	4,4444	4,1250	3,8692	4,4044	4,4100	4,3100	4,5250	3,9400
	Ecart type	1,54445	1,40179	1,38992	1,35334	1,44990	1,12017	1,31542	1,28784	1,58818	1,27303	1,47490

Source : créé par l'auteur.

Dans le but de simplifier l'interprétation des résultats de l'analyse Post hoc réalisée, nous avons regroupé les valeurs qui avaient une différence significative. L'annexe D présente en détail tous les résultats obtenus.

Les résultats obtenus révèlent que les bannières qui autorisent un consentement éclairé de l'utilisateur ou une configuration personnalisée diminuent considérablement le sentiment de résignation et de perception de vulnérabilité comparativement aux bannières les plus strictes telles que les bannières Tout ou accepter ou encore les bannières accepter avec politique de confidentialité. On note une différence significative entre les autres types de paramètres de

protection de donnée et la bannière consentement éclairé. Aussi, les entreprises qui ne présentent pas d'option de paramétrage des données sont celles qui produisent des niveaux supérieurs d'insécurité et de résignation.

Tableau 4-10 : Résultats Post hoc

Comparaison des bannières de sécurité	**P-Value (résignation)**	**Significatif**	**P-Value (perception)**	**Significatif**
Acc. avec politique Vs Cons. éclairé	<.001	✅	<.001	✅
Acc. ou paramétrer Vs Cons. éclairé	<.001	✅	<.001	✅
Acc. Tout Vs Cons. éclairé	<.001	✅	<.001	✅
Sans bannière Vs Acc. Avec politique	<.001	✅	<.001	✅
Cons. Eclairé Vs cookies essentiels	<.001	✅	<.001	✅
Accepter tout Vs Sans bannière	.285	❌	.004	✅

Source : créé par l'auteur

4.5.2 **Hypothèse 2 :** Plus la connaissance de la Loi 25 est grande, plus faible est le sentiment d'insécurité des utilisateurs face à l'utilisation de leurs informations personnelles en ligne.

Le but de cette partie est de confirmer ou d'infirmer l'hypothèse H2 en examinant le lien entre le dégré de connaissance de la Loi 25 de ma population d'étude et leur sentiment d'insécurité quant à l'utilisation de leurs données privées sur les plateformes numériques.

Le test de Box est le plus utilisé pour définir si les matrices de covariance des différents groupes de l'analyse MANCOVA sont constantes ou pas. Il est semblable à une homogénéité de variance multivariée. Selon ce test, l'hypothèse nulle H0 teste l'égalité des matrices de covariance donc elle vérifie de ce fait si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig $\geq$ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig $\leq$ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, ce test est égal à <0.001 donc c'est inférieur à la P value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-11: Test d'égalité des matrices de covariance H2

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	119,331
F	3,431
df1	33
df2	18643,401
Sig.	<,001

Source : créé par l'auteur

Étant donné que l'hypothèse d'égalité des matrices de covariance n'a pas été respectée, nous allons utiliser les résultats de la statistique de Pillai's Trace qui est plus robuste que les trois autres

statistiques (Lambda de Wilks, la trace de Hotelling et la plus grande racine de Roy) lorsque nous sommes en présence d'une violation de l'hypothèse d'égalité des matrices de covariance.

Tableau 4-12 : Tests multivariés H2

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,381	87,015[b]	2,000	283,000	<,001	,381
	Lambda de Wilks	,619	87,015[b]	2,000	283,000	<,001	,381
	Trace de Hotelling	,615	87,015[b]	2,000	283,000	<,001	,381
	Plus grande racine de Roy	,615	87,015[b]	2,000	283,000	<,001	,381
Genre	Trace de Pillai	,013	1,861[b]	2,000	283,000	,157	,013
	Lambda de Wilks	,987	1,861[b]	2,000	283,000	,157	,013
	Trace de Hotelling	,013	1,861[b]	2,000	283,000	,157	,013
	Plus grande racine de Roy	,013	1,861[b]	2,000	283,000	,157	,013
R_gion	Trace de Pillai	,002	,241[b]	2,000	283,000	,786	,002
	Lambda de Wilks	,998	,241[b]	2,000	283,000	,786	,002
	Trace de Hotelling	,002	,241[b]	2,000	283,000	,786	,002
	Plus grande racine de Roy	,002	,241[b]	2,000	283,000	,786	,002
A_ge	Trace de Pillai	,003	,408[b]	2,000	283,000	,665	,003
	Lambda de Wilks	,997	,408[b]	2,000	283,000	,665	,003
	Trace de Hotelling	,003	,408[b]	2,000	283,000	,665	,003
	Plus grande racine de Roy	,003	,408[b]	2,000	283,000	,665	,003
Loi_25	Trace de Pillai	,023	3,323[b]	2,000	283,000	,037	,023
	Lambda de Wilks	,977	3,323[b]	2,000	283,000	,037	,023
	Trace de Hotelling	,023	3,323[b]	2,000	283,000	,037	,023
	Plus grande racine de Roy	,023	3,323[b]	2,000	283,000	,037	,023
Mesure_taux_d_info_1	Trace de Pillai	,165	4,268	12,000	568,000	<,001	,083
	Lambda de Wilks	,840	4,294[b]	12,000	566,000	<,001	,083
	Trace de Hotelling	,184	4,319	12,000	564,000	<,001	,084
	Plus grande racine de Roy	,135	6,398[c]	6,000	284,000	<,001	,119
Loi_25 * Mesure_taux_d_info_1	Trace de Pillai	,010	,274	10,000	568,000	,987	,005
	Lambda de Wilks	,990	,273[b]	10,000	566,000	,987	,005
	Trace de Hotelling	,010	,272	10,000	564,000	,987	,005
	Plus grande racine de Roy	,005	,308[c]	5,000	284,000	,908	,005

Cette statistique est à valeur positive, ce qui signifie que ses valeurs croissantes définissent des impacts qui contribuent davantage au modèle (Olson C, 1974). Elle permet également de

mesurer l'hypothèse nulle H0 qui teste l'existence d'une relation entre la variable indépendante et une ou plus variables dépendantes. Si P-Value ≤ 0.05, on doit rejeter l'hypothèse 0 donc la variable dépendante a une interaction avec la variable indépendante.

Les variables indépendantes Mesure du taux d'info et Loi 25 ont respectivement des résultats du Trace de Pillai (distribution F) égaux à 4,268 et 3.323 et des Sig égaux à $< .001$ et 0.037 par conséquent inférieur à la P-value ≤ 0.05. Ces résultats indiquent que ces variables ont un effet moyen sur les variables dépendantes, résignation et perception psychologique et elles influencent significativement ces variables. Toutefois, l'effet d'interaction qu'ils produisent ne contribue pas dans le modèle, car il a une valeur très faible de sa distribution F = .274 et un Sig = .987. Il en est de même pour les covariables âge, genre et région qui n'ont pas d'effet significatif sur les variables perception et résignation, car elles ont des résultats du coefficient de signification supérieur au P-Value (0.05) égaux respectivement à 0,665; 0,157 et 0.786 accompagnés des valeurs F de 0,408; 1,861 et 0.241.

C'est le tableau des tests des effets intersujets qui renferment la réponse à notre hypothèse de recherche. Le tableau suivant présente les résultats des tests des effets des variables de contrôle âge et genre et les variables indépendantes mesure du taux d'info et loi 25 une fois les les effets de l'âge et du genre contrôlés.

Tableau 4-13: Tests des effets intersujets H2

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	53,035[a]	15	3,536	3,117	<,001	,141
	RESIGNATION	53,482[b]	15	3,565	2,183	,007	,103
Constante	PERCEPTION	176,767	1	176,767	155,837	<,001	,354
	RESIGNATION	179,535	1	179,535	109,914	<,001	,279
Genre	PERCEPTION	,397	1	,397	,350	,555	,001
	RESIGNATION	5,664	1	5,664	3,467	,064	,012
R_gion	PERCEPTION	,522	1	,522	,461	,498	,002
	RESIGNATION	,099	1	,099	,060	,806	,000
A_ge	PERCEPTION	,023	1	,023	,020	,888	,000
	RESIGNATION	,731	1	,731	,448	,504	,002
Loi_25	PERCEPTION	7,446	1	7,446	6,564	,011	,023
	RESIGNATION	4,604	1	4,604	2,819	,094	,010
Mesure_taux_d_info_1	PERCEPTION	42,397	6	7,066	6,230	<,001	,116
	RESIGNATION	42,657	6	7,109	4,353	<,001	,084
Loi_25 * Mesure_taux_d_info_1	PERCEPTION	1,693	5	,339	,298	,913	,005
	RESIGNATION	1,984	5	,397	,243	,943	,004
Erreur	PERCEPTION	322,143	284	1,134			
	RESIGNATION	463,890	284	1,633			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

Dans un premier temps nous constatons que les covariables âge, genre et région n'ont pas d'effet significatif sur la perception de vulnérabilité des consommateurs, car elles ont des valeurs de signification supérieures au P-value 0.05 sur les variables dépendantes (0,498; 0,806; 0.888; 0.504; 0,554; et 0,064). Nous pouvons dire que l'âge. La région et le genre n'influencent pas significativement la vulnérabilité des utilisateurs québécois.

Une fois ces trois variables contrôlées, le tableau révèle un impact significatif de la variable mesure taux d'info sur les variables dépendantes perception et résignation ($sig = < .001$) et un effet statistiquement prouvé de la variable Loi 25 sur la variable dépendante perception (sig = 0.011), mais pas sur la variable résignation (sig = 0.094).

Au vu des différentes analyses interprétées, nous pouvons conclure que la connaissance de la Loi 25 a effectivement un impact significatif sur la perception de vulnérabilité des consommateurs québécois en ligne. De ce fait, l'hypothèse 2 est confirmée.

4.5.3 **Hypothèse 3 :** L'adoption des mesures de protection des données a un effet positif sur la réduction du sentiment de vulnérabilité par les utilisateurs dans le secteur de la Fintech.

L'hypothèse 3 nous permet d'examiner si l'adoption des mesures de protection des données par les entreprises de technologie financière est liée à une réduction du sentiment de vulnérabilité des utilisateurs.

Nous testons l'égalité des matrices de covariance donc le test de Box vérifie de ce fait si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig ≥ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig ≤ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, il est égal à < 0.001 donc c'est inférieur à la P value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-14: Test d'égalité des matrices de covariance H3

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	214,414
F	3,052
df1	63
df2	8122,632
Sig.	<,001

Source : créé par l'auteur

D’après les résultats obtenus, l’hypothèse d’égalité des matrices de covariance n’a pas été respectée. Nous allons de ce fait utiliser les résultats de la statistique de Pillai’s Trace qui est plus robuste que les trois autres statistiques lorsque nous sommes en présence d’une violation de l’hypothèse d’égalité des matrices de covariance.

Tableau 4-15: Tests multivariés H3

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,121	13,583[b]	2,000	197,000	<,001	,121
	Lambda de Wilks	,879	13,583[b]	2,000	197,000	<,001	,121
	Trace de Hotelling	,138	13,583[b]	2,000	197,000	<,001	,121
	Plus grande racine de Roy	,138	13,583[b]	2,000	197,000	<,001	,121
CONSENTEMENT	Trace de Pillai	,234	1,873	28,000	396,000	,005	,117
	Lambda de Wilks	,779	1,868[b]	28,000	394,000	,005	,117
	Trace de Hotelling	,266	1,864	28,000	392,000	,006	,117
	Plus grande racine de Roy	,161	2,273[c]	14,000	198,000	,007	,138
Genre	Trace de Pillai	,001	,136[b]	2,000	197,000	,873	,001
	Lambda de Wilks	,999	,136[b]	2,000	197,000	,873	,001
	Trace de Hotelling	,001	,136[b]	2,000	197,000	,873	,001
	Plus grande racine de Roy	,001	,136[b]	2,000	197,000	,873	,001
R_gion	Trace de Pillai	,032	3,290[b]	2,000	197,000	,039	,032
	Lambda de Wilks	,968	3,290[b]	2,000	197,000	,039	,032
	Trace de Hotelling	,033	3,290[b]	2,000	197,000	,039	,032
	Plus grande racine de Roy	,033	3,290[b]	2,000	197,000	,039	,032
A_ge	Trace de Pillai	,003	,249[b]	2,000	197,000	,780	,003
	Lambda de Wilks	,997	,249[b]	2,000	197,000	,780	,003
	Trace de Hotelling	,003	,249[b]	2,000	197,000	,780	,003
	Plus grande racine de Roy	,003	,249[b]	2,000	197,000	,780	,003
CONSENTEMENT * Genre	Trace de Pillai	,216	1,597	30,000	396,000	,026	,108
	Lambda de Wilks	,795	1,594[b]	30,000	394,000	,026	,108
	Trace de Hotelling	,244	1,592	30,000	392,000	,027	,109
	Plus grande racine de Roy	,153	2,015[c]	15,000	198,000	,016	,132
CONSENTEMENT * R_gion	Trace de Pillai	,327	2,767	28,000	396,000	<,001	,164
	Lambda de Wilks	,697	2,786[b]	28,000	394,000	<,001	,165
	Trace de Hotelling	,401	2,806	28,000	392,000	<,001	,167
	Plus grande racine de Roy	,276	3,906[c]	14,000	198,000	<,001	,216
CONSENTEMENT * A_ge	Trace de Pillai	,241	1,809	30,000	396,000	,007	,121
	Lambda de Wilks	,772	1,814[b]	30,000	394,000	,006	,121
	Trace de Hotelling	,278	1,818	30,000	392,000	,006	,122
	Plus grande racine de Roy	,188	2,486[c]	15,000	198,000	,002	,158
CONSENTEMENT * Genre * R_gion * A_ge	Trace de Pillai	,212	1,468	32,000	396,000	,051	,106
	Lambda de Wilks	,797	1,479[b]	32,000	394,000	,048	,107
	Trace de Hotelling	,243	1,490	32,000	392,000	,045	,108
	Plus grande racine de Roy	,179	2,218[c]	16,000	198,000	,006	,152

Comme précisé dans le paragraphe de l'analyse sur l'hypothèse 1, la statistique du Tracé de Pillai permet de mesurer l'hypothèse nulle H0 qui teste l'existence d'une relation entre la variable

indépendante et une ou plus variables dépendantes. Si P-Value ≤ 0.05, on doit rejeter l'hypothèse 0 donc la variable dépendante affecte la variable indépendante.

La variable indépendante consentement a comme résultats du Trace de Pillai la distribution F égal à 1,873 et un coefficient de signification égal à $.005$ par conséquent inférieur à la P-value ≤ 0.05. Ces résultats indiquent que cette variable a un impact significatif sur la résignation et la perception psychologique et elle influence significativement ces variables. De même, la variable région ainsi que les effets d'interaction consentement – âge, consentement – genre et consentement – région ont des coefficients de signification inférieurs ou égales à 0.05 donc ils ont également un effet significatif sur les variables dépendantes.

Toutefois, la variable genre et l'effet d'interaction consentement - genre – région – âge qu'il produit ne contribuent pas dans le modèle, car ils ont des coefficients Sig respectifs de 0.873 et 0.051. Le tableau des tests des effets intersujets nous permet de donner une réponse à notre question de recherche.

Tableau 4-16: Tests des effets intersujets H3

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	248,760[a]	101	2,463	3,858	<,001	,663
	RESIGNATION	321,754[b]	101	3,186	3,224	<,001	,622
Constante	PERCEPTION	15,597	1	15,597	24,429	<,001	,110
	RESIGNATION	13,847	1	13,847	14,015	<,001	,066
CONSENTEMENT	PERCEPTION	20,071	14	1,434	2,245	,008	,137
	RESIGNATION	24,659	14	1,761	1,783	,043	,112
Genre	PERCEPTION	,169	1	,169	,265	,607	,001
	RESIGNATION	,023	1	,023	,023	,879	,000
R_gion	PERCEPTION	3,855	1	3,855	6,037	,015	,030
	RESIGNATION	3,151	1	3,151	3,190	,076	,016
A_ge	PERCEPTION	,248	1	,248	,389	,534	,002
	RESIGNATION	,332	1	,332	,336	,563	,002
CONSENTEMENT * Genre	PERCEPTION	19,182	15	1,279	2,003	,017	,132
	RESIGNATION	19,173	15	1,278	1,294	,209	,089
CONSENTEMENT * R_gion	PERCEPTION	34,609	14	2,472	3,872	<,001	,215
	RESIGNATION	33,680	14	2,406	2,435	,004	,147
CONSENTEMENT * A_ge	PERCEPTION	22,696	15	1,513	2,370	,004	,152
	RESIGNATION	26,960	15	1,797	1,819	,034	,121
CONSENTEMENT * Genre * R_gion * A_ge	PERCEPTION	22,651	16	1,416	2,217	,006	,152
	RESIGNATION	17,463	16	1,091	1,105	,353	,082
Erreur	PERCEPTION	126,417	198	,638			
	RESIGNATION	195,618	198	,988			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

Les résultats du tableau des tests des effets intersujets démontrent que la variable région et les interactions consentement – genre et consentement – âge - genre ont des effets significatifs partiels, car elles ont un impact sur la variable dépendante perception, mais pas sur celle de la résignation. Par la suite, les variables genre et âge n'ont pas d'effet sur les variables dépendantes de vulnérabilité avec des coefficients de signification supérieurs à 0.50. Néanmoins, la variable indépendante principale consentement et les interactions consentement – âge et consentement - région ont des valeurs de signification inférieures au P-value 0.05 sur les variables dépendantes (0,008 et 0,043; 0.0014 et 0.034; <0.001 et 0.004). Nous pouvons dire que ces variables ont un effet global sur la vulnérabilité des utilisateurs québécois.

Au regard de l'interprétation des résultats obtenus, nous pouvons conclure que l'adoption des mesures de protection au travers de la variable Consentement a effectivement un effet significatif sur la réduction du sentiment de vulnérabilité des consommateurs québécois en ligne. De ce fait,

l'hypothèse 3 est confirmée. Aussi, son association avec les covariables âge et région sont toutes aussi déterminantes pour réduire le sentiment de la vulnérabilité des consommateurs.

4.5.4 **Hypothèse 4 :** La transparence dans les modes de collecte et d'utilisation des données des entreprises de Fintech réduit favorablement la perception de la vulnérabilité des consommateurs.

Cette section explore l'hypothèse 4 en considérant l'influence de la transparence perçue dans les méthodes de collecte et d'exploitation des informations sur la perception de la vulnérabilité des consommateurs.

Comme dans les hypothèses 1 et 2, nous débutons notre analyse par le test de l'égalité des matrices de covariance, le test de Box qui vérifie si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig ≥ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig ≤ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, l est égale à <0.001 donc c'est inférieur à la P value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-17: Test d'égalité des matrices de covariance H4

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	52,448
F	2,460
df1	15
df2	1022,443
Sig.	,002

Source : créé par l'auteur

D’après les résultats obtenus, l’hypothèse d’égalité des matrices de covariance n’a pas été respectée, car la valeur du coefficient de signification est de 0.002. Nous allons de ce fait utiliser les résultats de la statistique de Pillai’s Trace qui est plus robuste que les trois autres statistiques lorsque nous sommes en présence d’une violation de l’hypothèse d’égalité des matrices de covariance.

Tableau 4-18: Tests multivariés H4

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,485	56,986[b]	2,000	121,000	<,001	,485
	Lambda de Wilks	,515	56,986[b]	2,000	121,000	<,001	,485
	Trace de Hotelling	,942	56,986[b]	2,000	121,000	<,001	,485
	Plus grande racine de Roy	,942	56,986[b]	2,000	121,000	<,001	,485
Genre	Trace de Pillai	,022	1,379[b]	2,000	121,000	,256	,022
	Lambda de Wilks	,978	1,379[b]	2,000	121,000	,256	,022
	Trace de Hotelling	,023	1,379[b]	2,000	121,000	,256	,022
	Plus grande racine de Roy	,023	1,379[b]	2,000	121,000	,256	,022
R_gion	Trace de Pillai	,001	,075[b]	2,000	121,000	,928	,001
	Lambda de Wilks	,999	,075[b]	2,000	121,000	,928	,001
	Trace de Hotelling	,001	,075[b]	2,000	121,000	,928	,001
	Plus grande racine de Roy	,001	,075[b]	2,000	121,000	,928	,001
A_ge	Trace de Pillai	,006	,389[b]	2,000	121,000	,679	,006
	Lambda de Wilks	,994	,389[b]	2,000	121,000	,679	,006
	Trace de Hotelling	,006	,389[b]	2,000	121,000	,679	,006
	Plus grande racine de Roy	,006	,389[b]	2,000	121,000	,679	,006
CLARTÉ	Trace de Pillai	,477	2,386	32,000	244,000	<,001	,238
	Lambda de Wilks	,565	2,495[b]	32,000	242,000	<,001	,248
	Trace de Hotelling	,695	2,605	32,000	240,000	<,001	,258
	Plus grande racine de Roy	,563	4,291[c]	16,000	122,000	<,001	,360
PERTINENCE	Trace de Pillai	,490	2,472	32,000	244,000	<,001	,245
	Lambda de Wilks	,567	2,480[b]	32,000	242,000	<,001	,247
	Trace de Hotelling	,663	2,488	32,000	240,000	<,001	,249
	Plus grande racine de Roy	,431	3,289[c]	16,000	122,000	<,001	,301
TransparenceFintech	Trace de Pillai	,736	5,924	24,000	244,000	<,001	,368
	Lambda de Wilks	,398	5,903[b]	24,000	242,000	<,001	,369
	Trace de Hotelling	1,176	5,881	24,000	240,000	<,001	,370
	Plus grande racine de Roy	,680	6,918[c]	12,000	122,000	<,001	,405
CLARTÉ * PERTINENCE	Trace de Pillai	,687	3,191	40,000	244,000	<,001	,343
	Lambda de Wilks	,410	3,403[b]	40,000	242,000	<,001	,360
	Trace de Hotelling	1,205	3,616	40,000	240,000	<,001	,376
	Plus grande racine de Roy	,960	5,855[c]	20,000	122,000	<,001	,490
CLARTÉ * TransparenceFintech	Trace de Pillai	,587	3,619	28,000	244,000	<,001	,293
	Lambda de Wilks	,489	3,711[b]	28,000	242,000	<,001	,300
	Trace de Hotelling	,887	3,803	28,000	240,000	<,001	,307
	Plus grande racine de Roy	,646	5,633[c]	14,000	122,000	<,001	,393
PERTINENCE * TransparenceFintech	Trace de Pillai	,582	2,501	40,000	244,000	<,001	,291
	Lambda de Wilks	,503	2,482[b]	40,000	242,000	<,001	,291
	Trace de Hotelling	,821	2,463	40,000	240,000	<,001	,291
	Plus grande racine de Roy	,436	2,661[c]	20,000	122,000	<,001	,304
CLARTÉ * PERTINENCE * TransparenceFintech	Trace de Pillai	,002	,133[b]	2,000	121,000	,876	,002
	Lambda de Wilks	,998	,133[b]	2,000	121,000	,876	,002
	Trace de Hotelling	,002	,133[b]	2,000	121,000	,876	,002
	Plus grande racine de Roy	,002	,133[b]	2,000	121,000	,876	,002

Sans grande surprise, les résultats révèlent qu'il n'y a pas d'effets entre les covariables âge, région et genre et la réduction du sentiment de vulnérabilité étant donné que leurs coefficients de

signification sont supérieurs à 0.05. Ce qui signifie que peu importe l'âge, le genre et la région d'habitation des utilisateurs québécois, ils auront des réactions comparables face au sentiment de vulnérabilité. Il en est de même pour l'interaction transparence fintech - clarté - pertinence.

Par contre, les variables transparence fintech, clarté, pertinence et les interactions transparence fintech – clarté, transparence fintech – pertinence et clarté – pertinence ont toutes des coefficients de signification égaux à <0.001. Ce qui traduit un effet significatif de ces variables indépendantes sur les variables dépendantes, pertinence et résignation.

Pour terminer, les résultats des tests des effets intersujets sont similaires aux résultats des tests multivariés effectués précédemment, en dehors de la variable clarté qui présente des résultats différents avec des variables de signification supérieures à 0.05. Les covariables âge et genre et l'interaction transparence fintech - clarté – pertinence présentent des valeurs supérieures au P-value

Tableau 4-19: Test des effets intersujets H4

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	335,288[a]	177	1,894	5,794	<,001	,894
	RESIGNATION	442,897[b]	177	2,502	4,099	<,001	,856
Constante	PERCEPTION	34,113	1	34,113	104,335	<,001	,461
	RESIGNATION	54,015	1	54,015	88,484	<,001	,420
Genre	PERCEPTION	,102	1	,102	,311	,578	,003
	RESIGNATION	1,413	1	1,413	2,315	,131	,019
R_gion	PERCEPTION	,046	1	,046	,139	,710	,001
	RESIGNATION	,019	1	,019	,032	,859	,000
A_ge	PERCEPTION	,184	1	,184	,562	,455	,005
	RESIGNATION	,450	1	,450	,737	,392	,006
CLARTÉ	PERCEPTION	7,722	16	,483	1,476	,119	,162
	RESIGNATION	15,165	16	,948	1,553	,092	,169
PERTINENCE	PERCEPTION	16,082	16	1,005	3,074	<,001	,287
	RESIGNATION	19,291	16	1,206	1,975	,020	,206
TransparenceFintech	PERCEPTION	24,409	12	2,034	6,221	<,001	,380
	RESIGNATION	50,356	12	4,196	6,874	<,001	,403
CLARTÉ * PERTINENCE	PERCEPTION	10,777	20	,539	1,648	,052	,213
	RESIGNATION	36,341	20	1,817	2,977	<,001	,328
CLARTÉ * TransparenceFintech	PERCEPTION	9,760	14	,697	2,132	,014	,197
	RESIGNATION	30,895	14	2,207	3,615	<,001	,293
PERTINENCE * TransparenceFintech	PERCEPTION	16,108	20	,805	2,463	,001	,288
	RESIGNATION	32,446	20	1,622	2,658	<,001	,303
CLARTÉ * PERTINENCE * TransparenceFintech	PERCEPTION	,064	1	,064	,197	,658	,002
	RESIGNATION	,152	1	,152	,249	,619	,002
Erreur	PERCEPTION	39,889	122	,327			
	RESIGNATION	74,475	122	,610			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

Au vu des résultats des tests des effets intersujets qui sont similaires aux résultats des tests multivariés, on peut conclure que l'hypothèse selon laquelle la transparence dans les modes de collecte et d'utilisation des données privées des entreprises de Fintech réduit favorablement la perception de la vulnérabilité des consommateurs est vérifiée, car les résultats prouvent que les variables indépendantes ont un effet direct sur les variables de vulnérabilité. Toutefois, il est vrai que la variable clarté des paramètres de sécurité influence la vulnérabilité (effet significatif aux

tests multivariés), mais l'effet spécifique n'est pas clair puis que nous avons obtenu des valeurs de signification élevées au P-value aux tests des effets intersujets.

4.5.5 **Hypothèse 5 :** L'utilité perçue des paramètres de sécurité a un effet positif sur la réduction du sentiment de vulnérabilité sur les plateformes de technologies financières.

Cette partie teste dans quelle proportion l'utilité perçue des paramètres de sécurité contribue à diminuer le sentiment de vulnérabilité sur les plateformes de technologies financières.

Pour rappel, le test de Box vérifie si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig ≥ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig ≤ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, l est égale à <0.001 donc c'est inférieur à la P value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-20: Test d'égalité des matrices de covariance H5

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	204,109
F	2,311
df1	69
df2	3372,004
Sig.	<,001

D'après le tableau précédent, le coefficient de signification pour le test de Box est de <,001 ce qui signifie que l'hypothèse d'égalité des matrices de covariance n'a pas été respectée. Nous allons de ce fait utiliser les résultats de la statistique de Pillai's Trace qui est plus robuste que les

trois autres statistiques lorsque nous sommes en présence d'une violation de l'hypothèse d'égalité des matrices de covariance.

Tableau 4-21: Tests multivariés H5

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,151	7,997[b]	2,000	90,000	<,001	,151
	Lambda de Wilks	,849	7,997[b]	2,000	90,000	<,001	,151
	Trace de Hotelling	,178	7,997[b]	2,000	90,000	<,001	,151
	Plus grande racine de Roy	,178	7,997[b]	2,000	90,000	<,001	,151
ATTITUDE	Trace de Pillai	,351	3,225	12,000	182,000	<,001	,175
	Lambda de Wilks	,678	3,213[b]	12,000	180,000	<,001	,176
	Trace de Hotelling	,431	3,200	12,000	178,000	<,001	,177
	Plus grande racine de Roy	,277	4,199[c]	6,000	91,000	<,001	,217
UTILITÉ	Trace de Pillai	,265	2,317	12,000	182,000	,009	,133
	Lambda de Wilks	,749	2,331[b]	12,000	180,000	,008	,135
	Trace de Hotelling	,316	2,344	12,000	178,000	,008	,136
	Plus grande racine de Roy	,236	3,578[c]	6,000	91,000	,003	,191
Genre	Trace de Pillai	,099	4,962[b]	2,000	90,000	,009	,099
	Lambda de Wilks	,901	4,962[b]	2,000	90,000	,009	,099
	Trace de Hotelling	,110	4,962[b]	2,000	90,000	,009	,099
	Plus grande racine de Roy	,110	4,962[b]	2,000	90,000	,009	,099
R_gion	Trace de Pillai	,039	1,815[b]	2,000	90,000	,169	,039
	Lambda de Wilks	,961	1,815[b]	2,000	90,000	,169	,039
	Trace de Hotelling	,040	1,815[b]	2,000	90,000	,169	,039
	Plus grande racine de Roy	,040	1,815[b]	2,000	90,000	,169	,039
A_ge	Trace de Pillai	,122	6,259[b]	2,000	90,000	,003	,122
	Lambda de Wilks	,878	6,259[b]	2,000	90,000	,003	,122
	Trace de Hotelling	,139	6,259[b]	2,000	90,000	,003	,122
	Plus grande racine de Roy	,139	6,259[b]	2,000	90,000	,003	,122
ATTITUDE * UTILITÉ	Trace de Pillai	,385	2,172	20,000	182,000	,004	,193
	Lambda de Wilks	,649	2,174[b]	20,000	180,000	,004	,195
	Trace de Hotelling	,489	2,176	20,000	178,000	,004	,196
	Plus grande racine de Roy	,329	2,998[c]	10,000	91,000	,003	,248
ATTITUDE * Genre	Trace de Pillai	,047	2,230[b]	2,000	90,000	,113	,047
	Lambda de Wilks	,953	2,230[b]	2,000	90,000	,113	,047
	Trace de Hotelling	,050	2,230[b]	2,000	90,000	,113	,047
	Plus grande racine de Roy	,050	2,230[b]	2,000	90,000	,113	,047
ATTITUDE * R_gion	Trace de Pillai	,170	2,813	6,000	182,000	,012	,085
	Lambda de Wilks	,834	2,855[b]	6,000	180,000	,011	,087
	Trace de Hotelling	,195	2,896	6,000	178,000	,010	,089
	Plus grande racine de Roy	,171	5,179[c]	3,000	91,000	,002	,146
ATTITUDE * A_ge	Trace de Pillai	,190	3,186	6,000	182,000	,005	,095
	Lambda de Wilks	,811	3,322[b]	6,000	180,000	,004	,100
	Trace de Hotelling	,233	3,456	6,000	178,000	,003	,104
	Plus grande racine de Roy	,230	6,963[c]	3,000	91,000	<,001	,187
UTILITÉ * Genre	Trace de Pillai	,225	2,889	8,000	182,000	,005	,113
	Lambda de Wilks	,785	2,897[b]	8,000	180,000	,005	,114
	Trace de Hotelling	,261	2,904	8,000	178,000	,005	,115
	Plus grande racine de Roy	,194	4,403[c]	4,000	91,000	,003	,162
UTILITÉ * R_gion	Trace de Pillai	,231	2,968	8,000	182,000	,004	,115
	Lambda de Wilks	,779	2,996[b]	8,000	180,000	,004	,118
	Trace de Hotelling	,272	3,024	8,000	178,000	,003	,120
	Plus grande racine de Roy	,215	4,882[c]	4,000	91,000	,001	,177
UTILITÉ * A_ge	Trace de Pillai	,151	1,857	8,000	182,000	,069	,075
	Lambda de Wilks	,853	1,866[b]	8,000	180,000	,068	,077
	Trace de Hotelling	,169	1,876	8,000	178,000	,066	,078
	Plus grande racine de Roy	,138	3,144[c]	4,000	91,000	,018	,121
ATTITUDE * UTILITÉ * Genre * R_gion * A_ge	Trace de Pillai	,863	2,302	60,000	182,000	<,001	,431
	Lambda de Wilks	,318	2,324[b]	60,000	180,000	<,001	,436
	Trace de Hotelling	1,581	2,345	60,000	178,000	<,001	,441
	Plus grande racine de Roy	1,028	3,119[c]	30,000	91,000	<,001	,507

Les résultats de cette analyse des variables indépendantes qui mesurent l'utilité des paramètres de sécurité, les covariables âge et genre ont un effet sur la vulnérabilité des consommateurs lorsque nous regardons les résultats des tests multivariés avec des coefficients de signification égaux à 0.003 et 0.009. Il n'y a que la covariable région qui n'a aucun effet significatif.

Par ailleurs, les variables indépendantes attitude et utilité et les interactions entre les variables attitude – utilité, attitude – région, attitude – âge, utilité – genre, utilité – région et attitude – utilité – genre – région – âge ont des valeurs de coefficients de signification tous inférieurs au P-value respectivement égaux à <0.001; 0.009; 0.004; 0.012; 0.005; 0.005; 0.004 et <0.001. Les interactions attitude – genre et attitude – région n'ont pas d'impact significatif sur les variables perception et résignation.

Pour pouvoir répondre à notre question de recherche, les tests des effets intersujets et leur interprétation sont réalisés dans les phrases qui suivent.

Tableau 4-22 : Tests des effets intersujets H5

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	329,002[a]	208	1,582	3,117	<,001	,877
	RESIGNATION	426,329[b]	208	2,050	2,049	<,001	,824
Constante	PERCEPTION	7,605	1	7,605	14,987	<,001	,141
	RESIGNATION	11,869	1	11,869	11,863	<,001	,115
ATTITUDE	PERCEPTION	9,008	6	1,501	2,959	,011	,163
	RESIGNATION	14,527	6	2,421	2,420	,032	,138
UTILITÉ	PERCEPTION	3,805	6	,634	1,250	,289	,076
	RESIGNATION	16,507	6	2,751	2,750	,017	,153
Genre	PERCEPTION	4,357	1	4,357	8,587	,004	,086
	RESIGNATION	8,318	1	8,318	8,314	,005	,084
R_gion	PERCEPTION	,232	1	,232	,458	,500	,005
	RESIGNATION	3,132	1	3,132	3,131	,080	,033
A_ge	PERCEPTION	2,374	1	2,374	4,679	,033	,049
	RESIGNATION	12,536	1	12,536	12,530	<,001	,121
ATTITUDE * UTILITÉ	PERCEPTION	7,893	10	,789	1,556	,133	,146
	RESIGNATION	18,807	10	1,881	1,880	,058	,171
ATTITUDE * Genre	PERCEPTION	,085	1	,085	,168	,683	,002
	RESIGNATION	1,533	1	1,533	1,532	,219	,017
ATTITUDE * R_gion	PERCEPTION	1,333	3	,444	,876	,457	,028
	RESIGNATION	7,011	3	2,337	2,336	,079	,072
ATTITUDE * A_ge	PERCEPTION	1,967	3	,656	1,292	,282	,041
	RESIGNATION	3,244	3	1,081	1,081	,361	,034
UTILITÉ * Genre	PERCEPTION	5,291	4	1,323	2,607	,041	,103
	RESIGNATION	17,512	4	4,378	4,376	,003	,161
UTILITÉ * R_gion	PERCEPTION	2,641	4	,660	1,301	,276	,054
	RESIGNATION	12,748	4	3,187	3,185	,017	,123
UTILITÉ * A_ge	PERCEPTION	2,642	4	,661	1,302	,275	,054
	RESIGNATION	12,063	4	3,016	3,014	,022	,117
ATTITUDE * UTILITÉ * Genre * R_gion * A_ge	PERCEPTION	32,459	30	1,082	2,132	,003	,413
	RESIGNATION	52,376	30	1,746	1,745	,023	,365
Erreur	PERCEPTION	46,175	91	,507			
	RESIGNATION	91,043	91	1,000			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

La covariable région et les variables d'interaction attitude – utilité, attitude – genre, attitude – région, attitude – âge, n'ont d'effet ni sur la variable perception et encore moins sur la variable résignation. Ensuite, nous avons la variable indépendante utilité et les variables d'interaction utilité - région, utilité – âge qui ont une influence partielle, car elles ont un impact sur la variable résignation, mais pas sur la variable perception. Il n'y a que les variables attitude, genre, âge et

l'interaction attitude – utilité – genre – âge qui ont un effet global significatif sur la vulnérabilité des consommateurs québécois.

Nous pouvons tirer comme conclusion que l'hypothèse selon laquelle l'utilité perçue des paramètres a un effet global positif sur la réduction du sentiment de vulnérabilité. Toutefois, l'utilité a un effet faible ou à cause du facteur perception.

4.5.6 **Hypothèse 6 :** Plus les paramètres de sécurité sont faciles d'utilisation, moins le consommateur en ligne se sent vulnérable sur les plateformes de technologies financières.

Ce volet se concentre sur l'analyse du lien entre la facilité d'utilisation des paramètres de sécurité et le sentiment de vulnérabilité perçu des utilisateurs sur les différentes plateformes financières.

Pour rappel, le test de Box vérifie si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig ≥ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig ≤ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, le coefficient de signification est égal à <0.001 donc c'est inférieur à la P-value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-23 : Test d'égalité des matrices de covariance H6

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	170,397
F	3,728
df1	42
df2	9220,431
Sig.	<,001

D'après le tableau précédent, le coefficient de signification pour le test de Box est de <,001 ce qui signifie que l'hypothèse d'égalité des matrices de covariance n'a pas été respectée. Nous allons de ce fait utiliser les résultats de la statistique de Pillai's Trace qui est plus robuste que les trois autres statistiques lorsque nous sommes en présence d'une violation de l'hypothèse d'égalité des matrices de covariance.

Tableau 4-24: Tests multivariés H6

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,367	80,172[b]	2,000	277,000	<,001	,367
	Lambda de Wilks	,633	80,172[b]	2,000	277,000	<,001	,367
	Trace de Hotelling	,579	80,172[b]	2,000	277,000	<,001	,367
	Plus grande racine de Roy	,579	80,172[b]	2,000	277,000	<,001	,367
Genre	Trace de Pillai	,008	1,121[b]	2,000	277,000	,328	,008
	Lambda de Wilks	,992	1,121[b]	2,000	277,000	,328	,008
	Trace de Hotelling	,008	1,121[b]	2,000	277,000	,328	,008
	Plus grande racine de Roy	,008	1,121[b]	2,000	277,000	,328	,008
R_gion	Trace de Pillai	,008	1,109[b]	2,000	277,000	,331	,008
	Lambda de Wilks	,992	1,109[b]	2,000	277,000	,331	,008
	Trace de Hotelling	,008	1,109[b]	2,000	277,000	,331	,008
	Plus grande racine de Roy	,008	1,109[b]	2,000	277,000	,331	,008
A_ge	Trace de Pillai	,001	,175[b]	2,000	277,000	,840	,001
	Lambda de Wilks	,999	,175[b]	2,000	277,000	,840	,001
	Trace de Hotelling	,001	,175[b]	2,000	277,000	,840	,001
	Plus grande racine de Roy	,001	,175[b]	2,000	277,000	,840	,001
FacilitéUsage	Trace de Pillai	,379	3,608	36,000	556,000	<,001	,189
	Lambda de Wilks	,657	3,604[b]	36,000	554,000	<,001	,190
	Trace de Hotelling	,469	3,599	36,000	552,000	<,001	,190
	Plus grande racine de Roy	,272	4,199[c]	18,000	278,000	<,001	,214

Le tableau des tests multivariés à travers l'analyse du tracé de Pillai permet de montrer que la variable indépendante facilité d'usage a un effet significatif sur la vulnérabilité des consommateurs, même si les covariables genre, région et âge n'ont d'effet.

Analysons ensemble le tableau des tests des effets intersujets pour pouvoir répondre à notre hypothèse de recherche.

Tableau 4-25: Tests des effets intersujets H6

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	77,523[a]	21	3,692	3,448	<,001	,207
	RESIGNATION	89,117[b]	21	4,244	2,755	<,001	,172
Constante	PERCEPTION	154,092	1	154,092	143,918	<,001	,341
	RESIGNATION	165,280	1	165,280	107,291	<,001	,278
Genre	PERCEPTION	,315	1	,315	,295	,588	,001
	RESIGNATION	1,029	1	1,029	,668	,415	,002
R_gion	PERCEPTION	1,848	1	1,848	1,726	,190	,006
	RESIGNATION	,058	1	,058	,038	,846	,000
A_ge	PERCEPTION	,345	1	,345	,322	,571	,001
	RESIGNATION	,339	1	,339	,220	,640	,001
FacilitéUsage	PERCEPTION	75,112	18	4,173	3,897	<,001	,201
	RESIGNATION	84,870	18	4,715	3,061	<,001	,165
Erreur	PERCEPTION	297,654	278	1,071			
	RESIGNATION	428,255	278	1,540			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

Les résultats démontrent que la facilité d'usage a un impact statistiquement significatif sur la vulnérabilité des consommateurs québécois et cela nous permet de répondre positivement à notre question de recherche. Par conséquent, nous pouvons affirmer que plus les paramètres de sécurité sont faciles d'utilisation, moins le consommateur se sent vulnérable sur les plateformes de technologies financières.

4.5.7 **Hypothèse 7** : Plus l'utilisateur est convaincu de la performance des bannières de sécurité, plus faible sera son sentiment de vulnérabilité.

L'hypothèse 7 nous permet d'évaluer si la certitude des utilisateurs concernant l'efficacité des bannières de sécurité est liée à une atténuation de leur sentiment de vulnérabilité.

L'hypothèse nulle du test de Box vérifie si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig ≥ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig ≤ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, le coefficient de signification est égal à <0.001 donc c'est inférieur à la P-value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-26 : Test d'égalité des matrices de covariance H7

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	109,685
F	3,410
df1	30
df2	10465,084
Sig.	<,001

D'après les résultats obtenus, l'hypothèse d'égalité des matrices de covariance n'a pas été respectée, car la valeur du coefficient de signification est de < 0.001. Nous allons de ce fait utiliser les résultats de la statistique de Pillai's Trace qui est plus robuste que les trois autres statistiques lorsque nous sommes en présence d'une violation de l'hypothèse d'égalité des matrices de covariance.

Tableau 4-27: Tests multivariés H7

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,397	92,967[b]	2,000	283,000	<,001	,397
	Lambda de Wilks	,603	92,967[b]	2,000	283,000	<,001	,397
	Trace de Hotelling	,657	92,967[b]	2,000	283,000	<,001	,397
	Plus grande racine de Roy	,657	92,967[b]	2,000	283,000	<,001	,397
Genre	Trace de Pillai	,021	3,068[b]	2,000	283,000	,048	,021
	Lambda de Wilks	,979	3,068[b]	2,000	283,000	,048	,021
	Trace de Hotelling	,022	3,068[b]	2,000	283,000	,048	,021
	Plus grande racine de Roy	,022	3,068[b]	2,000	283,000	,048	,021
R_gion	Trace de Pillai	,004	,624[b]	2,000	283,000	,536	,004
	Lambda de Wilks	,996	,624[b]	2,000	283,000	,536	,004
	Trace de Hotelling	,004	,624[b]	2,000	283,000	,536	,004
	Plus grande racine de Roy	,004	,624[b]	2,000	283,000	,536	,004
A_ge	Trace de Pillai	,001	,096[b]	2,000	283,000	,909	,001
	Lambda de Wilks	,999	,096[b]	2,000	283,000	,909	,001
	Trace de Hotelling	,001	,096[b]	2,000	283,000	,909	,001
	Plus grande racine de Roy	,001	,096[b]	2,000	283,000	,909	,001
EfficacitéLoi25	Trace de Pillai	,219	2,910	24,000	568,000	<,001	,109
	Lambda de Wilks	,793	2,903[b]	24,000	566,000	<,001	,110
	Trace de Hotelling	,246	2,896	24,000	564,000	<,001	,110
	Plus grande racine de Roy	,140	3,318[c]	12,000	284,000	<,001	,123

Le tableau des tests multivariés à travers l'analyse du tracé de Pillai a permis de montrer que la variable indépendante Efficacité Loi 25 a un effet significatif avec un coefficient de signification égale à <.001 sur la vulnérabilité des consommateurs ainsi que la covariable genre qui a un coefficient de signification Sig = 0.048. Par ailleurs, les covariables région et âge n'ont d'impact sur les variables dépendantes.

Analysons ensemble le tableau des tests des effets intersujets pour pouvoir répondre à notre hypothèse de recherche.

Tableau 4-28 : Tests des effets intersujets H7

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	PERCEPTION	43,780[a]	15	2,919	2,501	,002	,117
	RESIGNATION	66,650[b]	15	4,443	2,800	<,001	,129
Constante	PERCEPTION	188,524	1	188,524	161,561	<,001	,363
	RESIGNATION	203,669	1	203,669	128,332	<,001	,311
Genre	PERCEPTION	,006	1	,006	,005	,942	,000
	RESIGNATION	6,360	1	6,360	4,008	,046	,014
R_gion	PERCEPTION	1,366	1	1,366	1,171	,280	,004
	RESIGNATION	1,146	1	1,146	,722	,396	,003
A_ge	PERCEPTION	,023	1	,023	,020	,888	,000
	RESIGNATION	,109	1	,109	,069	,793	,000
EfficacitéLoi25	PERCEPTION	41,368	12	3,447	2,954	<,001	,111
	RESIGNATION	62,403	12	5,200	3,277	<,001	,122
Erreur	PERCEPTION	331,398	284	1,167			
	RESIGNATION	450,722	284	1,587			
Total	PERCEPTION	4866,313	300				
	RESIGNATION	6337,111	300				
Total corrigé	PERCEPTION	375,177	299				
	RESIGNATION	517,372	299				

Les résultats démontrent que la variable efficacité de Loi 25 a un impact statistiquement significatif sur la vulnérabilité des consommateurs québécois et cela nous permet de répondre positivement à notre question de recherche. La covariable genre a un impact partiel sur la vulnérabilité des consommateurs (Sig = 0.046 pour la résignation et 0.942 pour la perception) et les covariables âge et région n'ont aucun effet.

Par conséquent, nous pouvons affirmer que plus l'utilisateur est convaincu de la performance des bannières de sécurité, faible est son sentiment de vulnérabilité sur les plateformes de technologies financières.

4.5.8 **Hypothèse 8 :** Le sentiment de vulnérabilité perçue par les consommateurs en ligne au Québec a un effet sur l'adoption des Fintechs conformes à la Loi 25.

Cette section a pour objectif d'étudier l'hypothèse 8 en examinant l'impact du sentiment de vulnérabilité perçue par les consommateurs Québécois sur leur volonté d'adoption des Fintech en conformité avec la Loi 25.

L'hypothèse nulle du test de Box vérifie si la matrice des covariances est constante à l'intérieur des groupes de la variable X.

- H0 : Sig ≥ 0.05, l'hypothèse d'égalité des matrices de covariance est validée.
- H1 : Sig ≤ 0.05, les matrices de covariance des groupes ne sont pas homogènes.

D'après le tableau suivant, le coefficient de signification est égal à <0.001 donc c'est inférieur à la P-value 0.05 donc nous rejetons l'hypothèse nulle d'égalité des matrices de covariances. Ce qui signifie qu'au moins deux de ces matrices ne sont pas égales.

Tableau 4-29: Test d'égalité des matrices de covariance H8

Test de Box de l'égalité des matrices de covariance[a]

Test de Box	226,707
F	1,870
df1	90
df2	3404,738
Sig.	<,001

D'après le tableau précédent, le coefficient de signification pour le test de Box est de <,001 ce qui signifie que l'hypothèse d'égalité des matrices de covariance n'a pas été respectée. Nous allons de ce fait utiliser les résultats de la statistique de Pillai's Trace qui est plus robuste que les trois autres statistiques lorsque nous sommes en présence d'une violation de l'hypothèse d'égalité des matrices de covariance.

Tableau 4-30: Tests multivariés H8

Tests multivariés[a]

Effet		Valeur	F	ddl de l'hypothèse	Erreur ddl	Sig.	Eta-carré partiel
Constante	Trace de Pillai	,557	78,664[b]	3,000	188,000	<,001	,557
	Lambda de Wilks	,443	78,664[b]	3,000	188,000	<,001	,557
	Trace de Hotelling	1,255	78,664[b]	3,000	188,000	<,001	,557
	Plus grande racine de Roy	1,255	78,664[b]	3,000	188,000	<,001	,557
A_ge	Trace de Pillai	,015	,985[b]	3,000	188,000	,401	,015
	Lambda de Wilks	,985	,985[b]	3,000	188,000	,401	,015
	Trace de Hotelling	,016	,985[b]	3,000	188,000	,401	,015
	Plus grande racine de Roy	,016	,985[b]	3,000	188,000	,401	,015
Genre	Trace de Pillai	,018	1,167[b]	3,000	188,000	,324	,018
	Lambda de Wilks	,982	1,167[b]	3,000	188,000	,324	,018
	Trace de Hotelling	,019	1,167[b]	3,000	188,000	,324	,018
	Plus grande racine de Roy	,019	1,167[b]	3,000	188,000	,324	,018
R_gion	Trace de Pillai	,048	3,180[b]	3,000	188,000	,025	,048
	Lambda de Wilks	,952	3,180[b]	3,000	188,000	,025	,048
	Trace de Hotelling	,051	3,180[b]	3,000	188,000	,025	,048
	Plus grande racine de Roy	,051	3,180[b]	3,000	188,000	,025	,048
PERCEPTION	Trace de Pillai	,669	2,724	60,000	570,000	<,001	,223
	Lambda de Wilks	,463	2,761	60,000	561,724	<,001	,227
	Trace de Hotelling	,898	2,794	60,000	560,000	<,001	,230
	Plus grande racine de Roy	,451	4,288[c]	20,000	190,000	<,001	,311
RESIGNATION	Trace de Pillai	,450	2,235	45,000	570,000	<,001	,150
	Lambda de Wilks	,606	2,285	45,000	559,281	<,001	,154
	Trace de Hotelling	,562	2,330	45,000	560,000	<,001	,158
	Plus grande racine de Roy	,315	3,996[c]	15,000	190,000	<,001	,240
PERCEPTION * RESIGNATION	Trace de Pillai	1,428	2,465	210,000	570,000	<,001	,476
	Lambda de Wilks	,141	2,483	210,000	564,697	<,001	,480
	Trace de Hotelling	2,814	2,502	210,000	560,000	<,001	,484
	Plus grande racine de Roy	1,287	3,494[c]	70,000	190,000	<,001	,563

Le tracé de Pillai est à valeur positive et il permet également de mesurer l'hypothèse nulle H0 qui teste l'existence d'une relation entre la variable indépendante et une ou plus variables dépendantes. Si P-Value ≤ 0.05, on doit rejeter l'hypothèse 0 donc la variable dépendante affecte la variable indépendante.

Les variables indépendantes perception et résignation et leur interaction perception - résignation ont respectivement des résultats du Tracé de Pillai (distribution F) égaux à 2,724; 2.235 et 2.465 et des Sig. tous égaux à $< .001$ par conséquent inférieur à la P-value ≤ 0.05. Ces résultats indiquent que ces variables ont un effet statistiquement significatif sur les variables dépendantes confiance et expérience et qu'elles influencent significativement ces variables.

S'agissant des covariables, la covariable région est celle qui a un impact statistiquement significatif sur l'adoption des plateformes de Fintech. Elle a un coefficient de signification égal à 0,025 et une distribution de . Par contre, les covariables genre et âge n'ont pas d'effet significatif sur les variables dépendantes, car elles ont des résultats du coefficient de signification supérieur au P-Value (0.05).

Grâce au tableau des tests des effets intersujets qui suit, nous pourrons répondre à notre hypothèse de recherche.

Tableau 4-31 : Tests des effets intersujets H8

Tests des effets intersujets

Source	Variable dépendante	Somme des carrés de Type III	df	Carré moyen	F	Sig.	Eta-carré partiel
Modèle corrigé	ConfianceFintech	519,445[a]	109	4,766	3,858	<,001	,689
	ExpériencePassée	468,063[b]	109	4,294	3,309	<,001	,655
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	209,360[c]	109	1,921	1,913	<,001	,523
Constante	ConfianceFintech	141,084	1	141,084	114,201	<,001	,375
	ExpériencePassée	102,891	1	102,891	79,282	<,001	,294
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	32,052	1	32,052	31,916	<,001	,144
A_ge	ConfianceFintech	,009	1	,009	,007	,933	,000
	ExpériencePassée	1,941	1	1,941	1,496	,223	,008
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	,881	1	,881	,877	,350	,005
Genre	ConfianceFintech	3,260	1	3,260	2,639	,106	,014
	ExpériencePassée	,362	1	,362	,279	,598	,001
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	,156	1	,156	,155	,694	,001
R_gion	ConfianceFintech	8,226	1	8,226	6,659	,011	,034
	ExpériencePassée	2,223	1	2,223	1,713	,192	,009
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	,452	1	,452	,450	,503	,002
PERCEPTION	ConfianceFintech	79,753	20	3,988	3,228	<,001	,254
	ExpériencePassée	97,619	20	4,881	3,761	<,001	,284
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	31,640	20	1,582	1,575	,062	,142
RESIGNATION	ConfianceFintech	73,987	15	4,932	3,993	<,001	,240
	ExpériencePassée	47,083	15	3,139	2,419	,003	,160
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	8,591	15	,573	,570	,895	,043
PERCEPTION * RESIGNATION	ConfianceFintech	263,220	70	3,760	3,044	<,001	,529
	ExpériencePassée	238,887	70	3,413	2,630	<,001	,492
	À quelle fréquence utilisez-vous des services bancaires en ligne par semaine (paiements en ligne, prêts numériques, gestion financière, cryptomonnaie, assurance, etc.) ?	145,333	70	2,076	2,067	<,001	,432

Les résultats du tableau des tests des effets intersujets démontrent que les variables indépendantes perception, résignation ont une influence significative sur la confiance aux Fintechs et sur l'expérience client, mais pas sur la fréquence d'utilisation des services financiers. Il n'y a que la variable d'interaction résignation * perception qui a une influence totale sur toutes les variables dépendantes. Par ailleurs, la covariable région a un impact sur la confiance aux fintechs, mais pas sur l'expérience et la fréquence d'utilisation. Pour finir, les covariables âge et genre n'ont aucun impact sur l'adoption des plateformes de Fintech.

Au regard de l'interprétation des résultats obtenus, nous pouvons conclure que la vulnérabilité des consommateurs québécois a un effet significatif sur l'adoption des Fintechs conformes à la Loi 25.

Tableau 4-32 : Récapitulatif des tests d'hypothèses

HYPOTHÈSES	RÉSULTATS
H1 : Le type de bannière de bannière de sécurité conçu par les entreprises dans le secteur de la Fintech a un effet positif sur la réduction du sentiment de vulnérabilité perçu par les utilisateurs	**Confirmé**
H2 : Plus la connaissance de la Loi 25 est grande, plus faible est le sentiment d'insécurité des utilisateurs face à l'utilisation de leurs informations personnelles en ligne.	**Confirmé**
H3 : L'adoption des mesures de protection des données a un effet positif sur la réduction du	**Confirmé**

sentiment de vulnérabilité par les utilisateurs dans le secteur de la Fintech.	
H4 : La transparence dans les modes de collecte et d'utilisation des données privées des entreprises de Fintech réduit favorablement la perception de la vulnérabilité des consommateurs.	**Confirmé**
H5 : L'utilité perçue des paramètres de sécurité a un effet positif sur la réduction du sentiment de vulnérabilité sur les plateformes de technologies financières.	**Confirmé**
H6 : Plus les paramètres de sécurité sont faciles d'utilisation, moins le consommateur en ligne se sent vulnérable sur les plateformes de technologies financières.	**Confirmé**
H7 : Plus l'utilisateur est convaincu de la performance des bannières de sécurité, plus faible sera son sentiment de vulnérabilité.	**Confirmé**
H8 : Le sentiment de vulnérabilité perçue par les consommateurs en ligne au Québec a un effet sur l'adoption des Fintechs conformes à la Loi 25.	**Confirmé**

4.5.9 Relation entre le type de bannière et action prioritaire sur une plateforme

Le tableau ci-dessous présente le profil des choix d'action prioritaire sur une page d'accueil selon le type de bannière de sécurité qui est présentée. Ce tableau nous permettra dans l'analyse de

nos hypothèses de recherche à déterminer l'impact des paramètres de sécurité sur le parcours client des utilisateurs ainsi que la meilleure stratégie à adopter pour proposer une meilleure expérience client aux consommateurs en ligne.

Tableau 4-33 : Tableau croisé entre action prioritaire et type de bannière de publicité.

Tableau croisé Après consultation de cette page d'accueil, choisissez votre première action sur le site. * Goal

			Goal						
			Acc. avec politique	Acc. ou paramétrer	Accepter tout	Cons. éclairé	Cookies essentiels	Sans bannière	Total
Après consultation de cette page d'accueil, choisissez votre première action sur le site.	Modifier les paramétrages de cookies	Effectif	1	13	2	3	2	2	23
		% du total	0,3%	4,3%	0,7%	1,0%	0,7%	0,7%	7,7%
	Lire la politique de confidentialité	Effectif	2	4	2	5	2	5	20
		% du total	0,7%	1,3%	0,7%	1,7%	0,7%	1,7%	6,7%
	Valider le consentement des cookies	Effectif	30	11	29	15	9	2	96
		% du total	10,0%	3,7%	9,7%	5,0%	3,0%	0,7%	32,0%
	Refuser l'utilisation des cookies	Effectif	11	14	13	23	7	10	78
		% du total	3,7%	4,7%	4,3%	7,7%	2,3%	3,3%	26,0%
	Valider les cookies essentiels	Effectif	0	6	4	0	27	6	43
		% du total	0,0%	2,0%	1,3%	0,0%	9,0%	2,0%	14,3%
	Contacter l'entreprise pour ses différents services	Effectif	0	0	0	1	0	9	10
		% du total	0,0%	0,0%	0,0%	0,3%	0,0%	3,0%	3,3%
	Consulter les prestations proposées	Effectif	6	2	0	3	0	15	26
		% du total	2,0%	0,7%	0,0%	1,0%	0,0%	5,0%	8,7%
	Quitter le site faute de paramètre	Effectif	0	0	0	0	3	1	4
		% du total	0,0%	0,0%	0,0%	0,0%	1,0%	0,3%	1,3%
Total		Effectif	50	50	50	50	50	50	300
		% du total	16,7%	16,7%	16,7%	16,7%	16,7%	16,7%	100,0%

Un test du chi carré (X^2) a également été réalisé dans le but d'évaluer la pertinence statistique de la liaison entre ces deux variables. Ce test permet de constater s'il y'a une relation significative entre deux variables qualitatives. Les résultats obtenus montrent effectivement qu'il existe une relation statistiquement significative entre le type de bannière de sécurité et l'action prioritaire car nous avons le coefficient de signification asymptotique P <, 001. Cette donnée indique que les participants au sondage réagissent différemment selon le design proposé.

Tableau 4-34: Test du chi carré type de bannière et action prioritaire

Tests du khi-carré

	Valeur	df	Signification asymptotique (bilatérale)
Khi-deux de Pearson	466,367[a]	35	<,001
Rapport de vraisemblance	399,452	35	<,001
N d'observations valides	300		

Ces résultats soulèvent l'importance de la prise en considération des intentions comportementales des utilisateurs lors de la conception des paramètres de sécurité. En d'autres termes, les bannières qui proposent une option claire (accepter ou configurer) ont tendance à stimuler des actions plus engagées de la part des consommateurs, alors que d'autres paramètres (Tout accepter), favorisent des actions passives.

À la lumière de ces résultats, nous pouvons affirmer que les dispositifs de transparence et de contrôle proposés aux usagers influencent directement leur sentiment de vulnérabilité en ligne, ce qui est cohérent avec les modèles SOR et UTAUT utilisés dans cette recherche. En effet, ils soutiennent la posture selon laquelle la conception éthique des paramètres de sécurité contribue à une perception plus positive et sécurisante des plateformes numériques, notamment dans le secteur des technologies financières.

CHAPITRE 5 : DISCUSSIONS, LIMITES ET AVENUES DE RECHERCHE

Après avoir présenté tout au long du chapitre précédent les résultats des analyses effectuées et les réponses aux questions de recherche, nous présentons dans cette partie une discussion des résultats obtenus, les limites de notre recherche et les différentes perspectives de recherche.

5.1 Discussion des résultats

Cette branche a pour objectif d'examiner et d'expliquer les résultats obtenus en considérant le cadre théorique et les recherches établis antérieurement. Une fois toutes les hypothèses validées, il est crucial d'évaluer leur portée et d'en tirer les implications aussi bien dans le domaine théorique que pratiques et de repérer toute nuance ou potentielle restriction.

5.1.1 Discussion des résultats obtenus sur l'analyse des bannières de sécurité

Le rapport d'étude des différentes bannières de sécurité conçues dans le secteur de la Fintech révèle un manque de considération de la protection des consommateurs, des règlements autour de la protection des données personnelles des utilisateurs et par conséquent du consentement des concepteurs de plateformes de Fintech au Québec.

En effet, l'analyse établie ci-dessus montre une différence importante dans les modèles de conception des secteurs de la Fintech versus les autres secteurs d'activité. Relativement aux volets légal, responsable et éthique que doivent respecter les entreprises dans l'élaboration des bannières de sécurité, le type de paramètres à mettre en exergue, car respecte les démarches imposées est la bannière << **Consentement libre** >>, peu importe la terminologie mise (approuver, c'est OK, Non merci, tout accepter, tout refuser, etc.), est celle qui donne le plein pouvoir à l'utilisateur en **Un Clic** d'accepter, de refuser ou de paramétrer les cookies durant leur parcours sur les plateformes donc il est le modèle le plus recommandé.

Ensuite vient le type de bannière << **Accepter ou configurer**>>, car ce type de paramètres donne la possibilité à l'utilisateur de consentir en **Un clic** que ses données soient utilisées, mais pour refuser ou faire un choix de cookies qu'on valide, il faut effectuer au moins **2 clics**, ce qui peut exercer un frein au consentement éclairé. La bannière << accepter ou accepter les cookies

essentiels>> a un caractère obligatoire sur les consommateurs à valider les témoins qu'ils soient en totalité ou ceux essentiels.

Les paramètres de sécurité << **Accepter avec politique de confidentialité**>> et << accepter>> ne donnent pas la possibilité à l'utilisateur de réfuter l'utilisation de ses données personnelles, car celui-ci est obligé de valider ou encore, même s'il ne valide pas, l'utilisation de la plateforme fait office de validation, ce qui est contraire aux règlements sur la protection des données et des consommateurs. Elles ne sont pas différentes des entreprises qui ne présentent pas de paramètres de sécurité et par conséquent qui n'appliquent pas les lois imposées aux entreprises pour le respect de la vie privée des consommateurs en ligne.

Aux vues des analyses des captures d'écran effectuées, nous pouvons affirmer que :

- Sur 130 entreprises de Fintech étudiées, 90 n'ont pas de bannières relatives à la protection des données, ce qui représente un pourcentage trop élevé d'entreprises de Fintech qui ne respectent pas la Loi, comparativement à 13 entreprises sur 134 dans les autres secteurs. Les Fintechs étant un secteur purement technologique où les données des consommateurs sont très utilisées, il serait primordial que ces entreprises s'alignent au règlement pour favoriser la protection et la confiance des consommateurs envers leurs services et produits.
- Les paramètres les plus utilisés dans les autres secteurs sont le modèle 46% de la population d'étude << accepter ou configurer>> et le modèle << Consentement libre>> 41% ce qui permet de dire que les entreprises des autres secteurs respectent plus le consentement du consommateur comparativement au secteur de la Fintech qui a un très faible taux représentatif de ces bannières, 5,38% pour << accepter ou configurer>> et 16,25% pour << Consentement libre>>.
- Sur 134 entreprises tous secteurs confondus, on a 04 entreprises qui utilisent les paramètres << tout accepter >> et 24 pour la bannière << accepter avec politique de confidentialité>> contre 7 sur 130 entreprises de Fintech pour le modèle << tout accepter >> et 3 Fintechs pour celui << accepter avec politique de confidentialité>>, ce qui représente un pourcentage plus faible pour le secteur de la Fintech.

Au vu des analyses et résultats obtenus, nous pouvons affirmer qu'il y'a encore du chemin à faire afin que la protection du consommateur soit effective dans le secteur de la Fintech au Québec. En effet, non seulement la plupart de ces entreprises (69,23%) ne respectent aucun volet (légal, éthique, responsable) de conception de paramètres de sécurité, car c'est inexistant, mais en plus sur les 30,77 restants, il n'y a que 16,25% d'entreprises qui respectent les volets de conception des bannières de sécurité et proposent un consentement éclairé aux consommateurs en ligne. Ceci dénote à suffisance qu'il est nécessaire d'établir un guide de recommandation optimal de consentement du consentement du consommateur en ligne sur les plateformes en Fintech au Québec.

5.1.2 Connaissance de la Loi 25

Le postulat 2 suppose que plus un consommateur détient les informations sur la Loi 25, moins il est exposé à un sentiment d'insécurité face à l'utilisation de ses informations personnelles en ligne. Pour rappel, notre cadre théorique souligne à travers le rapport du sondage réalisé en 2022 par le Commissariat à la protection de la vie privée du Canada (CPVPV, 2023) la présentation des enjeux en relation avec la protection de la vie privée des Canadiens, et ce par région. Il en ressort l'augmentation de la proportion des Canadiens préoccupés et plus enclins à suivre les actualités sur la gestion de leurs données personnelles pour se prémunir contre les dangers liés à l'utilisation de ces données par des tiers. L'un des changements importants qu'apporte la Loi 25 est l'obligation pour les entreprises d'informer et publier les politiques de confidentialité mises en place sur leurs sites, informer et publier également les conditions d'utilisation de ces sites web afin que l'utilisateur donne un consentement éclairé et juste sur la gestion de ses données privées. Il en résulte l'importance pour les utilisateurs de détenir les informations liées à la Loi 25 pour une meilleure gestion de leurs données en ligne.

Pour tester notre hypothèse de recherche, nous avons utilisé comme variables indépendantes la Loi 25 et la mesure du taux d'information illustrant respectivement le niveau de connaissance des consommateurs concernant la Loi 25 et leur degré d'exposition aux données relatives à cette Loi. L'évaluation de la vulnérabilité perçue des consommateurs s'est effectuée sur les aspects de perception et de résignation. Les résultats du tableau des tests multivariés confirment l'existence

d'un lien statistiquement important entre la connaissance de la Loi 25 et la diminution du sentiment de vulnérabilité des consommateurs.

L'analyse des effets spécifiques sur la perception et la résignation offre des éclaircissements sur l'effet distinctif des variables indépendantes sur les variables dépendantes précédemment citées. D'entrée de jeu, la variable mesure du taux d'information a un impact à la fois marqué et puissant sur les variables dépendantes, ce qui implique qu'un consommateur plus informé sur la Loi ressent une diminution de son sentiment de vulnérabilité face aux dangers associés à l'exploitation de ses données personnelles. Par contre, bien que la variable Loi 25 ait obtenu un impact statistiquement notable sur la perception (sig =0.011), son influence sur la résignation n'est pas avérée (sig = 0.094). Ce constat indique que le simple fait d'être au courant de la Loi 25 peut renforcer la perception de protéger ses données et diminuer le sentiment d'insécurité sans toutefois avoir un sentiment d'abandon des consommateurs. En d'autres termes, bien que la Loi 25 puisse donner l'impression aux utilisateurs d'une meilleure protection, cela ne veut pas dire que les consommateurs se sentent nécessairement plus maîtres des pratiques des entreprises.

Ces résultats corroborent en partie l'hypothèse H2 et mettent en lumière l'importance de la communication des informations relatives à la Loi 25. Il semblerait de ce fait que l'exposition à des contenus éducatifs (mesure du taux d'information) soit un moyen crucial pour diminuer la vulnérabilité perçue du consommateur dans ses deux aspects. Ceci permet de souligner l'importance des initiatives de sensibilisation des démarches éducatives pour informer les consommateurs sur la manière dont la Loi 25 participe à la protection de leurs données. Néanmoins, l'impact restreint d'une simple compréhension de la Loi 25 sur la résignation indique que d'autres éléments influencent la façon dont les consommateurs adoptent des comportements proactifs ou passifs en matière de protection de leurs données. La résignation des utilisateurs pourrait être influencée par divers facteurs tels que la confiance dans la pratique de la Loi, les expériences antérieures avec les Fintechs, le degré d'alphabétisation numérique.

Pour conclure, nous pouvons affirmer que l'hypothèse H2 est partiellement validée, car la compréhension de la Loi 25 contribue effectivement à atténuer le sentiment de vulnérabilité, mais son impact sur la résignation est restreint.

5.1.3 Adoption des mesures de protection des données.

Le postulat 3 soutient que l'adoption des mesures de protection des données a un effet positif sur la réduction du sentiment de vulnérabilité par les utilisateurs dans le secteur de la Fintech. Pour tester cette hypothèse, nous avons utilisé la variable indépendante consentement comme indicateur de mesure des pratiques de protection des données et les variables de vulnérabilité restent les mêmes.

À travers les résultats des tests multivariés (F = 1.873 et Sig. = 0.005), on peut affirmer que plus un utilisateur a l'impression d'avoir la maître de son consentement concernant les méthodes de collecte et d'exploitation des données, moins il se sent vulnérable. Plus précisément, l'analyse indique que le niveau de consentement a une influence significative sur la perception psychologique et l'attitude de résignation face aux enjeux liés à la protection des données. Cela met en évidence l'importance fondamentale de permettre aux utilisateurs de sélectionner et de modifier leurs préférences de confidentialité pour atténuer leur sentiment de vulnérabilité.

Les résultats des tests intersujets indiquent que la perception des dispositifs de protection des données peut fluctuer en fonction de la région et du profil démographique des personnes, ce qui peut par conséquent affecter leur sentiment d'insécurité. Ils soulignent également que les variations dans la compréhension du consentement aux politiques des données selon l'âge et la localisation influencent indirectement à la fois la perception et la résignation des utilisateurs.

Ces conclusions confirment l'hypothèse H3 en soulignant l'importance cruciale des politiques de consentement pour atténuer le sentiment de vulnérabilité des utilisateurs. En outre, l'influence des facteurs démographiques suggère que la compréhension du consentement et son incidence sur la vulnérabilité diffèrent en fonction du profil des personnes concernées. Par exemple, l'interprétation et la réaction des consommateurs aux politiques de confidentialité varient en fonction de l'âge et de la région.

Par ailleurs, le fait que certaines interactions n'aient pas un impact notable sur la résignation révèle aussi que, même si l'accord peut influencer la perception de la protection des données, il ne parvient pas toujours à prévenir un sentiment d'impuissance chez les consommateurs. Cela met en

évidence la nécessité de mesures additionnelles, telles que l'instruction numérique et une plus grande transparence en matière de gestion des données personnelles.

5.1.4 La transparence dans les modes de collecte

L'hypothèse 4 soutient la théorie selon laquelle la transparence dans les modes de collecte et d'utilisation des données privées des entreprises de Fintech réduit favorablement la perception de la vulnérabilité des consommateurs. Elle a été évaluée avec les mêmes variables de vulnérabilité que les hypothèses précédentes et avec les variables clarté, pertinence et transparence Fintech comme variables indépendantes.

Les résultats obtenus soutiennent l'hypothèse que la perception d'une plus grande transparence diminue les criantes des utilisateurs concernant l'utilisation de leurs données personnelles. Il est également à noter que le fait que les covariables âge, région et genre n'aient pas d'effet significatif sur la vulnérabilité indique que, indépendamment de ces variables personnelles, c'est véritablement la perception de la transparence des entreprises de Fintech qui est déterminante pour atténuer les sentiments de vulnérabilité. Toutefois, même si la clarté des paramètres de sécurité est un élément crucial pour une transparence perçue, son impact direct sur la perception et l'acceptation peut être influencé par d'autres facteurs (valeurs de signification élevées au P-value aux tests des effets intersujets : 0.119 et .092). Il se peut que la simple clarté ne soit pas suffisante pour diminuer la vulnérabilité. D'autres facteurs, tels que l'importance et la confiance accordée aux plateformes Fintech, pourraient avoir un impact plus déterminant.

Les conclusions tirées corroborent largement l'hypothèse H4, soulignant le rôle crucial de la transparence des plateformes Fintech dans la diminution de la vulnérabilité perçue des consommateurs. Ils démontrent que plus les sociétés mettent en œuvre des démarches explicites, intelligibles et appropriées pour la protection des données, plus les usagers se sentent protégés lors de l'utilisation des services Fintech. Toutefois, les conclusions mettent aussi en évidence l'importance d'examiner plus en détail l'impact spécifique de la clarté des paramètres de sécurité. Son impact sur la perception de la vulnérabilité n'est pas aussi manifeste que celui des autres aspects de la transparence, ce qui sous-entend que la simple clarté des informations ne suffit pas à réduire le sentiment de vulnérabilité.

Par conséquent, afin d'optimiser l'effet de la transparence sur la confiance des clients, les entreprises de Fintech doivent non seulement clarifier leurs paramètres, mais aussi s'assurer que ces données soient considérées comme véritablement significatives et en adéquation avec les préoccupations des utilisateurs.

5.1.5 L'utilité perçue des paramètres de sécurité

L'hypothèse 5 suppose que l'utilité perçue des paramètres de sécurité a un effet positif sur la réduction du sentiment de vulnérabilité sur les plateformes de technologies financières. Les variables dépendantes sont les mêmes que dans les hypothèses précédentes et les variables indépendantes utilisées pour mesurer l'utilité perçue sont l'attitude face aux paramètres et la variable utilité.

Les résultats aux tests multivariés attestent de l'effet bénéfique de la perception de l'utilité des paramètres de sécurité sur la diminution du sentiment de vulnérabilité et soutiennent les recherches antérieures qui indiquent que, plus les utilisateurs considèrent les paramètres de sécurité comme bénéfiques et significatifs, plus ils adoptent une attitude positive à leur égard, ce qui réduit leur sensation d'exposition aux risques numériques. La covariable région n'a pas d'impact sur les variables dépendantes, mais il est important de relever l'importance de l'effet de l'âge et du genre. Une influence notable de ces deux facteurs indique que certaines catégories de consommateurs en ligne, selon leur âge et leur sexe, pourraient appréhender différemment l'effet des paramètres de sécurité sur leur sentiment de vulnérabilité. Il se peut que les jeunes consommateurs soient plus au courant des mesures de protection et, de ce fait, présentent moins de vulnérabilité alors que les plus âgés, moins expérimentés avec les interfaces numériques, éprouvent un sentiment d'insécurité plus prononcé. De la même façon, les disparités de perception entre les hommes et les femmes peuvent être dues à des différences dans la prise de conscience des dangers numériques ou dans les comportements de navigation sur le Net comme présentés dans les résultats des statistiques descriptives.

Cependant, les tests intersujets présentent une distinction essentielle dans ces résultats. Bien que l'attitude et l'utilité perçue aient un impact général et notable sur la vulnérabilité ressentie des utilisateurs. Certaines interactions influencent uniquement une des facettes de la vulnérabilité. La

variable dépendante de résignation est exclusivement influencée par la variable utilité ainsi que les interactions utilité-région et utilité-âge, mais aucun impact sur la perception. Cela implique que la compréhension de l'importance des mesures de sécurité peut contribuer à diminuer l'acceptation passive des risques numériques (résignation), sans forcément affecter la perception générale de vulnérabilité. En d'autres termes, un utilisateur qui trouve utiles les bannières de sécurité peut être moins enclin à renoncer à toute tentative de protection de ses données, mais cela ne veut pas dire qu'il perçoit nécessairement un risque réduit.

Les observations établies mettent en évidence le fait que l'impact de l'utilité perçue sur la vulnérabilité n'est pas constant et peut varier selon la façon dont les utilisateurs assimilent ces critères de sécurité. Il se peut que certains choisissent d'adopter une approche proactive en incorporant ces outils dans leurs habitudes numériques, tandis que d'autres, bien qu'ils reconnaissent leur valeur, peuvent ne pas percevoir immédiatement le changement dans leur perception du risque.

Nous pouvons tirer comme conclusion que les résultats obtenus valident en grande partie l'hypothèse H5, prouvant que l'opinion sur les éléments de sécurité et leur valeur perçue ont un impact notable sur la vulnérabilité des consommateurs. Cependant, l'effet est plus prononcé sur la résignation que sur la perception, indiquant ainsi que les utilisateurs se sentent moins démunis face aux dangers numériques lorsqu'ils considèrent ces instruments comme bénéfiques. Cela ne veut pas dire pour autant qu'ils identifient moins de risques.

5.1.6 Facilité d'utilisation des bannières de sécurité.

Le postulat 6 soutient que plus les paramètres de sécurité sont faciles d'utilisation, moins le consommateur en ligne se sent vulnérable sur les plateformes de technologies financières. Nous avons la variable indépendante facilitée d'usage qui mesure la facilité d'utilisation des paramètres de sécurité et les variables dépendantes, perception et résignation qui mesurent la vulnérabilité des consommateurs québécois.

Les tests multivariés et intersujets confirment l'hypothèse initiale. Ceci implique que si les réglages de sécurité sont clairs et faciles d'accès, les utilisateurs se sentent moins exposés aux

dangers associés à la sauvegarde de leurs informations personnelles. Ce constat rejoint les études établies dans notre cadre conceptuel qui attestent que la complexité perçue des dispositifs de sécurité freine leur adoption et peut intensifier le sentiment d'impuissance des consommateurs face aux dangers du numérique. Cependant, une interface bien conçue et intuitive augmente la confiance des utilisateurs et favorise leur participation à des usages proactifs de protection. Par ailleurs, les covariables âge, sexe et région n'influent pas de manière significative sur le lien entre la facilité d'utilisation et la vulnérabilité. Ceci indique que l'effet de la simplicité d'utilisation sur le sentiment de sécurité peut s'appliquer à tous les utilisateurs sans tenir compte de leur profil démographique.

Au vu de ce rapport, nous pouvons affirmer que l'hypothèse H6 est confirmée : plus les paramètres de sécurité sont faciles d'utilisation, moins le consommateur en ligne se sent vulnérable sur les plateformes de technologies financières. Ce facteur, à l'inverse de plusieurs autres, paraît indépendant des variables sociodémographiques. Cela met en lumière la nécessité d'un design axé sur l'utilisateur lors de la mise en œuvre des mesures de protection de données.

5.1.7 Attente de performance de la Loi 25

L'hypothèse 7 soutient que plus l'utilisateur est convaincu de la performance des bannières de sécurité, plus faible sera son sentiment de vulnérabilité. La variable indépendante utilisée pour cette analyse est la variable efficacité Loi 25 et les variables dépendantes restent inchanger.

Les résultats des tests multivariés et intersujets sur l'effet de la variable efficacité Loi 25 sur la vulnérabilité des consommateurs montrent que lorsque ces derniers estiment que la Loi 25 est efficace et bien mise en œuvre, leur sentiment d'insécurité concernant l'utilisation de leurs informations personnelles est réduit. Cette observation est en accord avec les théories de la confiance institutionnelle, qui soutiennent que l'établissement de structures règlementaires robustes apaise les consommateurs et diminue leur inquiétude face aux dangers du numérique. Autrement dit, plus un utilisateur estime que la Loi 25 assure efficacement la protection de ses données, plus il se sent en toute sécurité lorsqu'il utilise des services numériques.

S'agissant du rôle modérateur du genre, les résultats montrent son impact partiel sur la vulnérabilité des consommateurs étant donné qu'il influence principalement la variable résignation,

mais pas celle de la perception. Ce constat indique que les disparités de genre pourraient influencer la façon dont les consommateurs associent la protection règlementaire à leur perception de sécurité numérique. Il est donc fort possible que les hommes et les femmes possèdent des échelles de sensibilisation ou des postures distinctes face aux dangers du numérique et aux dispositifs de sauvegarde des données, ce qui pourrait justifier cette influence déséquilibrée sur la perception et la résignation. Il serait de ce fait nécessaire de mettre l'accent sur l'importance de mieux appréhender la manière dont les diverses catégories de consommateurs assimilent et répondent aux mécanismes de protection des données, pour ajuster les actions de sensibilisation et les dispositifs d'accompagnement en fonction des nécessités particulières de chaque groupe.

Pour conclure, les résultats appuient l'hypothèse H7 selon laquelle plus l'utilisateur est convaincu de la performance des bannières de sécurité, plus faible sera son sentiment de vulnérabilité. En outre, bien que cet effet ne soit pas lié à l'âge ou à la région, il semble être modulé par le genre, qui a un impact significatif sur la résignation et non sur la perception. Ces résultats mettent en évidence le rôle crucial des régulations de protection des données dans l'établissement de la confiance numérique des consommateurs. Ils soulignent aussi l'importance de considérer les disparités individuelles dans la perception de la vulnérabilité numérique, pour assurer une protection efficiente et inclusive à tous les utilisateurs.

5.1.8 Sentiment de vulnérabilité et adoption des Fintechs

Le postulat 8 soutient que le sentiment de vulnérabilité perçue par les consommateurs en ligne au Québec a un effet sur l'adoption des Fintechs conformes à la Loi 25. Les variables dépendantes utilisées pour cette analyse pour déterminer l'adoption des Fintechs sont la variable confiance Fintech, la variable expérience et la fréquence d'utilisation des services financiers. Les variables indépendantes qui représentent le sentiment de vulnérabilité sont les variables perception et résignation.

L'ensemble des tests effectués corroborent l'existence d'un impact statistiquement significatif des variables indépendantes sur l'adoption des Fintechs qui respectent l'application de la Loi 25 et affirment que la perception de vulnérabilité et le renoncement face aux défis de la protection des données affectent la confiance et l'expérience des utilisateurs avec les Fintechs.

Néanmoins, l'examen des effets intersujets apporte une nuance à ces conclusions en démontrant que bien que la perception et la résignation affectent effectivement la confiance et l'expérience client, elles n'ont pas d'incidence directe sur la fréquence d'usage des services financiers. Ces résultats concordent avec les théories en vigueur sur l'adoption des innovations technologiques, qui stipulent que la confiance joue un rôle crucial dans l'acceptation des nouvelles technologies. Autrement dit, plus un utilisateur considère les plateformes de technologies financières sécurisées et transparentes, plus il leur témoigne sa confiance, augmentant ainsi son implication dans ces services. En revanche, un sentiment prononcé de vulnérabilité peut créer une réticence à s'impliquer avec ces plateformes, ce qui freine leur adoption. En ce qui concerne l'absence d'impact sur la fréquence d'usage, il se peut que d'autres éléments aient un rôle capital sur cette variable, comme les besoins financiers des utilisateurs, leur accès aux institutions classiques ou encore leur degré de maîtrise des outils digitaux. Ces facteurs pourraient clarifier pourquoi, malgré la confiance d'un consommateur en une plateforme Fintech et une expérience satisfaisante, cela ne se manifeste pas systématiquement par une utilisation plus régulière.

Un point intéressant à noter est l'impact global de l'interaction entre perception et résignation sur toutes les variables dépendantes d'adoption (confiance, expérience et fréquence d'utilisation). À l'impact des impacts isolés des deux facteurs, leur interaction paraît avoir un effet amplifiant : une perception marquée de vulnérabilité associée à une résignation croissante a tendance à réduire considérablement l'adoption des Fintechs, alors qu'une vision plus optimiste et une démarche proactive en termes de protection des données encouragent leur adoption. Ce constat indique que la vulnérabilité perçue et la résignation ne devraient pas être examinées de manière isolée, mais plutôt comme un mécanisme combiné qui influence le comportement des utilisateurs. En d'autres termes, un client qui se sent exposé, mais prend des précautions pour sécuriser ses informations peut conserver une certaine confiance dans les Fintechs, tandis qu'un client qui se sent exposé et choisit de ne rien faire développera une posture méfiante, ce qui diminue son utilisation des services Fintech.

L'étude des covariables a démontré que l'emplacement géographique des consommateurs affecte leur confiance envers les services financiers numériques, mais nous n'avons pas de répercussions notables sur leur expérience ou sur la fréquence d'utilisation des plateformes. Cette conclusion pourrait être due aux inégalités d'accès aux services numériques et aux infrastructures

technologiques qui existent entre diverses régions du Québec. Dans des régions où l'offre de ces services numériques est plus développée et mieux encadrée, les consommateurs pourraient accorder davantage de confiance à ces plateformes. À l'inverse, ceux qui résident dans des zones dont l'accès aux produits bancaires digitaux est restreint pourraient manifester une certaine réticence.

Par contre, les variables liées au genre et à l'âge n'ont pas d'impact sur l'adoption des plateformes de Fintech. On peut interpréter cette absence de diverses façons. D'un côté, l'adoption pourrait être davantage associée à des éléments psychologiques (confiance, perception des risques) et contextuels (besoins financiers, aisance avec les technologies) qu'aux caractéristiques sociodémographiques. Il est aussi envisageable que les disparités générationnelles ou de genre concernant l'utilisation des services financiers numériques commencent à diminuer, surtout avec la vulgarisation de ces services en ligne et des programmes de sensibilisation sur la sécurité des données.

Pour résumer, l'hypothèse 8 est confirmée grâce aux résultats obtenus : le sentiment de vulnérabilité perçue par les consommateurs en ligne au Québec a un effet sur l'adoption des Fintechs conformes à la Loi 25. Néanmoins, cet effet n'est pas affecté par l'âge et le sexe des utilisateurs, mais semble être atténué par les divergences régionales qui agissent principalement sur la confiance, sans toucher directement l'expérience des clients.

5.2 Limites de notre étude

Bien que cette étude soit méthodologiquement solide et que toutes les hypothèses de recherche aient été confirmées, il est nécessaire de relever certaines limites pour mieux comprendre l'ampleur des résultats et suggérer des orientations pour des recherches futures.

- La vulnérabilité mesurée par deux échelles et la confiance qui est intégrée à l'adoption.

Le premier point de limitation de cette étude concerne la mise en œuvre du concept de vulnérabilité perçue. Ce concept, fréquemment identifié dans les écrits comme étant complexe et à multiples facettes, a été évalué grâce à deux échelles distinctes conçues pour en saisir diverses dimensions complémentaires. L'approche méthodologique adoptée ne visait pas explicitemnt une

structure de vulnérabilité en deux dimensions, mais plutôt à consolider la validité du concept en prenant en compte ses aspects émotionnels et intellectuels. Les deux outils ont été conjointement utilisés, dans un but d'évaluation globale du sentiement de vulnérabilité, sans chercher à les comparer ou à mettre en opposition leurs aspects respectifs.

Par ailleurs, l'intégration de confiance dans le cadre du modèle d'adoption des services Fintech. Cette décision reflète une vision étendue de l'adoption, perçue non seulement comme une action réelle ou une intention d'utilisation, mais aussi comme un processus psychologique basé sur la confiance en la plateforme, surtout dans les environnements numériques présentant un risque élevé lié à des données financières délicates. Par conséquent, la confiance n'est pas considérée comme une variable indépendante séparée mais plutôt comme une partie intégrante de l'adoption, en accord avec les modèles d'acceptation technologique et les recherches sur la finance numérique.

Il est aussi essentiel de noter que des simplifications conceptuelles visibles dans cette recherche résultent de décisions méthodologiques prises, afin de garantir la concordance entre le cadre théorique, le plan expérimental et les exigences inhérentes à un travail de maîtrise. Même si certains concepts pourraient être conceptualisés de façon plus précises dans de recherches ultérieures, ils ont été regroupés à un niveau d'analyse pour assurer une interprétation claire et solide des résultats, sans nuire à la validité interne des tests effectués.

- Le facteur temporel des résultats à considérer

Il est nécessaire de rappeler que les actions et bonnes pratiques proposées dans l'application de la Loi 25 sont entrées en vigueur progressivement en septembre 2022, 2023 et 2024 et c'est à partir de septembre 2023 que les politiques de communication encadrant la gouvernance des données personnelles sont entrées en vigueur. De ce fait, cette Loi est encore toute nouvelle pour le consommateur québécois et cela limite le niveau de connaissance par tous comme l'a démontré le tableau des fréquences statistiques de la population ayant entendu parler la Loi 25 régissant la vie privée des consommateurs québécois en ligne. Par ailleurs, l'enquête ayant été réalisée à un moment donné, ceci indique que les opinions des consommateurs pourraient changer au fil du temps et surtout à mesure que la Loi est davantage comprise et mise en œuvre. Aussi, dans la

période de collecte réalisée sur une longue période, les résultats ont pu être influencés par le facteur temps.

- Un indice de vulnérabilité basée sur la perception.

Une des limites notables est l'évaluation de la vulnérabilité des consommateurs qui s'est faite au moyen d'indicateurs subjectifs, comme l'appréhension du risque et le sentiment d'impuissance face à la protection des données. Même si ces variables aident à saisir la perception des consommateurs, elles ne représentent pas des indicateurs objectifs de la sécurité des plateformes de technologies financières ni d'exemples précis de violation des données. Une recherche ultérieure pourrait associer ces perceptions à des indices concrets comme le dénombrement d'incidents de cybersécurité signalés ou l'efficacité des recours juridiques prévus par la Loi 25.

- Une prise en compte partielle des facteurs technologiques

Nous avons concentré notre recherche sur la perception des consommateurs sans toutefois approfondir les aspects technologiques des plateformes de technologies financières tels que la qualité des mesures de cybersécurité mises en œuvre ou encore le design des interfaces utilisateur qui pourraient avoir un impact direct sur la perception de vulnérabilité. Il serait donc judicieux de mener une étude plus approfondie des facteurs technologiques et ergonomiques afin de mieux saisir l'expérience utilisateur et son influence sur l'adoption des Fintechs.

- La représentativité de la population d'étude

Le mode de recrutement de notre échantillon par la technique de la boule de neige a favorisé une ressemblance de la population d'études. De ce fait, nous avons une concentration des échelles d'âge 24 – 29 ans et 30 – 35 ans au détriment des autres tranches d'âge. De ce fait, malgré la présence des autres tranches d'âge, l'échantillon ne reflète pas fidèlement la population du Québec. Par conséquent, on ne peut totalement étendre ces résultats à toute la population.

- Le contexte d'études

Étant donné que cette étude a principalement porté sur l'industrie des finances technologiques, et plus spécifiquement sur celles établies sur le territoire québécois uniquement, les conclusions ne peuvent pas être étendues à toute l'industrie des fintechs canadiennes ni sur les autres secteurs d'activités.

5.3 Proposition de contributions et avenues de recherche

Nous ne serons terminer notre travail de recherche sans proposer de façon distincte des contributions aussi bien scientifiques que managériales des avenues de recherche futures qui pourront aider les entreprises de ce secteur d'activité dans la construction d'un design du consentement de leur plateforme. Cette différenciation est cruciale pour souligner l'importance de notre étude, tant d'un point de vue théorique que pratique, tout en définissant la possibiliité à de futures recherches.

5.3.1 Contributions de la recherche

✓ Contributions théoriques

Notre travail enrichit la littérature existante relative à la protection des données personnelles et à l'adoption des technologies financières en offrant une analyse intégrée du sentiment de vulnérabilité perçue dans le cadre règlementaire de la Loi 25 au Québec. De manière plus détaillée, cette recherche propose plusieurs apports sur le plan théorique :

- Elle met en pratique l'idée de vulnérabilité perçue dans un cadre règlementaire Fintech, tout en l'associant à des aspects cognitifs (Connaissance de la Loi 25), fonctionnels (utilité perçue, facilité d'utilisation), informationnels (transparence des plateformes).
- Elle souligne également l'importance cruciale des paramètres de consentement en tant qu'intermédiaires entre la règlementation, la perception de risque et l'adoption des technologies.
- Elle approfondit les modèles d'adoption technologique (TAM, SOR) en incluant spécifiquement la vulnérabilité perçue comme facteur explicatif de l'adoption des services Fintech dans un contexte législatif restrictif.

✓ Contributions méthodologiques

Cette étude met en avant sur le plan méthodologique un design novateur qui associe une analyse descriptive du marché à une expérimentation quantitative. Voici les principales contributions méthodologiques :

- La conception d'un dispositif expérimental inter-sujets à un seul facteur et six conditions, basé sur de véritables bannières créées à partir de plateformes existantes.
- Dans une perspective multivariée, nous avons intégré des variables expérimentales (telles que le type de bannière) et des variables individuelles (telles que la connaissance de la Loi 25).
- Une mise en œuvre multidimensionnelle des notions de vulnérabilité perçue et d'adoption, offrant une analyse plus détailléée que les méthodes unidimensionnelles généralement utilisées dans la littérature.

✓ Contributions managériales

Cette recherche propose des conseils pratiques et immédiatement applicables pour les intervenants de la Fintech au Québec. Elle souligne en particulier ces éléments :

- L'élaboration des bannières de sécurité a un impact direct sur la confiance et l'utilisation des plateformes en ligne.
- Il faut considérer ces bannières comme des instruments d'expérience utilisateur et pas seulement comme des impératifs juridiques.
- Une conception de bannières de sécurité clair, transparent, accessible et adaptable contribue à diminuer considérablement le sentiment de vulnérabilité.
- Notre étude suggère un modèle de bannière de sécurité éthique, responsable et en conformité, basé sur une information exhaustive, un consentement éclairé et un contrôle réel fourni à l'utilisateur.

✓ Proposition de modèles types de bannières de sécurité conforme à la Loi 25

Afin de minimiser le sentiment de vulnérabilité des consommateurs québécois en ligne, il est crucial pour les plateformes Fintech de perfectionner l'ergonomie et l'accessibilité des paramètres de sécurité. La définition des normes claires, des choix de personnalisation intuitifs et un accompagnement transparent peut permettre aux utilisateurs de mieux maîtriser leurs données et par la suite, atténuer leur appréhension face aux risques du numérique. Il est donc crucial pour les entreprises du secteur de se concentrer sur la conception de leurs interfaces de sécurité, en adoptant des pratiques telles que :

- Des paramètres de sécurité facilement accessibles (interfaces simplifiées, notifications claires sur les options de confidentialité.
- Présenter des guides et des tutoriels pour accompagner les utilisateurs dans la configuration optimale de leurs préférences.
- Avec l'évolution de l'intelligence artificielle, il serait possible de présenter une approche axée sur la personnalisation qui offre aux utilisateurs d'ajuster facilement leurs paramètres de sécurité selon leurs besoins.

En facilitant la gestion de ces bannières de sécurité, les entreprises de Fintech ont non seulement la possibilité d'accroître la confiance de leurs utilisateurs, mais aussi de promouvoir une adoption plus large et active des meilleures pratiques dans le domaine de la cybersécurité. Aussi, les inégalités régionales notées suggèrent qu'une stratégie personnalisée par région aura des chances d'être judicieuse pour renforcer la confiance des consommateurs et ajuster des services aux particularités locales.

Concernant le pourcentage élevé d'entreprises de Fintech québécoises qui n'ont pas de paramètres de sécurité comme l'exige la Loi 25, on reconnaît que les grandes entreprises technologiques continuent de mépriser la vie privée des consommateurs dans cette industrie (Cachecho et Prom Tep, 2022) et cela est dû à l'absence d'engagement des consommateurs à participer à l'évaluation des risques mentionnés dans les termes et conditions de service.

Dans cette perspective, il serait bénéfique de configurer des paramètres de sécurité spécifiques dans les plateformes de Fintech afin d'améliorer la sécurité des données des consommateurs.

Il est recommandé de privilégier le concept de design éthique qui valorise un meilleur consentement des consommateurs et prend en compte leur niveau de connaissance avant d'offrir tout service ou fonctionnalité, afin d'équilibrer la relation entre le consommateur et la Fintech (Cachecho et Prom Tep, 2022). Il est probable que les consommateurs qui prennent des risques financiers ou qui sont compromis dans le respect de leur vie privée ne deviendront pas des clients fidèles à moyen et long terme. Les entreprises de technologie financière qui perdent leur réputation en raison de ces clients non protégés finiront par y laisser leur bénéfice, les deux parties sont donc perdantes si le système de protection des données n'est pas revu. Nous proposons par exemple l'utilisation d'un seul type de paramètres à appliquer pour toutes les entreprises de Fintech.

La particularité du type de paramètres à imposer est, qu'en un clic, il donne toutes les informations nécessaires à l'utilisateur sur la possibilité de valider, de refuser ou de paramétrer ses cookies, le type et le nom de cookies utilisés, leurs finalités, leurs dates d'expiration, etc. Les trois bannières présentées ci-dessous sont représentatives de ce qui peut être exécuté comme bannière de sécurité modèle. La bannière de la Structure Equisoft a pour seule limite qu'elle ne permet pas au consommateur en ligne de refuser l'utilisation de ses données personnelles, mais elle détaille : l'objectif de l'utilisation des cookies, les catégories de cookies (nécessaires, préférentiels, statistiques, marketing, non classés), le nom des cookies dans chaque catégorie, les fournisseurs des cookies et leur finalité, la date d'expiration des cookies dans leur système. La phrase introductive de la bannière de sécurité de Tourisme Montréal ‘‘LE RESPECT DE VOTRE VIE PRIVÉE NOUS TIENT’’ met en confiance l'utilisateur et c'est un exemple à appliquer dans notre bannière modèle. En associant la bannière de sécurité de la structure Equisoft à celle de la structure Ores, on obtient la bannière de sécurité idéale pour tout individu, peu importe son âge, son genre, son expérience d'utilisation et le caractère volontaire de l'usage de la plateforme. L'utilisateur est clairement informé sur ses choix, donc le consentement est éclairé.

Il est à noter que ce modèle de bannière respecte les concepts légal, responsable et éthique de la création d'une bannière de sécurité et que ces différentes contributions servent de manuel pratique pour les entreprises qui cherchent à équilibrer le respect de la Loi 25, la confiance des utilisateurs et l'efficacité numérique.

Figure 5-1: Bannière de sécurité Équisoft

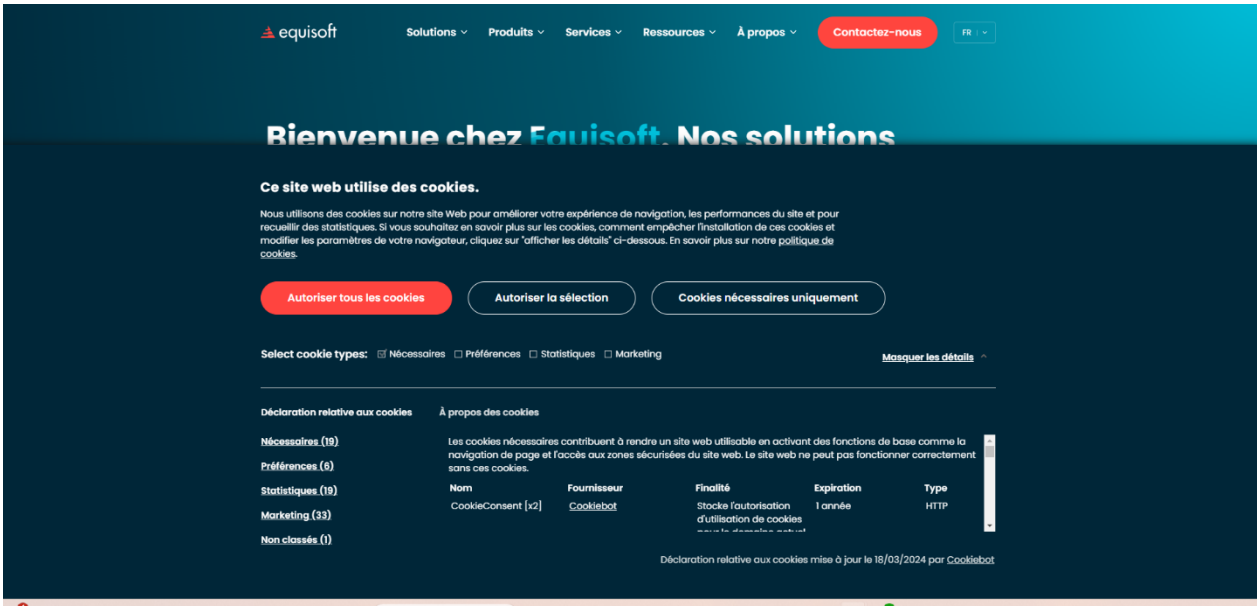
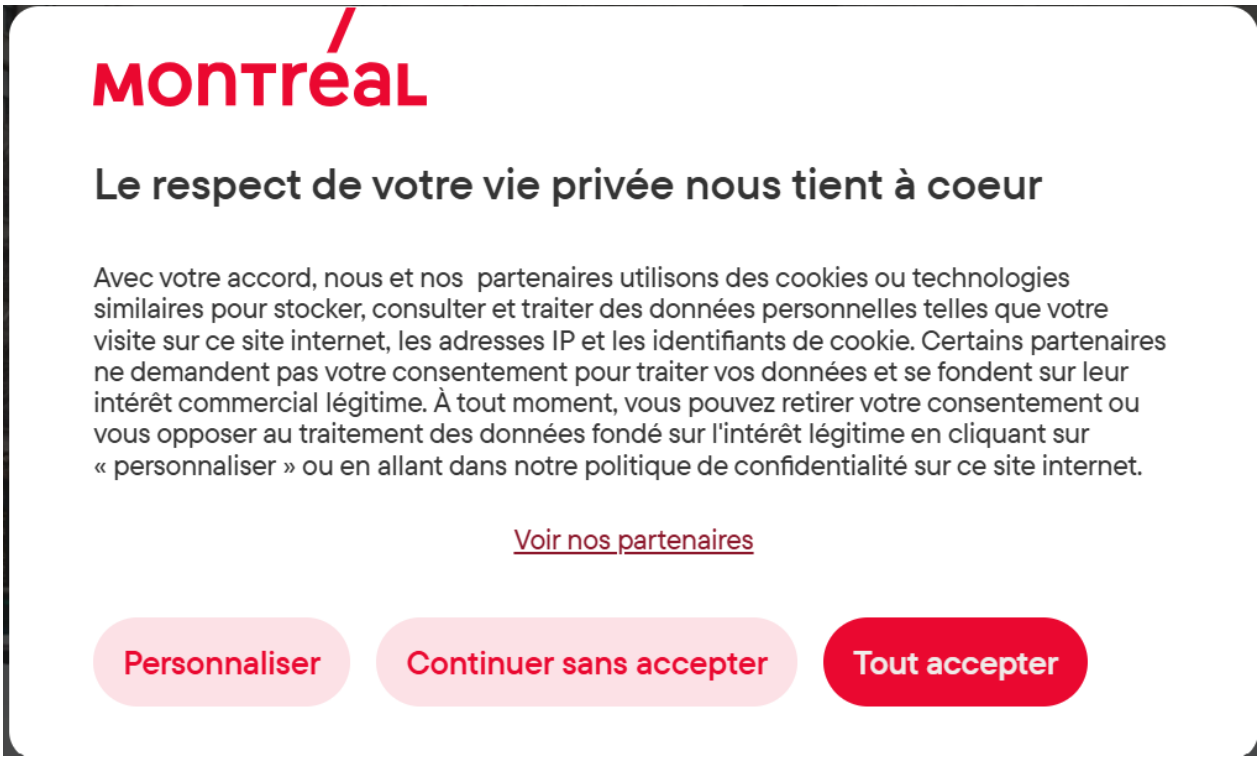


Figure 5-2: Bannière de sécurité Ores

Figure 5-3: Bannière de sécurité Tourisme Montréal



5.3.2 Avenues de recherche

- Étude sur le long terme des impacts de la Loi 25

Étant donné que la Loi 25 est encore nouvelle sur le territoire québécois, une recherche sur le long terme offrirait la possibilité de suivre l'évolution des perceptions du sentiment de vulnérabilité ainsi que les allures d'adoption des plateformes de Fintech au fur et à mesure que la Loi 25 est graduellement mise en œuvre par ces entreprises. Cela offrirait la possibilité de déterminer si la confiance des consommateurs se renforce au fil du temps ou si des inquiétudes subsistent en dépit des régulations.

- Une évaluation comparative internationale de l'impact des différentes règlementations

Une analyse comparative entre la Loi 25 du Québec, le RGPD européen et le CCPA californien peut aider à mieux saisir l'effet des différentes régulations sur la manière dont les consommateurs en ligne envisagent la protection de leurs informations, l'évolution de la confiance envers l'industrie, la technologie financière en fonction des différents environnements juridiques et les variations culturelles dans la manière dont la transparence et la sécurité des plateformes numériques sont perçues.

- Proposition de méthodes expérientielles et physiologiques en User Experience Design (UX)

Étant donné la sensibilité des données privées traitées sur les plateformes Fintech et du stress potentiel engendré par la gestion des finances personnelles pour bon nombre de personnes, des recherches futures pourraient se concentrer sur une analyse plus approfondie de l'expérience utilisateur en plus des indicateurs auto-déclarés. Des méthodes provenant de l'UX expérientiel pourraient par exemple être employés dans les recherches à venir combinant des questionnaires classiques avec des indicateurs physiologiques objectifs, tels que la réponse galvanique de la peau (GSR), le pouls ou l'observation du regard (Eye-tracking). Ces paramètres faciliteraient une évaluation plus détaillée du dégré de stress, de stimulation affective ou de charge mentale ressentie par les utilisateurs lorsqu'ils utilisent les plateformes financières et sont exposés à divers types de bannières de sécurité.

Cette démarche permet d'approfondir la compréhension des divergences possibles entre les perceptions stratégiques exprimées et les réactions affectives sous-jacentes, notamment dans un cadre règlememtaire rigoureux tel que celui de la Loi 25. Elle offrirait également la possibilité de repérer les aspects du design susceptibles de diminuer non seulement la vulnérabilité perçue, mais également le stress lié aux décisions de consentement et à la gestion des informations personnelles.

Pour conclure, l'incorporation des données physiologiques complèterait les recherches en UX éthique et responsable, en fournissant des éléments empiriques supplémentaires concerant l'influence émotionnel des paramètres de consentement dans le contexte financier numérique.

- Influence du type de bannières sur l'adoption des mesures de protection ou encore la perception de transparence des plateformes.

Cette recherche met en évidence, à travers les résultats obtenus, l'impact notable du type de bannières de sécurité sur la perception du sentiment de vulnérabilité. Néanmoins, sous une

approche théorique, il semble que cette variable manipulée aurait une portée plus étendue dans le cadre conceptuel suggéré.

Effectivement, la conception des bannières de consentement représente un èlèment visuel et cognitif primordial, qui pourrait influencer non seulement la vulnérabilité perçue, mais aussi d'autres perceptions essentielles comme la transparence des méthodes de collecte des données, la compréhension et l'acceptation des mesures de protection et enfin la perception de l'efficacité des systèmes de sécurité. Par exemple, une bannière explicite, précise et qui respecte le choix de l'utilisateur peut améliorer la perception de transparence et encourager une adoption plus réfléchie des paramètres de confidentialité. Le modèle examiné dans cette étude n'inclut pas ces éventuelles relations, pour préserver une structure d'analyses précise et conforme aux hypothèses établies.

Cependant, l'étude de ces effets indirects ou intermédiaires représentent une élaboration significative du modèle pour des recherches ultérieures en vue d'explorer le rôle du type de bannière en tant que précurseur des stimuli perceptuels, ou en tant qu'élément structurant l'exprience globale de consentement, en ayant recours à des analyses médiatrices ou des modèles d'équations structurales

CHAPITRE 6 : CONCLUSION

À travers l'exploration de la Loi 25, les débats sont de plus en plus centrés sur l'éthique, la protection des données personnelles et le pouvoir du consommateur dans la prise de décision. Il est clair que l'étau se resserre autour des entreprises de technologies financières afin que celles-ci respectent le consommateur dans la conception de ses paramètres de sécurité et que son consentement soit au centre de la création de ces bannières. Notre rapport a permis de démontrer préalablement, comparativement aux autres secteurs d'activité, que le secteur de la Fintech n'applique pas rigoureusement les mesures législatives, éthiques et responsables recommandées par les mesures de protection des consommateurs en ligne (plus de 70% de la population d'étude). Les bannières de sécurité des données sont presque inexistantes et pour celles présentes, à peine 7% offrent aux utilisateurs un consentement éclairé sur la gestion de ses données. Il revient à dire qu'un travail de longue haleine doit être établi dans ce secteur afin que la Loi soit appliquée par ces entreprises et que le consentement éclairé du consommateur ne soit pas une option, mais une obligation.

Ensuite, l'opportunité nous a été donnée d'évaluer l'effet de la Loi 25 sur la perception de vulnérabilité des consommateurs en ligne québécois dans le domaine des Fintechs. Nous avons examiné notamment comment différents éléments à l'instar de la transparence des plateformes, l'utilité et la facilité d'utilisation des paramètres de sécurité, l'efficacité de la Loi 25, etc., ont des effets significatifs sur le recours des consommateurs en ligne aux services financiers en ligne. Les résultats recueillis ont validé que la perception de vulnérabilité est un facteur essentiel dans l'adoption des plateformes de Fintech. Effectivement, nous avons démontré que la clarté des plateformes, l'utilité perçue des dispositifs de sécurité et les attentes en matière d'efficacité de la Loi 25 contribuent grandement à atténuer le sentiment d'insécurité chez les consommateurs. En outre, la recherche a souligné l'importance du consentement éclairé et de la simplicité d'utilisation des paramètres qui se présentent comme des outils stratégiques visant à réduire la résignation des utilisateurs face aux problématiques de protection des données. Cependant, l'usage des services

financiers numériques semble être moins touché, indiquant que certains clients pourraient persister à recourir à ces technologies en dépit de leur hésitation, soit par routine ou par besoin. Nos résultats mettent aussi en évidence que la région d'origine des consommateurs a une influence significative sur l'adoption des Fintechs.

Pour terminer, nous proposons comme principale voie de recherche future la personnalisation des paramètres de sécurité en fonction des choix de chaque utilisateur grâce à l'intelligence artificielle. L'intelligence artificielle permet une personnalisation donc en fonction des critères que la personne pourrait avoir comme choix au-delà des différentes couches (légal, responsable et éthique). Ce ne sera plus une question de configuration, d'interface ou de bouton que l'utilisateur doit choisir pour définir son consentement, il aura juste à décrire ce qu'il veut et l'intelligence artificielle fera l'adaptation avec le système.

ANNEXE A :
QUESTIONNAIRE

Sondage Vulnérabilité des consommateurs québécois en ligne

Bonjour et bienvenue.

Je m'appelle Phanie Mope, étudiante à l'École des Sciences de la Gestion de l'UQAM.

Dans le cadre de la rédaction de notre projet de mémoire, nous effectuons une étude du comportement des consommateurs en ligne face aux bannières de sécurité présents sur les sites web. À travers ce questionnaire, nous sollicitons votre participation à l'étude.

Le questionnaire ne prendra qu'une quinzaine de minutes! À gagner : une carte cadeau Winners d'une valeur de 50$.

Les critères de participation sont d'être majeur (18 ans et plus) et interagir avec les sites web pour n'importe quelle raison (magasiner, s'informer, etc.)

Il n'y a pas de bonnes ou de mauvaises réponses, seules vos opinions nous intéressent. **Certaines questions peuvent donner l'impression de se ressembler, mais elles mesurent chacune différents concepts.**

Votre anonymat sera préservé en tout temps, mais nous ne pourrons garantir l'anonymat total des réponses, car votre adresse courriel est requise de manière **optionnelle** dans le but de communiquer avec les gagnants du tirage.

Pour toute question additionnelle sur le projet et sur votre participation, vous pouvez communiquer avec l'étudiante chercheuse.

Phanie Manuela Mope Mbopda

Étudiante à la maîtrise en Sciences de Gestion en marketing numérique à l'ESG UQAM

mope_mbopda.phanie_manuela@courrier.uqam.ca

Sandrine Prom Tep, Ph.D

Professeure agrégée et directrice de recherche à l'ESG UQAM

Renato Hübner Barcelos

Professeur et co-directeur de recherche à L'ESG-UQAM

Section I : Questions générales

Q1 : J'accepte volontairement de participer à cette étude.

- J'accepte
- Je refuse

Q2 : Résidez-vous dans la province du Québec?

- Oui
- Non

Q3 : Quel âge avez-vous ?

- Moins de 18 ans.
- 18 - 23 ans
- 24 - 29 ans
- 30 - 35 ans
- 36 - 41 ans
- 42 - 47 ans
- 48 - 53 ans
- 54 - 59 ans
- 60 - 65 ans
- 66 ans et plus

Q4 : À quelle fréquence utilisez-vous les appareils connectés par jour (ordinateur, téléphone, tablette) ?

- 1 à 5 fois par jour
- 6 à 10 fois par jour
- 11 à 16 fois par jour
- Toute la journée
- Je n'utilise pas d'appareils connectés

Q5 : À quelle fréquence utilisez-vous des services Fintech par semaine (paiements en ligne, prêts numériques, gestion financière via applications, cryptomonnaie, assurance, etc.)?

- 0-2 fois
- 3-5 fois
- 6-8 fois
- 9-11 fois
- Plus de 12 fois
- Je n'utilise pas de services Fintech

Section 2 : Mise en situation projective en rapport à la bannière de sécurité présentée.

ATTENTION

Prenez le temps de consulter cette page d'accueil fictive du site web Atlas.

Considérez que cette page d'accueil vous est présentée lorsque vous accédez sur le site web de l'entreprise Atlas.

NB : la partie « **Nous respectons votre vie privée** » et son contenu représentent la **bannière de sécurité**.

Q6 : Après consultation de cette page d'accueil, choisissez parmi cette liste votre première action (action prioritaire sur le site).

- Refuser l'utilisation des cookies (Je refuse)
- Valider le consentement des cookies (Je suis d'accord)
- Modifier le paramétrage des cookies (Modifier mes préférences)
- Lire la politique de confidentialité (Politique de confidentialité)
- Contacter l'entreprise pour ses différents services (Contactez-nous)
- Consulter les prestations proposées (Nos prestations)
- Valider les cookies essentiels
- Quitter le site faute de paramètre

Q7 : Indiquez votre niveau d'accord avec les énoncés suivants :

- **<u>Pas du tout d'accord (1) Tout à fait d'accord (7)</u>**

	1	2	3	4	5	6	7
Je suis attentif (ve) face aux paramètres de sécurités présentés							

Je suis concentré (e) sur les paramètres de sécurité présentés							
Je consulte en détail ce qui m'est proposé comme choix de consentement							

Q8 : Indiquez votre niveau d'accord avec les énoncés suivants :

- **<u>Pas du tout d'accord (1) Tout à fait d'accord (7)</u>**

	1	**2**	**3**	**4**	**5**	**6**	**7**
La bannière de sécurité présentée est significative pour moi							
La bannière de sécurité présentée est utile pour moi							
La bannière de sécurité présentée est valable pour moi							

Q9 : Indiquez votre niveau d'accord avec les énoncés suivants :

- **<u>Pas du tout d'accord (1) Tout à fait d'accord (7)</u>**

	1	**2**	**3**	**4**	**5**	**6**	**7**
L'annonce est concrète							
L'annonce est utile							
L'annonce est détaillée							
L'annonce est explicite							

Q10 : Indiquez votre niveau d'accord avec les énoncés suivants :

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	2	3	4	5	6	7
Les paramètres sont persuasifs							
Les paramètres sont informatifs							
Les paramètres m'ont donné un aperçu différent de mon consentement							

Q11 : Indiquez votre niveau d'accord avec les énoncés suivants :

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	2	3	4	5	6	7
Je considère que mon consentement est juste							
Je considère être satisfait de mon choix de consentement							
Il est probable que je consente à une collecte de mes données privées							
Il est probable que je consente à une utilisation de mes données privées							

Q12 : Indiquez votre niveau d'accord avec les énoncés suivants :

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	2	3	4	5	6	7
Je me sens impuissant face aux paramètres de sécurité du site							
Les paramètres du site sont intrusifs							
Les paramètres du site me sont imposés							

Q13 : Perceptions psychologiques face à l'utilisation de mes données, indiquez votre niveau d'accord avec les énoncés suivants :

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	2	3	4	5	6	7
Je me sens exposé (e) sur cette page d'accueil							
Je me sens vulnérable sur cette page d'accueil							
Je me sens protégée sur cette page d'accueil							
Je me sens susceptible vis-à-vis de cette page d'accueil							

Q14 : Utilisation à long terme de mes données par le site Atlas, indiquez votre niveau d'accord avec les énoncés suivants :

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	2	3	4	5	6	7

J'ai l'impression que mes informations seront rendues publiques à travers ce site.							
J'ai l'impression que les informations resteront anonymes et confidentielles sur ce site.							

Section 3 : Connaissance de la *Loi* 25 et réactions face aux politiques de confidentialité

Bon à savoir : La **Loi 25** est celle qui exige un consentement clair de l'utilisateur avant toute utilisation de ses informations et impose aux entreprises de notifier rapidement les utilisateurs en cas de fuite de données à travers les **bannières de sécurité** qui vous sont présentées sur les pages d'accueil des sites web.

Q15 : Avez-vous déjà entendu parler de la Loi 25 régissant la vie privée des consommateurs québécois en ligne?

- Oui
- Non

Q16 : Si oui, où avez-vous entendu parler? (Cochez toutes les options pertinentes)

- Médias (télévision, journaux, etc.)
- Réseaux sociaux
- Sites web d'informations
- Par votre employeur
- Par un fournisseur de services Fintech
- Autre : _____

Q17 : Vous avez déjà entendu parler de la Loi 25, évaluer les affirmations suivantes selon votre degré d'accord.

Pas du tout d'accord (1) Tout à fait d'accord (7)

	1	**2**	**3**	**4**	**5**	**6**	**7**

Depuis l'application de la Loi 25, j'ai l'impression d'avoir un meilleur contrôle sur les données que je laisse en ligne.							
L'application des nouvelles mesures de protection (Loi 25) améliore ma confidentialité							
Depuis l'application de la Loi 25, j'ai l'impression que les données que je laisse en ligne sont gardées de manière plus sécurisée.							

Q18: Vous n'avez pas entendu parler de la Loi 25, évaluer les affirmations suivantes selon votre degré d'accord.

Pas du tout d'accord (1) Tout à fait d'accord (7)

	1	**2**	**3**	**4**	**5**	**6**	**7**
Je n'ai aucune idée de la Loi 25, mais j'ai l'impression d'avoir un meilleur contrôle sur les données que je laisse en ligne.							
Je n'ai aucune idée de la Loi 25, mais j'ai l'impression d'avoir une amélioration de ma confidentialité en ligne.							
Je n'ai aucune idée de la Loi 25, mais j'ai l'impression que les données que je laisse en ligne sont gardées de manière plus sécurisée.							

Q19 : Dans quelle mesure pensez-vous être informés sur les changements apportés par la Loi 25? Évaluer votre affirmation.

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	**2**	**3**	**4**	**5**	**6**	**7**

Je pense être assez informé (e) sur les différents changements apportés par la Loi 25.							

Q20 : Lisez-vous les politiques de confidentialité des sites web que vous utilisez?

- Oui
- Non

Q21 : Pourquoi ne lisez-vous pas les politiques de confidentialité?

- Elles sont trop longues
- Vous ne vous en souciez pas
- Elles contiennent trop de jargon juridique
- Vous faites confiance aux entreprises
- Vous souffrez d'une déficience de lecture
- Elles sont tous identiques

Q22 : Lisez-vous les bannières de sécurité des sites web que vous utilisez?

- Oui
- Non

Section 4 : Perception de la vulnérabilité dans le secteur de la Fintech québécoise

Q23 : Pensez-vous être plus à l'aise quant aux paramètres de protection de vos données par les services bancaires en ligne? Évaluer votre affirmation.

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	**2**	**3**	**4**	**5**	**6**	**7**
J'estime qu'il est plus facile d'interagir avec les paramètres de sécurité.							
J'estime que les bannières de sécurité sont faciles à apprendre à utiliser							

Les interactions avec les paramètres de sécurité sont faciles à comprendre pour moi							

Q24 : Ressentez-vous une quelconque crainte ou appréhension à l'égard de l'utilisation de services bancaires en ligne après l'entrée en vigueur de la Loi 25? Évaluer votre affirmation.

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	**2**	**3**	**4**	**5**	**6**	**7**
Je ressens une crainte lors du partage de mes informations personnelles sur les sites ou applications de Fintech.							
Je me sens plus en sécurité concernant la protection de mes données personnelles							

Q25 : Quelles sont les principales sources de cette vulnérabilité perçue? (Cochez toutes les options pertinentes)

- Crainte d'une violation de mes données privées.
- Manque de transparence sur l'utilisation des données.
- Complexité des conditions d'utilisation.
- Insécurité liée aux transactions financières.
- Difficulté à comprendre les nouveaux droits conférés par la Loi 25.
- Autre : _____

Q26 : Quel est votre niveau de confiance en les entreprises de services bancaires pour la gestion de vos données? Évaluer votre affirmation.

- **Pas du tout d'accord (1) Tout à fait d'accord (7)**

	1	**2**	**3**	**4**	**5**	**6**	**7**

J'ai confiance aux entreprises bancaires en ligne							
Les entreprises bancaires en ligne sont suffisamment sécurisées pour protéger mes données.							

Q27 : Évaluer votre affirmation.

- **<u>Pas du tout d'accord (1) Tout à fait d'accord (7)</u>**

	1	**2**	**3**	**4**	**5**	**6**	**7**
L'application de la Loi 25 est efficace pour réguler les entreprises de services bancaires et protéger mes données.							
L'application de la Loi 25 réduit mon sentiment de vulnérabilité lorsque j'utilise les services bancaires en ligne.							

Q28 : Quel est votre niveau d'accord avec les questions suivantes? Évaluer votre affirmation.

- **<u>Pas du tout d'accord (1) Tout à fait d'accord (7)</u>**

	1	**2**	**3**	**4**	**5**	**6**	**7**
Les services bancaires en ligne sont transparents quant à la façon dont elles collectent et utilisent mes données.							
Je comprends comment mes données sont gérées par les services bancaires en ligne que j'utilise							

Q29 : Expériences passées avec une entreprise de Fintech. Quel est votre niveau d'accord avec les questions suivantes? Évaluer votre affirmation.

- **<u>Pas du tout d'accord (1) Tout à fait d'accord (7)</u>**

	1	2	3	4	5	6	7
J'ai déjà été victime d'une violation de données par une entreprise de services bancaires.							
Mon expérience passée de violation de données me rend plus méfiant (e) vis-à-vis des entreprises de services bancaires.							

Section 5 : Variables individuelles et questions socio-démographiques

Q30 : Connaissances vis-à-vis des outils de protection des données. Indiquez votre niveau d'accord avec l'énoncé suivant :

Pas du tout d'accord (1) Tout à fait d'accord (7)

	1	2	3	4	5	6	7
Je communique de manière sûre avec les appareils technologiques (Téléphone, tablette, ordinateur).							
Je suis familière aux paramètres de sécurité.							
J'ai facilement accès aux moyens d'informations sur la protection des données.							

Q31 : Inquiétude concernant la protection de la vie privée. Indiquez votre niveau d'accord avec l'énoncé suivant :

Pas du tout d'accord (1) Tout à fait d'accord (7)

	1	2	3	4	5	6	7

En général, je me préoccupe de ma vie privée lorsque j'utilise internet.							
Je crains que les informations que je communique soient utilisées à mauvais escient.							
Je crains qu'une personne puisse avoir accès à des informations privées me concernant sur Internet.							

Q32 : A quel genre vous identifiez-vous ?

- Masculin
- Féminin
- Non-binaire
- Autre
- Je préfère ne pas répondre

Q33 : Dans quelle région du Québec résidez-vous présentement ?

- Abitibi-Témiscamingue
- Bas-Saint-Laurent
- Capitale-Nationale
- Centre-du-Québec
- Chaudière-Appalaches
- Côte-Nord
- Estrie
- Gaspésie–Îles-de-la-Madeleine
- Lanaudière
- Laurentides
- Laval
- Mauricie
- Montérégie
- Montréal
- Nord-du-Québec
- Outaouais
- Saguenay–Lac-Saint-Jean

Q34 : Parmi les catégories suivantes, quel est votre statut professionnel :

- Étudiant
- Salarié
- Fonctionnaire
- Travailleur indépendant

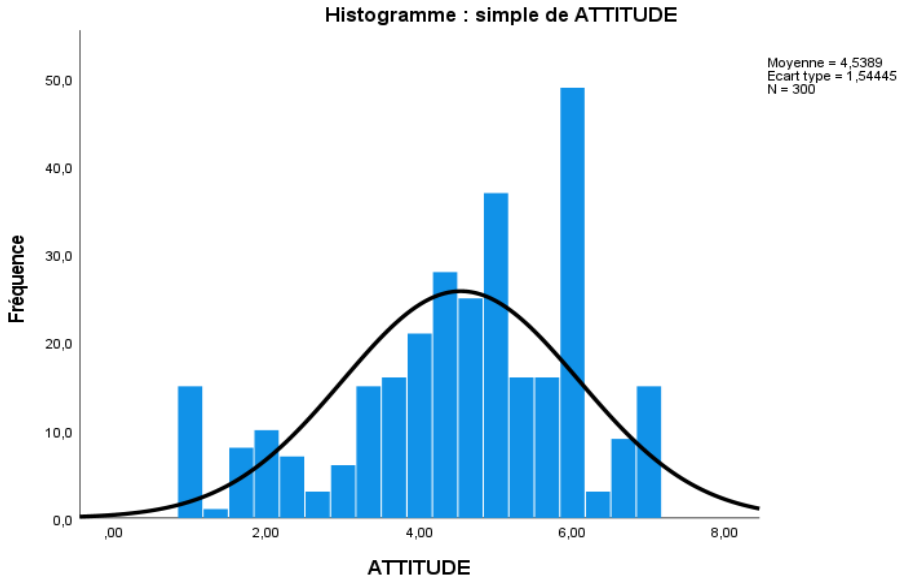
- Sans emploi

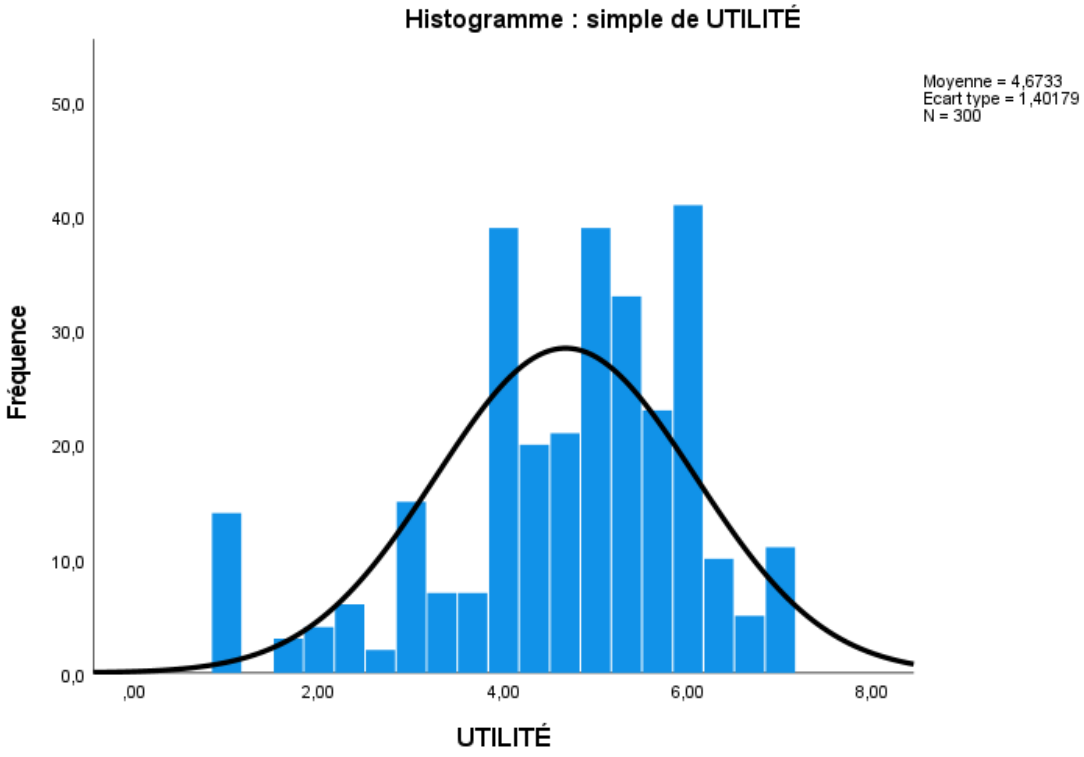
<u>Section 6 : Tirage au sort (FACULTATIF). Votre courriel ne sera pas utilisé à d'autres fins.</u>

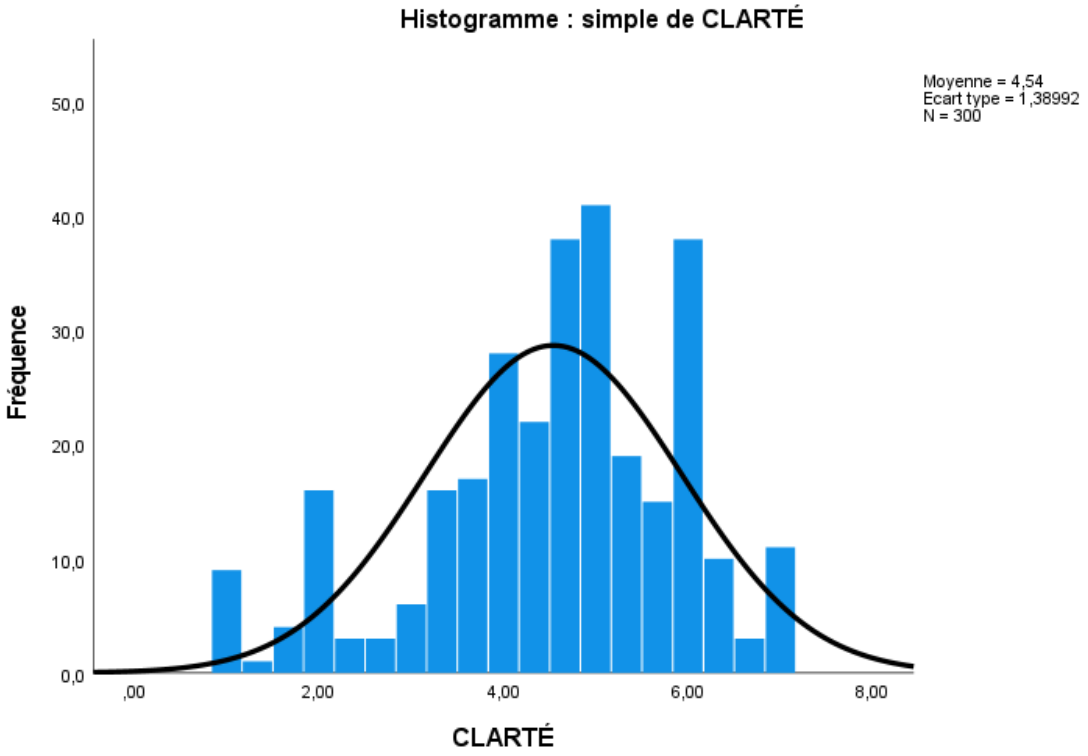
- *Si vous souhaitez gagner l'une des quatre cartes cadeaux de 25$ valables dans les magasins Winners, veuillez remplir la section ci-dessous. Ces cartes cadeaux seront aléatoirement attribuées par tirage au sort parmi les répondants de ce sondage. Une fois la collecte de données terminée, nous vous contacterons par courriel si vous gagnez.*

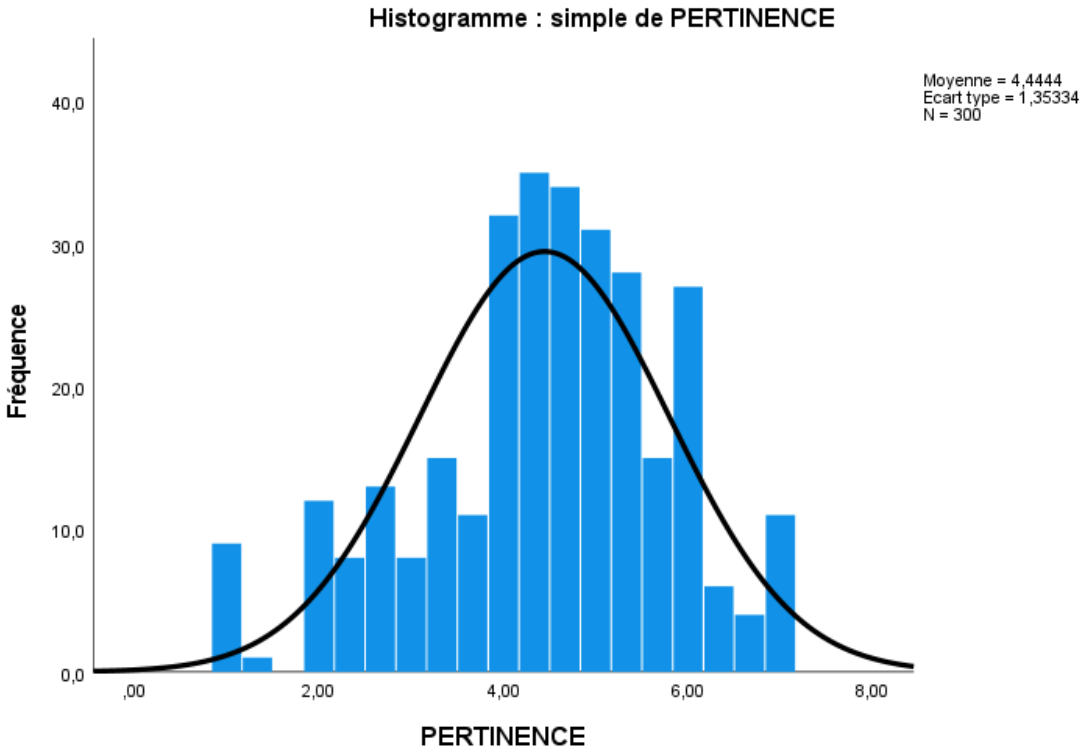
Votre adresse courriel: _____

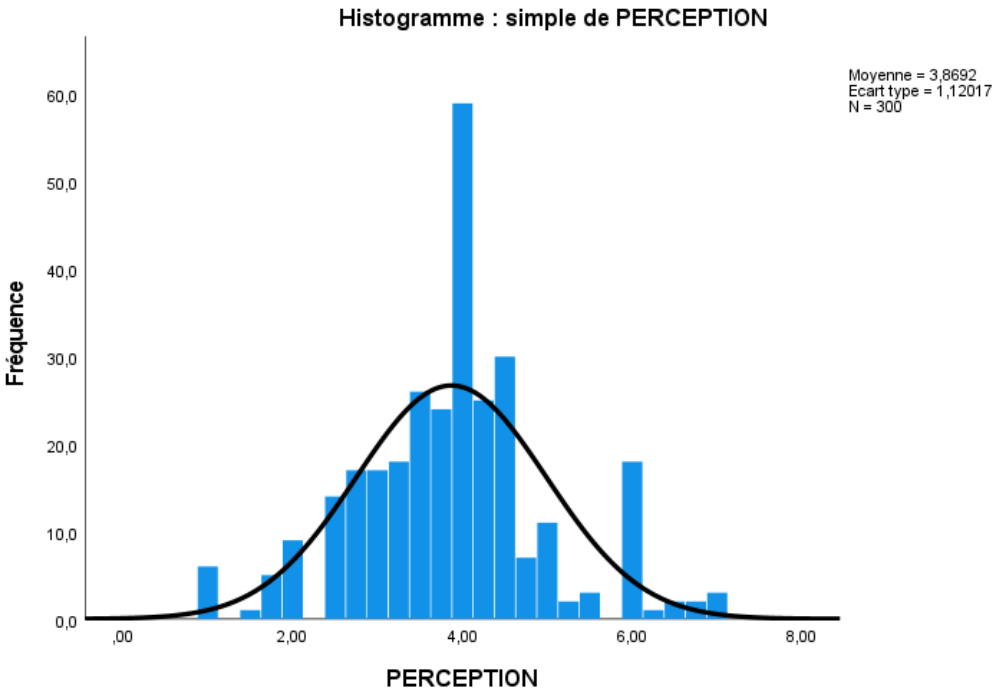
ANNEXE B : HISTOGRAMMES DE NORMALITÉ

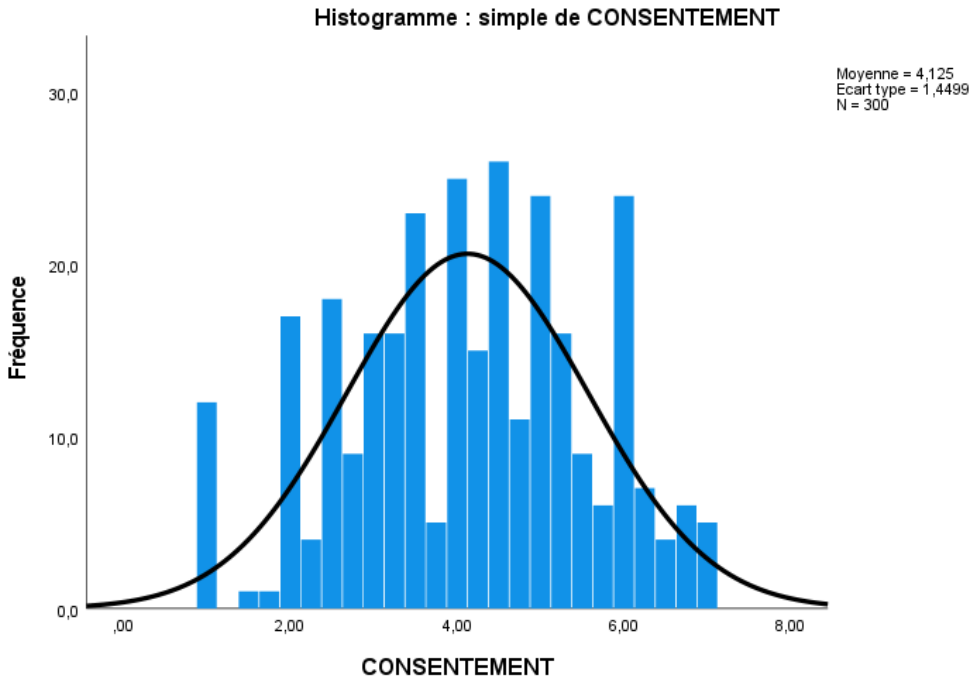


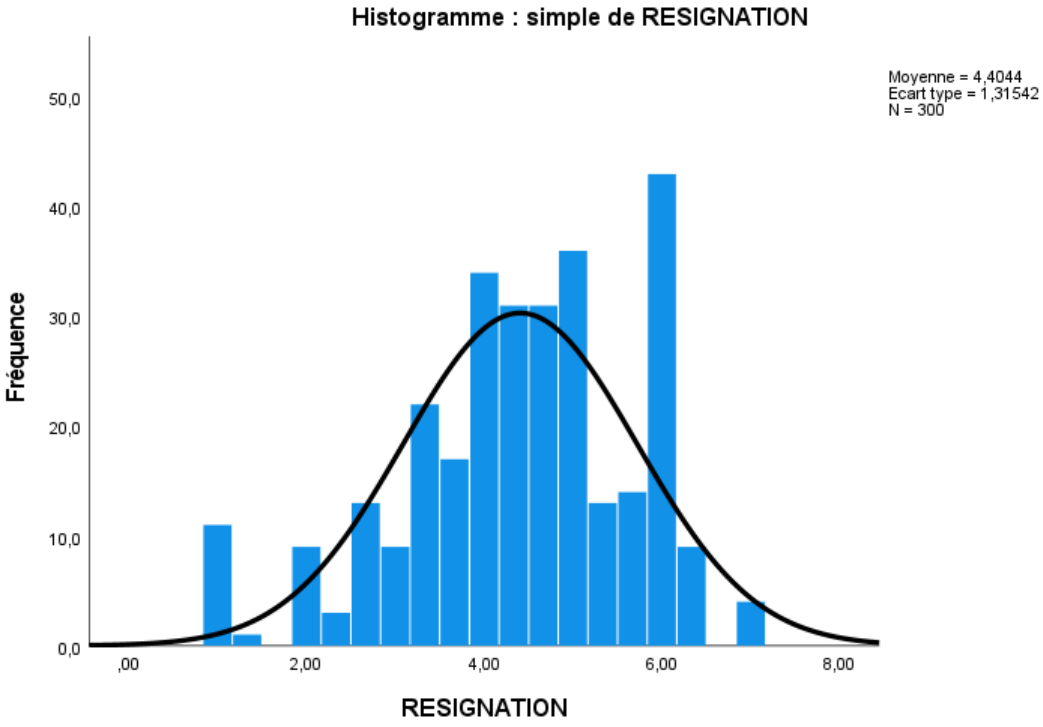


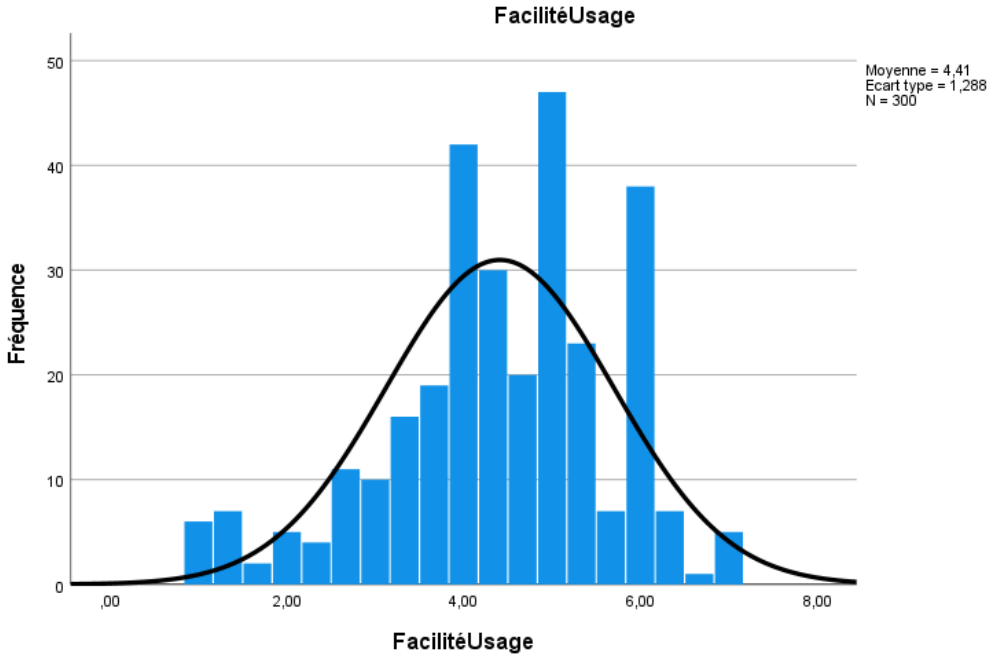

Histogramme : simple de CLARTÉ
Moyenne = 4,54
Ecart type = 1,38992
N = 300
Fréquence
50,0
40,0
30,0
20,0
10,0
0,0
,00
2,00
4,00
6,00
8,00
CLARTÉ

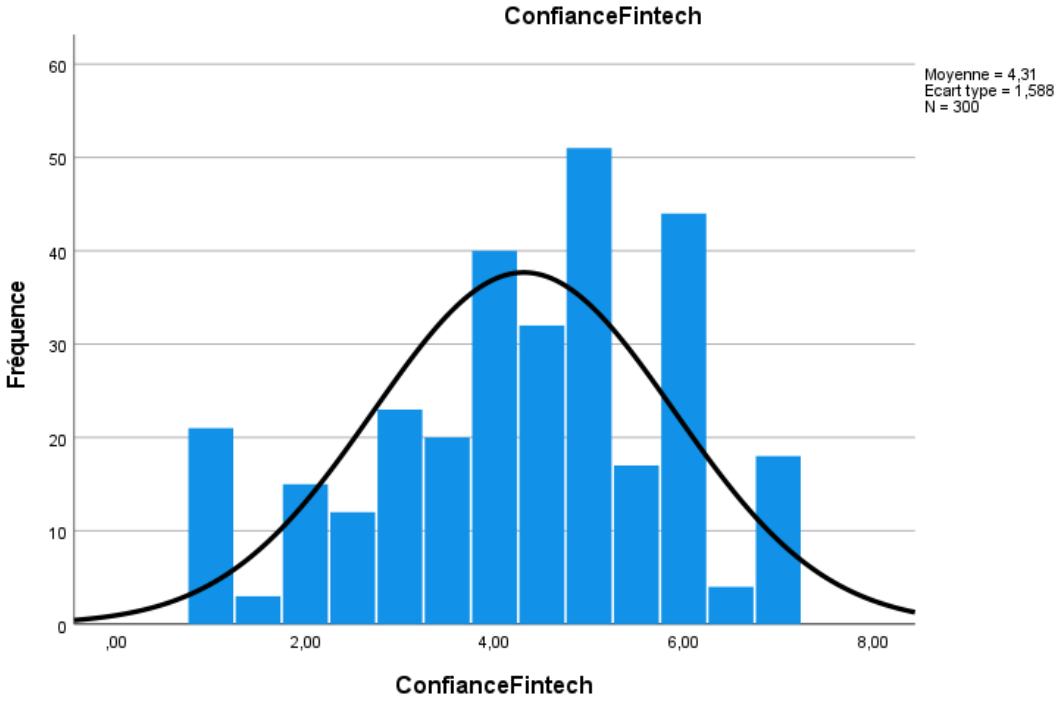

Histogramme : simple de PERTINENCE
Moyenne = 4,4444
Ecart type = 1,35334
N = 300
Fréquence
40,0
30,0
20,0
10,0
0,0
,00
2,00
4,00
6,00
8,00
PERTINENCE

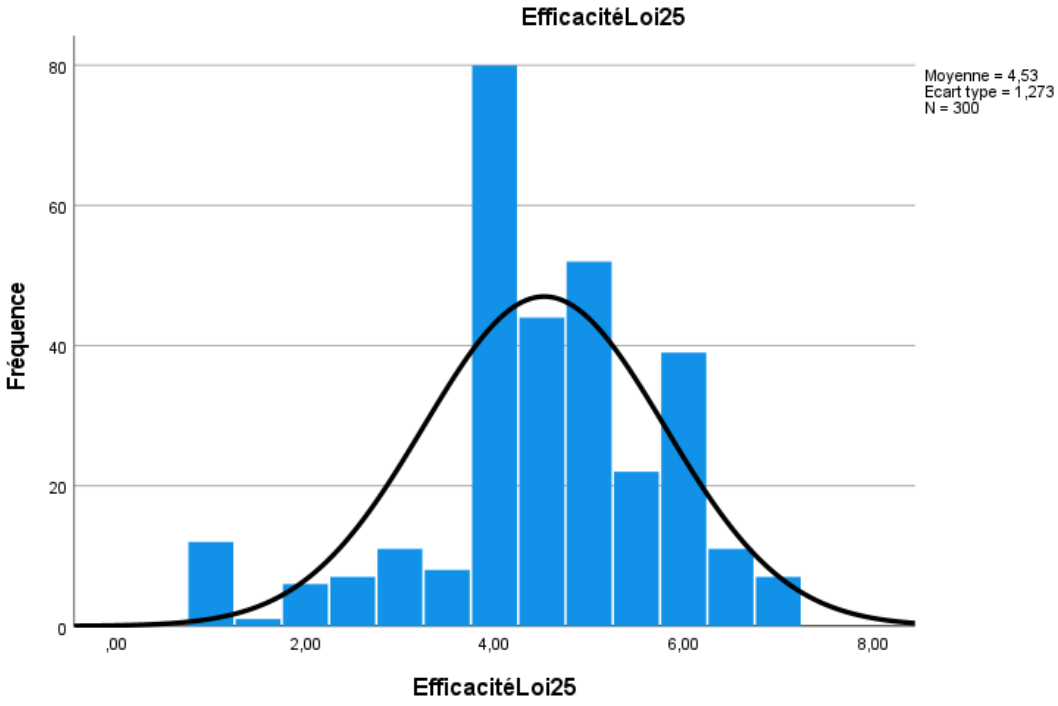

Histogramme : simple de PERCEPTION
Moyenne = 3,8692
Ecart type = 1,12017
N = 300
Fréquence
60,0
50,0
40,0
30,0
20,0
10,0
0,0
,00
2,00
4,00
6,00
8,00
PERCEPTION

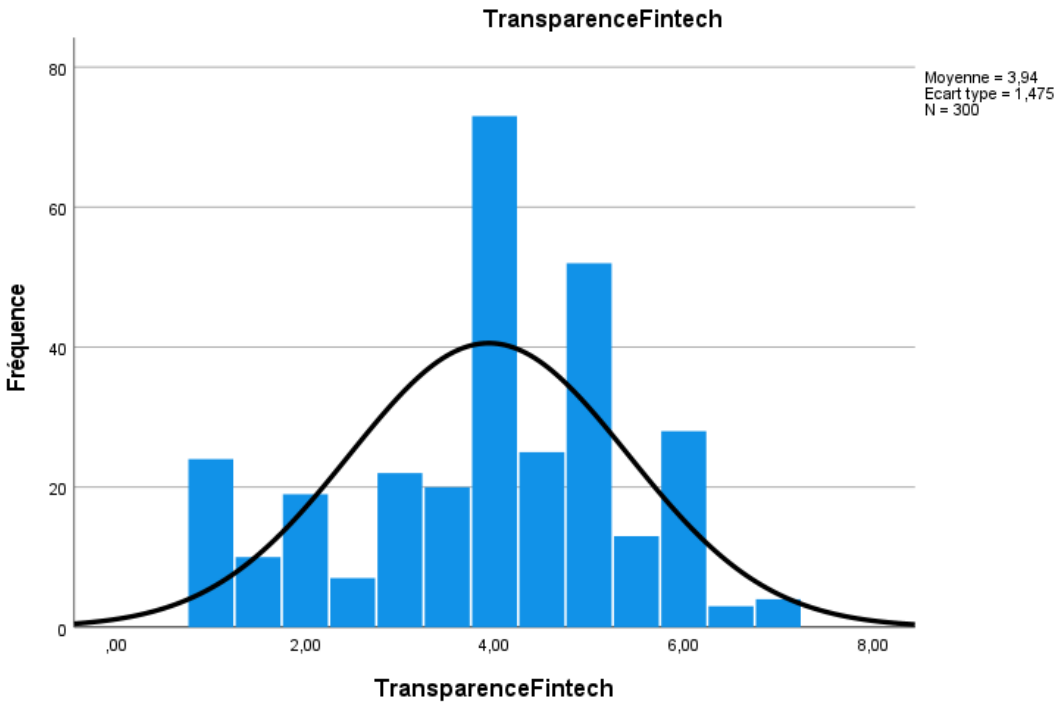

Histogramme : simple de CONSENTEMENT
Moyenne = 4,125
Ecart type = 1,4499
N = 300
Fréquence
30,0
20,0
10,0
0,0
,00
2,00
4,00
6,00
8,00
CONSENTEMENT


Histogramme : simple de RESIGNATION
Moyenne = 4,4044
Ecart type = 1,31542
N = 300
Fréquence
50,0
40,0
30,0
20,0
10,0
0,0
,00
2,00
4,00
6,00
8,00
RESIGNATION

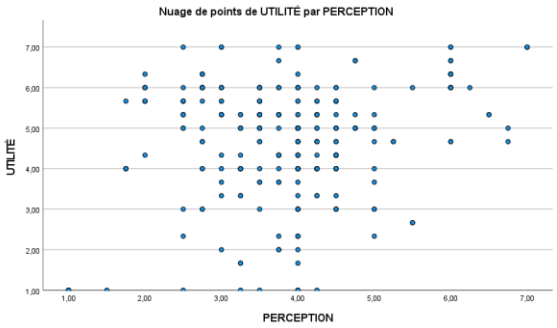

FacilitéUsage
Moyenne = 4,41
Ecart type = 1,288
N = 300
Fréquence
50
40
30
20
10
0
,00
2,00
4,00
6,00
8,00
FacilitéUsage

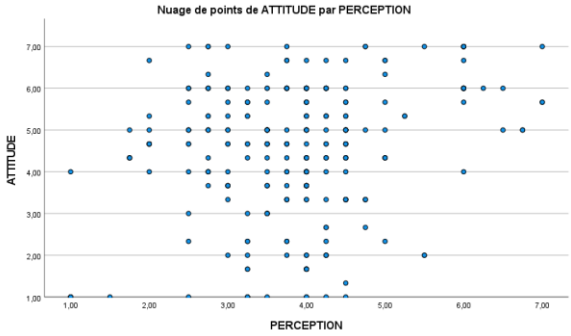

ConfianceFintech
Moyenne = 4,31
Ecart type = 1,588
N = 300
Fréquence
60
50
40
30
20
10
0
,00
2,00
4,00
6,00
8,00
ConfianceFintech

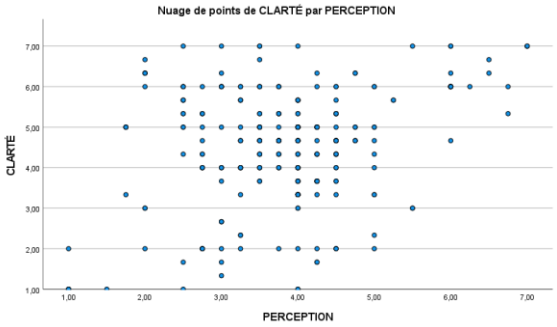

EfficacitéLoi25
Moyenne = 4,53
Ecart type = 1,273
N = 300
Fréquence
80
60
40
20
0
,00
2,00
4,00
6,00
8,00
EfficacitéLoi25

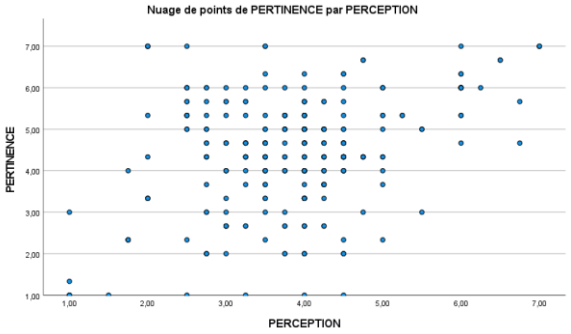

TransparenceFintech
Moyenne = 3,94
Ecart type = 1,475
N = 300
Fréquence
80
60
40
20
0
,00
2,00
4,00
6,00
8,00
TransparenceFintech

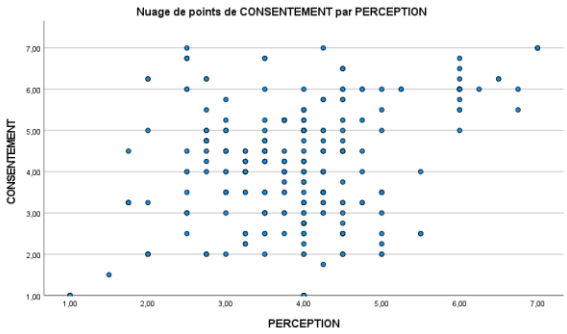
ANNEXE C : NUAGES DE POINTS RELATION ENTRE VARIABLES DÉPENDANTES ET COVARIABLES

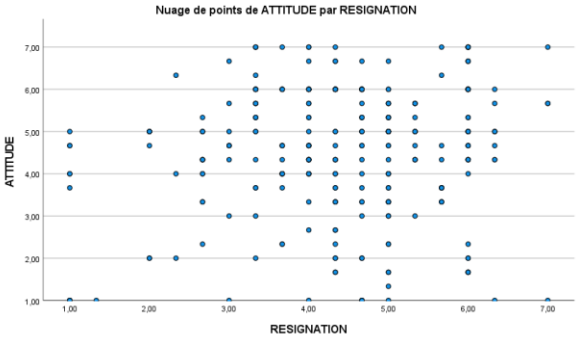


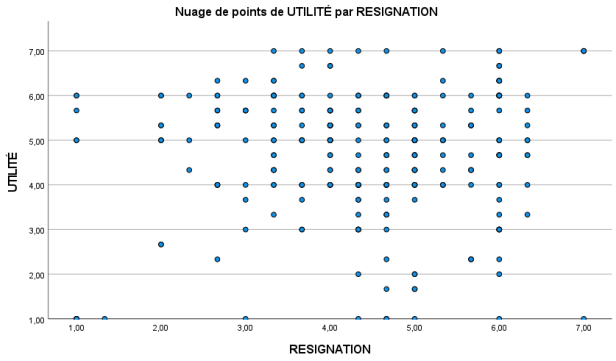


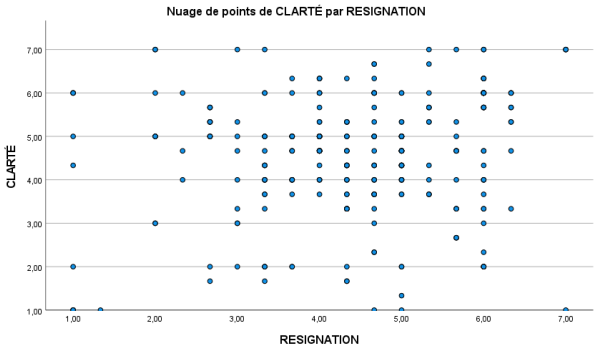


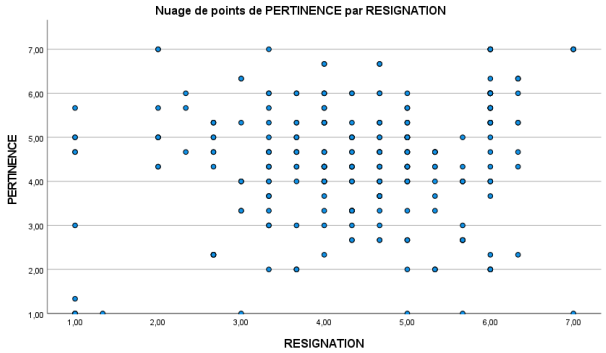


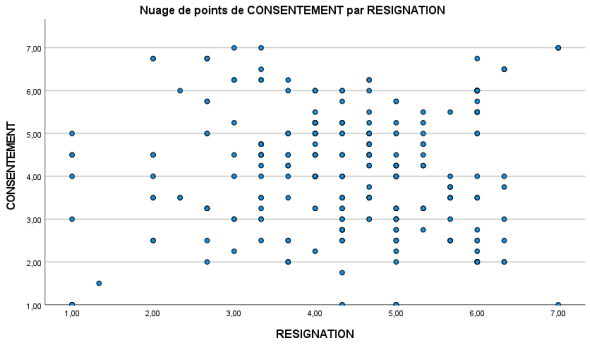


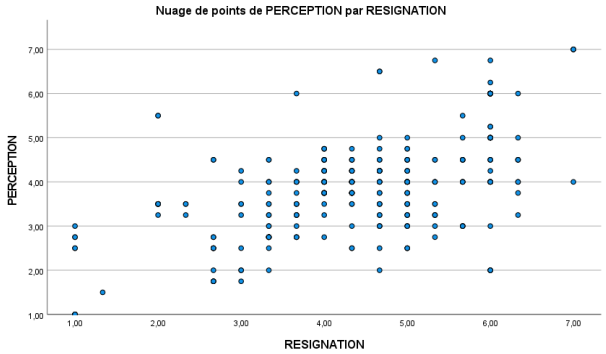


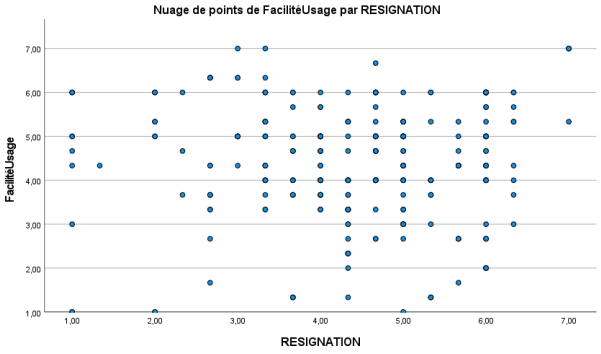

Nuage de points de UTILITÉ par RESIGNATION
UTILITÉ
RESIGNATION

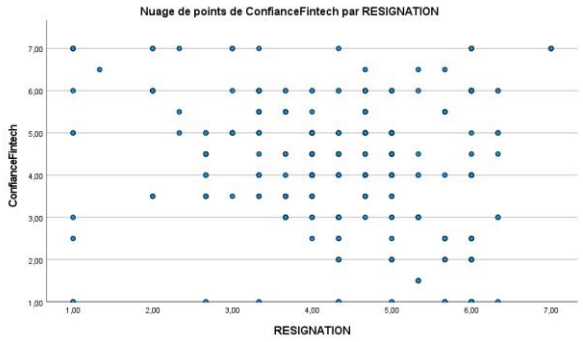

Nuage de points de CLARTÉ par RESIGNATION
CLARTÉ
RESIGNATION

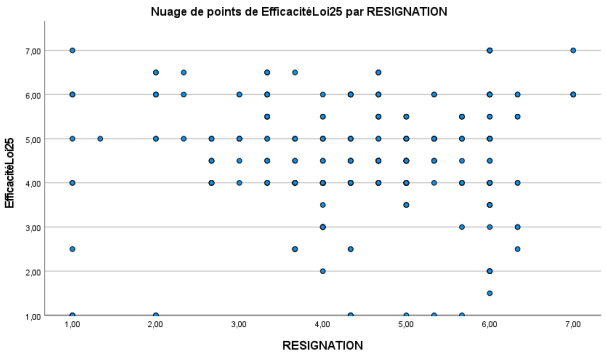

Nuage de points de PERTINENCE par RESIGNATION
PERTINENCE
RESIGNATION

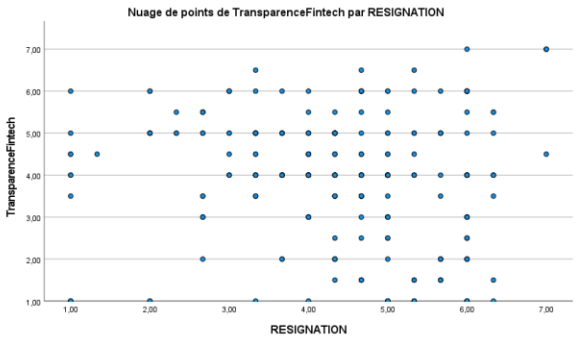

Nuage de points de CONSENTEMENT par RESIGNATION
CONSENTEMENT
RESIGNATION

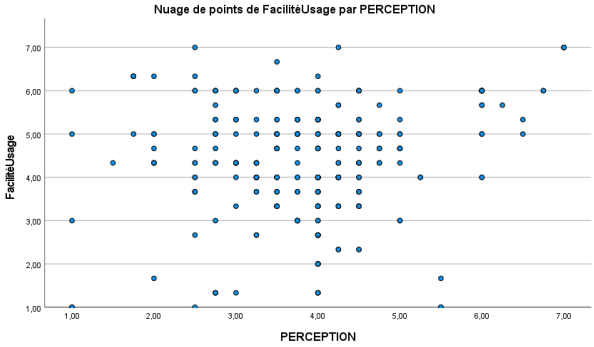

Nuage de points de PERCEPTION par RESIGNATION
PERCEPTION
RESIGNATION

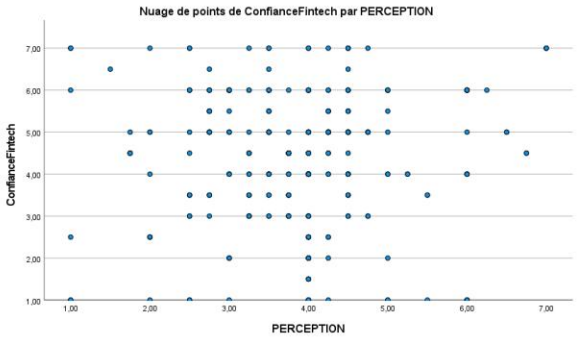

Nuage de points de FacilitéUsage par RESIGNATION
FacilitéUsage
RESIGNATION

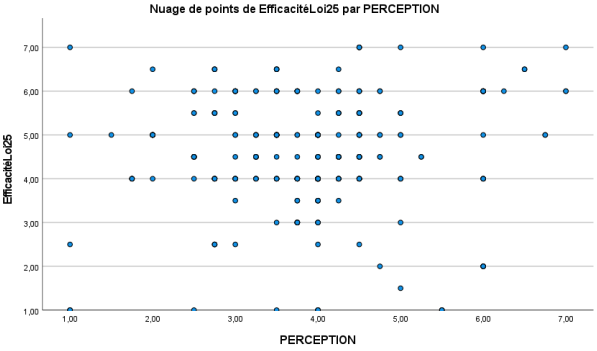

Nuage de points de ConfianceFintech par RESIGNATION
ConfianceFintech
RESIGNATION

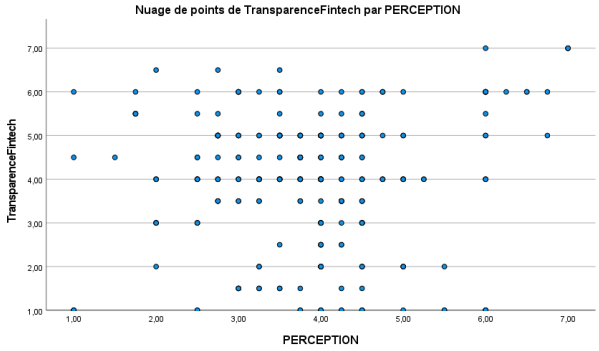

Nuage de points de EfficacitéLoi25 par RESIGNATION
EfficacitéLoi25
RESIGNATION


Nuage de points de TransparenceFintech par RESIGNATION
TransparenceFintech
RESIGNATION
1,00
2,00
3,00
4,00
5,00
6,00
7,00


Nuage de points de FacilitéUsage par PERCEPTION
FacilitéUsage
PERCEPTION
1,00
2,00
3,00
4,00
5,00
6,00
7,00


Nuage de points de ConfianceFintech par PERCEPTION
ConfianceFintech
PERCEPTION
1,00
2,00
3,00
4,00
5,00
6,00
7,00


Nuage de points de EfficacitéLoi25 par PERCEPTION
EfficacitéLoi25
PERCEPTION
1,00
2,00
3,00
4,00
5,00
6,00
7,00


Nuage de points de TransparenceFintech par PERCEPTION
TransparenceFintech
PERCEPTION
1,00
2,00
3,00
4,00
5,00
6,00
7,00

Intervalles de confiance

	Corrélation de Pearson	Sig. (bilatérale)	95% intervalles de confiance (bilatéral)[a] Inférieur	Supérieur
PERCEPTION - RESIGNATION	,573	<,001	,491	,644
PERCEPTION - ATTITUDE	,264	<,001	,155	,366
PERCEPTION - UTILITÉ	,247	<,001	,137	,350
PERCEPTION - CLARTÉ	,338	<,001	,234	,435
PERCEPTION - PERTINENCE	,372	<,001	,270	,465
PERCEPTION - CONSENTEMENT	,360	<,001	,257	,455
PERCEPTION - FacilitéUsage	,180	,002	,068	,287
PERCEPTION - ConfianceFintech	,013	,829	-,101	,126
PERCEPTION - EfficacitéLoi25	,063	,277	-,051	,175
PERCEPTION - TransparenceFintech	,079	,171	-,034	,191
RESIGNATION - ATTITUDE	,157	,006	,045	,266
RESIGNATION - UTILITÉ	,118	,041	,004	,228
RESIGNATION - CLARTÉ	,193	<,001	,081	,299
RESIGNATION - PERTINENCE	,188	,001	,076	,295
RESIGNATION - CONSENTEMENT	,086	,138	-,028	,197
RESIGNATION - FacilitéUsage	,051	,375	-,062	,164
RESIGNATION - ConfianceFintech	-,196	<,001	-,302	-,084
RESIGNATION - EfficacitéLoi25	,031	,590	-,082	,144
RESIGNATION - TransparenceFintech	-,104	,073	-,214	,010
ATTITUDE - UTILITÉ	,635	<,001	,562	,698
ATTITUDE - CLARTÉ	,490	<,001	,398	,571
ATTITUDE - PERTINENCE	,501	<,001	,410	,581
ATTITUDE - CONSENTEMENT	,456	<,001	,361	,541
ATTITUDE - FacilitéUsage	,355	<,001	,251	,449
ATTITUDE - ConfianceFintech	,103	,074	-,010	,214
ATTITUDE - EfficacitéLoi25	,147	,011	,034	,255
ATTITUDE - TransparenceFintech	,241	<,001	,131	,345
UTILITÉ - CLARTÉ	,647	<,001	,575	,708
UTILITÉ - PERTINENCE	,592	<,001	,512	,660
UTILITÉ - CONSENTEMENT	,549	<,001	,464	,623
UTILITÉ - FacilitéUsage	,320	<,001	,214	,418
UTILITÉ - ConfianceFintech	,041	,478	-,073	,154
UTILITÉ - EfficacitéLoi25	,196	<,001	,084	,302
UTILITÉ - TransparenceFintech	,201	<,001	,090	,307
CLARTÉ - PERTINENCE	,717	<,001	,656	,767
CLARTÉ - CONSENTEMENT	,515	<,001	,426	,593
CLARTÉ - FacilitéUsage	,377	<,001	,275	,470
CLARTÉ - ConfianceFintech	,048	,408	-,066	,160
CLARTÉ - EfficacitéLoi25	,155	,007	,042	,263
CLARTÉ - TransparenceFintech	,259	<,001	,150	,361
PERTINENCE - CONSENTEMENT	,525	<,001	,438	,602
PERTINENCE - FacilitéUsage	,327	<,001	,221	,424
PERTINENCE - ConfianceFintech	,010	,858	-,103	,123
PERTINENCE - EfficacitéLoi25	,184	,001	,072	,291
PERTINENCE - TransparenceFintech	,174	,002	,062	,282
CONSENTEMENT - FacilitéUsage	,374	<,001	,272	,467
CONSENTEMENT - ConfianceFintech	,115	,047	,002	,225
CONSENTEMENT - EfficacitéLoi25	,190	<,001	,079	,297
CONSENTEMENT - TransparenceFintech	,256	<,001	,147	,359
FacilitéUsage - ConfianceFintech	,525	<,001	,437	,602
FacilitéUsage - EfficacitéLoi25	,477	<,001	,384	,560
FacilitéUsage - TransparenceFintech	,471	<,001	,377	,554
ConfianceFintech - EfficacitéLoi25	,575	<,001	,493	,646
ConfianceFintech - TransparenceFintech	,595	<,001	,516	,663
EfficacitéLoi25 - TransparenceFintech	,588	<,001	,508	,657

a. L'estimation est basée sur la transformation r-à-z de Fisher avec ajustement de biais.

ANNEXE D : TEST POST HOC DIFFÉRENCES DE BANNIÈRES

Comparaisons multiples :

Différence significative de Tukey

Variable dépendante	(I) Goal	(J) Goal	Différence moyenne (I-J)	Erreur standard	Sig.	95% Intervalle de confiance	
						Borne inférieure	Borne supérieure
RESIGNATION	Acc. avec politique	Acc. ou paramétrer	,4667	,24012	,378	-,2222	1,1555
		Accepter tout	-,0267	,24012	1,000	-,7155	,6622
		Cons. éclairé	2,9733*	,24012	<,001	2,2845	3,6622
		Cookies essentiels	-,0800	,24012	,999	-,7688	,6088
		Sans bannière	,4800	,24012	,345	-,2088	1,1688
	Acc. ou paramétrer	Acc. avec politique	-,4667	,24012	,378	-1,1555	,2222
		Accepter tout	-,4933	,24012	,314	-1,1822	,1955
		Cons. éclairé	2,5067*	,24012	<,001	1,8178	3,1955
		Cookies essentiels	-,5467	,24012	,207	-1,2355	,1422
		Sans bannière	,0133	,24012	1,000	-,6755	,7022
	Accepter tout	Acc. avec politique	,0267	,24012	1,000	-,6622	,7155
		Acc. ou paramétrer	,4933	,24012	,314	-,1955	1,1822
		Cons. éclairé	3,0000*	,24012	<,001	2,3112	3,6888
		Cookies essentiels	-,0533	,24012	1,000	-,7422	,6355
		Sans bannière	,5067	,24012	,285	-,1822	1,1955
	Cons. éclairé	Acc. avec politique	-2,9733*	,24012	<,001	-3,6622	-2,2845
		Acc. ou paramétrer	-2,5067*	,24012	<,001	-3,1955	-1,8178
		Accepter tout	-3,0000*	,24012	<,001	-3,6888	-2,3112
		Cookies essentiels	-3,0533*	,24012	<,001	-3,7422	-2,3645
		Sans bannière	-2,4933*	,24012	<,001	-3,1822	-1,8045
	Cookies essentiels	Acc. avec politique	,0800	,24012	,999	-,6088	,7688
		Acc. ou paramétrer	,5467	,24012	,207	-,1422	1,2355
		Accepter tout	,0533	,24012	1,000	-,6355	,7422
		Cons. éclairé	3,0533*	,24012	<,001	2,3645	3,7422
		Sans bannière	,5600	,24012	,185	-,1288	1,2488
	Sans bannière	Acc. avec politique	-,4800	,24012	,345	-1,1688	,2088
		Acc. ou paramétrer	-,0133	,24012	1,000	-,7022	,6755
		Accepter tout	-,5067	,24012	,285	-1,1955	,1822
		Cons. éclairé	2,4933*	,24012	<,001	1,8045	3,1822
		Cookies essentiels	-,5600	,24012	,185	-1,2488	,1288
PERCEPTION	Acc. avec politique	Acc. ou paramétrer	-,1450	,20488	,981	-,7327	,4427
		Accepter tout	-,4050	,20488	,358	-,9927	,1827
		Cons. éclairé	1,8500*	,20488	<,001	1,2623	2,4377
		Cookies essentiels	-,2200	,20488	,891	-,8077	,3677
		Sans bannière	,3500	,20488	,527	-,2377	,9377
	Acc. ou paramétrer	Acc. avec politique	,1450	,20488	,981	-,4427	,7327
		Accepter tout	-,2600	,20488	,802	-,8477	,3277
		Cons. éclairé	1,9950*	,20488	<,001	1,4073	2,5827
		Cookies essentiels	-,0750	,20488	,999	-,6627	,5127
		Sans bannière	,4950	,20488	,154	-,0927	1,0827
	Accepter tout	Acc. avec politique	,4050	,20488	,358	-,1827	,9927
		Acc. ou paramétrer	,2600	,20488	,802	-,3277	,8477
		Cons. éclairé	2,2550*	,20488	<,001	1,6673	2,8427
		Cookies essentiels	,1850	,20488	,946	-,4027	,7727
		Sans bannière	,7550*	,20488	,004	,1673	1,3427
	Cons. éclairé	Acc. avec politique	-1,8500*	,20488	<,001	-2,4377	-1,2623
		Acc. ou paramétrer	-1,9950*	,20488	<,001	-2,5827	-1,4073
		Accepter tout	-2,2550*	,20488	<,001	-2,8427	-1,6673
		Cookies essentiels	-2,0700*	,20488	<,001	-2,6577	-1,4823
		Sans bannière	-1,5000*	,20488	<,001	-2,0877	-,9123
	Cookies essentiels	Acc. avec politique	,2200	,20488	,891	-,3677	,8077
		Acc. ou paramétrer	,0750	,20488	,999	-,5127	,6627
		Accepter tout	-,1850	,20488	,946	-,7727	,4027
		Cons. éclairé	2,0700*	,20488	<,001	1,4823	2,6577
		Sans bannière	,5700	,20488	,063	-,0177	1,1577
	Sans bannière	Acc. avec politique	-,3500	,20488	,527	-,9377	,2377
		Acc. ou paramétrer	-,4950	,20488	,154	-1,0827	,0927
		Accepter tout	-,7550*	,20488	,004	-1,3427	-,1673
		Cons. éclairé	1,5000*	,20488	<,001	,9123	2,0877
		Cookies essentiels	-,5700	,20488	,063	-1,1577	,0177

BIBLIOGRAPHIE

Acquisti, A. (2011). Les comportements de vie privée face au commerce électronique: Une économie de la gratification immédiate. *Réseaux*, 167, 105-130. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/res.167.0105

Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 5th ACM conference on Electronic commerce (pp. 21-29). Récupéré de https://www.academia.edu/download/30777892/Acquisti04.pdf

Amarnath, D.D., Jaidev (2021), U.P. Toward an integrated model of consumer reactance: a literature analysis. *Manag Rev Q* **71**, 41–90. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1007/s11301-020-00180-y

Amina, M. E. Z. Z. A. R. A., & Smail, O. U. I. D. D. A. D. (2022). Exploration de la communauté virtuelle marocaine de voyage «j'ai testé ce voyage»: résultats de l'approche netnographique. *Proceedings of Engineering & Technology*, *68*, 249-266.

Anthony Smith (2024, février 22). Ce que nous entendons par « facilité d'utilisation » meilleures pratiques affaires et technologies. [Billet de blogue]. Récupéré de https://www.insightly.com/blog/saas-ease-of-use/

Anjum, A., & Priya, R. M. (2024). Impact of AI-driven digital marketing on data privacy and consumer behavior: An SEM study. *IUP Journal of Marketing Management, 23*(4), 75-97. Retrieved from https://www.proquest.com/scholarly-journals/impact-ai-driven-digital-marketing-on-data/docview/3158175797/se-2

Ann Cavoukian, Privacy by Design (2013), en ligne : Commissaire à l'information et à la protection de la vie privée de l'Ontario. P 2-3. Récupéré de https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

Atlassian. (2023), *California Consumer Privacy Act*, Récupéré de https://www.atlassian.com/fr/trust/compliance/resources/ccpa

Autorité des marchés financiers, (2024, 20 avril). Fintech. [Billet de blogue]. Récupéré de https://lautorite.qc.ca/professionnels/fintech-technologie-financiere

Baker S.M. (2006). Consumer normalcy: Understan - ding the value of shopping through narratives of consumers with visual impairments. Journal of Retailing, 82(1): 37-50.

Baker S.M., Gentry J.W. et Rittenburg T.L. (2005). Building understanding of the domain of consu - mer vulnerability. Journal of Macromarketing 25(2): 128 -139.

Barth, S. et De Jong, MD (2017). Le paradoxe de la vie privée – Enquête sur les écarts entre les préoccupations exprimées en matière de confidentialité et le comportement réel en ligne – Une revue systématique de la littérature. Télématique et informatique , 34 (7), 1038-1058.

Belky F., (2023). Comment les institutions financières peuvent utiliser efficacement les réseaux sociaux pour se conformer à la loi C-11, améliorer l'engagement avec la génération Z, offrir une expérience client authentique et se démarquer face à la concurrence des fintechs ? (Activité de Synthèse ESG8100). Université du Québec à Montréal.

Blut, M., Chong, A. Y. L., Tsigna, Z., & Venkatesh, V. (2022). Meta-Analysis of the Unified Theory of Acceptance and Use of Technology (UTAUT): Challenging its Validity and Charting a Research Agenda in the Red Ocean. *Journal of the Association for Information Systems*, 23(1), 13–95. https://doi.org/10.17705/1JAIS.00719

Brehm JW (1966) Une théorie de la réactance psychologique. Presse académique, Oxford, Angleterre

Brehm SS, Brehm JW (1981) Réactance psychologique : une théorie de la liberté et du contrôle. Presse académique, New York

Brideau, I., Brosseau, L., Brown, G. d., Lord, F., & Ménard, M. (2022, février 17). Résumé législatif du projet de loi C-11 : Loi modifiant la Loi sur la radiodiffusion et apportant 93 des modifications connexes et corrélatives à d'autres lois. Récupéré de https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/LegislativeSummaries/441C11E

Bruner, G. C. (2017). *Marketing scales handbook. Volume 9, Multi-item measures for consumer insight research*. GCBII Productions, LLC.

Buabeng-Andoh, C. (2018), "*Predicting students' intention to adopt mobile learning: a combination of theory of reasoned action and technology acceptance model*", Journal of Research in Innovative Teaching and Learning, Vol. 11 No. 2, pp. 178-191, doi: 10.1108/JRIT-03-2017-0004.

Cachecho M., Prom Tep S., Parada A., Gholami V. (2022). Fintech : Conjuger innovation éthique et consommation. *Cahier de recherche de la Chaire Fintech AMF – Finance Montréal.* Récupéré de *https://chairefintech.uqam.ca/wp-content/uploads/2022/04/Cahierderecherche_MayaSandrineetcollaborateurs.pdf*

Cadario, R., Butori, R. et Parguel, B. (2017) . Chapitre 3. Choisir le design expérimental. Méthode expérimentale : analyses de modération et médiation. (p. 49 -59). De Boeck Supérieur. https://shs.cairn.info/methode-experimentale-analyses-de-moderation--9782807313378-page-49?lang=fr.

Cassell J, Kerr A, Levine S, (2020, 24 novembre). Comment le projet de loi C-11 changera-t-il la manière dont les organisations traitent les renseignements personnels? [Billet de blogue]. Récupéré de https://www.nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/c826be49/comment-le-projet-de-loi-c-11-changera-t-il-la-maniere-dont-les-organisations

Chan-Olmsted, S., Chen, H. and Kim, H.J. (2024, 3 septembre), "In smartness we trust: consumer experience, smart device personalization and privacy balance", *Journal of Consumer Marketing*,

Vol. 41 No. 6, pp. 597-609. https://doi-org.proxy.bibliotheques.uqam.ca/10.1108/JCM-12-2021-5072

Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research*, *16*(1), 64–73. https://doi.org/10.2307/3150876Columbus, L. (2014). 2014: The Year Big Data Adoption Goes Mainstream in the Enterprise. Forbes (January 12). Récupéré de http://www. forbes. com/sites/louiscolumbus/20, 1(4), 0.

Christine Dufour, (Automne 2022), SCI6005 Information numérique et informatique documentaire (A2022) : *Acceptation et utilisation des technologies (perspective micro)* EBSI, UdeM. Récupéré de : https://cours.ebsi.umontreal.ca/sci6005/a2022/co/appropriation_ti.html

Cohu Rémi, (2023). *Un numérique responsable pour tous*. (Mémoire de thèse). Haute École de Gestion Valais. Récupéré de https://sonar.ch/global/documents/326846

Commissariat à la protection de la vie privée au Canada (2023, mars 2023). *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2022-2023*. Récupéré de https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2023/por_ca_2022-23/#toc2-1

Commission d'accès à l'information du Québec, (2023, 08 février), *Entreprises : vers la conformité à la Loi sur le privé*. Récupéré de https://www.cai.gouv.qc.ca/documents/CAI_Guide_obligations_entreprises_vf.pdf

Cordeiro T. & Weevers I., (2016, 18 march). Design is No Longer an Option - User Experience (UX) in FinTech. *The FinTech Book.* Récupéré de *https://doi-org.proxy.bibliotheques.uqam.ca/10.1002/9781119218906.ch9*

Cronbach, L. J. (1951). Coefficient alpha and the internai structure of tests. Psychometrika, 16(3), 297-334.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. Récupéré de https://doi.org/10.2307/249008

Deb, M. and Lomo-David, E. (2014), "*An empirical examination of customers' adoption of m- banking in India*", Marketing Intelligence and Planning, Vol. 32 No. 4, pp. 475-494, doi: 10.1108/MIP-07-2013-0119.

Deslée, A. (2023). La vie privée en ligne: utopie ou réalité? Comprendre la vulnérabilité perçue relative aux données personnelles. Décision Marketing, (3), 11-37. Récupéré de https://www.cairn.info/revue-decisions-marketing-2023-3-page-11.htm

Designers Éthiques (2024). Designers éthiques. [Billet de blogue]. Récupéré de https://beta.designersethiques.org/#top

Division de l'information, (2018). Protection de la vie privée et Archives publiques, *Manuel sur l'accès à l'information et la protection à la vie privée*. Récupéré de https://files.ontario.ca/books/mgcs-foi-privacy-manual-fr-2021-09-02.pdf

Dorfleitner, G., Hornuf, L., Schmitt, M., Weber, M. (2017). Définition de Fintech et description de l'industrie Fintech. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1007/978-3-319-54666-7_2

Fard A., (2024). Tendances de conception Fintech UX pour 2024. [Billet de blogue]. Récupéré de https://adamfard.com/blog/fintech-ux-trends

Fathom4sight, Finance Montreal, Station Fintech Montreal (2024). Rapport Fintech Québec Semestriel 2024. Récupéré de https://www.stationfintech.com/fr/lire-une-nouvelle-et-publication/decouvrez-le-rapport-fintech-quebec-2023

Fitzegerald S., (2019). Carte du marché canadien de la technologie financière. Récupéré de https://www.pwc.com/ca/fr/industries/technology/canadian-fintech-market-map.html

Gardé A. (2024, 05 février). Tout savoir pour concevoir une bannière de consentement performante. [Billet de blogue]. Récupéré de https://www.adviso.ca/blog/conseils/concevoir-une-banniere-de-consentement-performante

Gendreau, P (2023). *GAFAM : le monstre à cinq têtes*. Les Éditions Écosociété

Gouvernement. (2020, Décembre 2). Projet de loi C-11 : Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois. Récupéré de https://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/c11.html

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (p. 534). ACM. Récupéré de 10.1145/3173574.3174108

Hill, R. P., & Sharma, E. (2020). Consumer vulnerability. Journal of Consumer Psychology, 30(3), 551-570.

Ho, F. N., Ho-Dac, N., & Huang, J. S. (2023). The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence. *SAGE Open*, *13*(3). https://doi-org.proxy.bibliotheques.uqam.ca/10.1177/21582440231181395 (Original work published 2023)

Hong W., Chan F.K.Y. et Thong J.Y.L. (2019). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Pers - pective. Journal of Business Ethics 168: 539- 564.

Houle Audrey, (2020). La protection du consommateur à l'ère du marketing intelligent : Une approche comparative France-Québec. Récupéré de https://hdl.handle.net/20.500.11794/67892

Huu Binh, N. (2014). Fiabilité et validité du Modèle d'acceptation de la technologie (TAM) dans le contexte d'apprenants vietnamiens du français comme langue étrangère face aux TIC. Revue

internationale des technologies en pédagogie universitaire /International Journal of Technologies in Higher Education, 11(3), 38–50. https://doi.org/10.7202/1035702ar

Humida, T., Al Mamun, M.H. and Keikhosrokiani, P. (2022), "*Predicting behavioral intention to use e-learning system: a case-study in Begum Rokeya University, Rangpur, Bangladesh*", Education and Information Technologies, Vol. 27 No. 2, pp. 2241-2265, doi: 10.1007/s10639-021-10707-9.

Jaillet, A. et Mabilon-Bonfils, B. (2021) . Chapitre 1. Qu'est-ce qu'une revue de littérature ? Je réussis mon mémoire de Master MEEF 1er degré : professeur des écoles. (p. 42 -42). Vuibert. https://shs.cairn.info/je-reussis-mon-memoire-de-master-meef--9782311210309-page-42?lang=fr.

Kouakou K.S., (2015). Adoption des réseaux sociaux numériques par les bibliothécaires des universités ivoiriennes : Une approche par l'UTAUT. *Les Cahiers du numérique, Apport de la gestion documentaire à la gouvernance de l'information*, 11 (2), pp.167-202. Récupéré de https://auf.hal.science/hal-01591731/document

KPMG, (2024). Pulse of Fintech H2'23, Global analysis of Fintech Funding. Récupéré de http://kpmg.com/fintechpulse

Kumar, J. et Rani, V. (2024). Enquête sur la dynamique de l'adoption des FinTech : une étude empirique du point de vue des services bancaires mobiles. *Journal of Economic and Administrative Sciences*. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1108/JEAS-12-2023-0334

Lai PC. (2017). La revue de la littérature sur les modèles et théories d'adoption de la technologie pour la technologie de nouveauté. *JISTEM - Journal de gestion des systèmes d'information et des technologies Vol. 14, n° 1, p. 21 à 38.* Récupéré de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005897

Larbaigt J. (2020). Améliorer l'utilité, l'utilisabilité et l'acceptabilité de solutions technologiques innovantes et interopérables en viticulture. Psychologie. Université Toulouse le Mirail - Toulouse II. Récupéré de https://theses.hal.science/tel-03368102v1/document

Lau, A. (2017). *La protection intégrée des renseignements: permettre au consommateur de faire des choix et de donner un consentement significatifs en matière de confidentialité*. Le Centre pour la défense de l'intérêt public. Récupéré de https://www.piac.ca/wp-content/uploads/2017/08/PIAC-THE-PRIVACY-BOX-OCA-REPORT-June-2017-FR-FINAL2.pdf

Lebrun, Pierre-bruce. (2015). La vie privée. *Empan*, 100, 168-172. https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/empa.100.0168

Lemoine, J-F. (2012). Pour une présentation du concept d'atmosphère des sites web et de ses effets sur le comportement des internautes. *Marché et organisations*, 15, 169-180. https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/maorg.015.0169

Leprince, C. (2023, 11 octobre). Faire évoluer sa pratique média dans un contexte de marketing respectueux de la vie privée. [Billet de blogue]. Récupéré de https://www.adviso.ca/blog/conseils/faire-evoluer-media-dans-un-contexte-marketing-respectueux-de-la-vie-privee?

Liendle, M. (2012). Vulnérabilité. Dans M. Formarier et L. Jovic Les concepts en sciences infirmières : 2ème édition (p. 304-306). Association de Recherche en Soins Infirmiers. https://doi.org/10.3917/arsi.forma.2012.01.0304.

Liu , Y. , Saleem , S. , Shabbir , R. , Shabbir , MS , Irshad , A. et Khan , S. (2021), «*La relation entre la responsabilité sociale des entreprises et la performance financière : un rôle modéré de la technologie fintech*»,Environmental Science and Pollution Research, vol. 28n° 16, pp. 20174-20187, doi:10.1007/s11356-020-11822-9.

Malhotra, N. (2011). Études marketing (6e éd.). Paris: Pearson Education France

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

Martin K.D., Kim J.J., Palmatier R.W.,Steinhoff L., Stewart D.W., Walker B.A., Wang Y. et Weaven S.K. (2020). Data Privacy in Retail. Journal of Retailing 96(4): 474-489.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

McKinsey&Compagny (2024, 16 April). Springtime for Canada's fintech industry? Récupéré de https://www.mckinsey.com/ca/overview/springtime-for-canadas-fintech-industry#/

Mission RGPD, 2023, *Qu'est ce le RGPD ? Tout comprendre* ! Récupéré de https://www.mission-rgpd.com/quest-ce-que-le-rgpd/

Mollen, A. and Wilson, H. (2010), "*Engagement, telepresence and interactivity in online consumer experience: reconciling scholastic and managerial perspectives*", Journal of Business Research, Vol. 63 Nos 9-10, pp. 919-925, doi: 10.1016/j.jbusres.2009.05.014.

Mordor Intelligence, (2024), Analyse de la taille et de la part du marché des technologies financières – Tendances et prévisions de croissance (2024 – 2029). Récupéré de https://www.mordorintelligence.com/fr/industry-reports/global-fintech-market

Nguyen, Y.T.H., Tapanainen, T. and Nguyen, H.T.T. (2022), "*Reputation and its consequences in Fintech services: the case of mobile banking*", International Journal of Bank Marketing, Vol. 40 No. 7, pp. 1364-1397, doi: 10.1108/IJBM-08-2021-0371.

Oliver M. (2024, 19 march), Exploring the Connections Between Sustainability and UX Design. [Billet de blogue]. Récupéré de https://www.loop11.com/exploring-the-connections-between-sustainability-and-ux-design/?utm_source=loop11&utm_campaign=fab-ux-five&ref=loop11

Olson, C. L. 1974. Comparative Robustness of Six Tests in Multivariate Analysis of Variance. *Journal of the American Statistical Association,* 69:348, 894-908.

Oursel H., Ravenel M., Meslin T., Panchout É., (2023). Étude de l'impact de l'interface et expérience utilisateur sur la prise de décision.

Portes A., Cases A.-S. et N'Goala G. (2017). Vers une définition de la transparence perçue de la relation client sur les canaux digitaux. Management & Avenir 94(4): 105-129.

Prom Tep, S., Rajaobelina, L., Archand, M., Brun, Is. et Ricard, L. (2022). Amélioration de l'expérience utilisateur (UX) en contexte d'intelligence artificielle : le cas du chatbot en fintech. *Cahier de recherche de la Chaire Fintech AMF – Finance Montréal*, (p. 1-58). Récupéré de https://chairefintech.uqam.ca/wp-content/uploads/2022/03/CahierSandrineLovaetcollaborateurs_Chatbot.pdf

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., et Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science 50(6): 1299-1323

Quilliou-Rioual, M. (mars 2023). Numérique, éthique et GAFAM sont-ils compatibles dans les pratiques professionnelles en travail social ? *Sociographe*, *81*(1), 89. https://doi.org/10.3917/graph1.081.0089

Robert V., (2023). Éthique de la gestion du consentement au traitement de données personnelles : une analyse au prisme des Dark patterns. *Actes du XLI Congrès INFORSID, La Rochelle, France,* Pages 133-148, Récupéré de http://inforsid.fr/actes/2023/INFORSID_2023_p133-148.pdf

Rowland, W. (2006). *La soif des entreprises*. Éditions Hurtubise HMH.

Saerens Pierre, 2019. *La connaissance des consommateurs du règlement général sur la protection des données (RGPD) affecte-t-elle les sentiment d'impuissance, vulnérabilité des consommateurs face aux publicités en ligne personnalisées? Cette connaissance peut-elle avoir des effets sur la*

réactance des consommateurs face aux publicités en ligne personnalisées?. (Mémoire de recherche). Louvain School of Management. Récupéré de http://hdl.handle.net/2078.1/thesis:25872

Schueffel P. (2016). *Taming the Beast: A Scientific Definition of Fintech*. Journal of Innovation Management 4, 32-54. Récupéré de https://journalsojs3.fe.up.pt/index.php/jim/article/view/2183-0606_004.004_0004

Sekulic N., (2022. 28 march). Universal, Inclusive, and Equity-Focused Design: Why They are Critical for Your Website. [Billet de blogue]. Récupéré de https://www.loop11.com/universal-inclusive-and-equity-focused-design-why-they-are-critical-for-your-website/

Selma M.B., Labouze-Nasica A., Chebbi H. (2021). Dynamique de la relation Fintech-grandes institutions financières à l'ère du Covid-19. *Cahier de recherche de la chaire fintech amf – finance Montréal.* Récupéré de https://chairefintech.uqam.ca/wp-content/uploads/2021/03/ChaireFintech_Cahier_BenSelmaLabouze-NasicaChebbi_Mars2021.pdf

Singh, S., Sahni, M.M. and Kovid, R.K. (2020), "*What drives FinTech adoption? A multi- method evaluation using an adapted technology acceptance model*", Management Decision, Vol. 58 No. 8, pp. 1675-1697, ISSN: 0025-1747, doi: 10.1108/MD-09-2019-1318.

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design. Dark patterns in cookie consents for online news outlets.

Statistique Canada, 20 décembre 2023, *Tableau 17-10-0009-01 Estimations de la population, trimestrielles*. Récupéré de https://doi.org/10.25318/1710000901-fra

Susilo, A.Z., Prabowo, M.I., Taman, A., Pustikaningsih, A. and Samlawi, A. (2019), "*A comparative study of factors affecting user acceptance of go-pay and OVo as a feature of Fintech application*", Procedia Computer Science, Vol. 161, pp. 876-884, doi: 10.1016/j.procs.2019.11.195.

Stewart, D. W. (1981). The application and misapplication of factor analysis in marketing research. *Journal of Marketing Research, 18*(1), 51–62. https://doi.org/10.2307/3151313

Tibère, V., Rasche, C. (2017). Modèles de modèles perturbateurs des Fintechs : éléments d'information, tendances et stratégies. *Bankmagazin*. https://doi-org.proxy.bibliotheques.uqam.ca/10.1007/978-3-658-14187-5_1

Tremblay A, (2023, 30 janvier), Comprendre les grands principes de la nouvelle Loi 25 au Québec. [Billet de blogue]. Récupéré de https://www.tink.ca/perspectives/comprendre-les-grands-principes-de-la-nouvelle-loi-25-au-quebec#

Usabilis. (2019, 23 mars). Design éthique ou quelle est la responsabilité du designer ? Récupéré de https://www.usabilis.com/design-ethique/

Utz, C., Degeling, M., Gahl, S., Schaub, F., Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS 19). *Association for Computing Machinery*, New York, NY, USA, 973990

Veilleux, M. *et coll.* (2020). Visualiser les parcours cognitifs et émotionnels d'un utilisateur : un cas Fintech. HCII 2020. Notes de cours en informatique, vol 12200. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1007/978-3-030-49713-2_38

Victor Papanek, (1970), Design for the real world, Human Ecology and Social change

Vuxe. (2018, 05 novembre). Qu'est-ce que le Design Éthique? [Billet de blogue]. Récupéré de https://www.vuxe.fr/le-design-ethique-mais-quest-ce-que-cest-au-juste/

Yergeau, E. et Poirier, M. (2023). *SPSS à l'UdeS*. Récupéré de : <http://spss.espaceweb.usherbrooke.ca>.

Yin J., (2023, 28 mars). La face cachée du design UX: les Dark patterns. Expérience Utilisateur, Strategie Marketing. [Billet de blogue]. Récupéré de https://digital.hec.ca/blog/la-face-cachee-du-design-ux-les-dark-patterns/

Zghal, M. & Aouinti, N. (2010). Le rôle des facteurs situationnels et personnels dans l'explication de la réalisation d'un achat impulsif : Une application du modèle S.O.R.. *La Revue des Sciences de Gestion*, 242, 113-121. https://doi-org.proxy.bibliotheques.uqam.ca/10.3917/rsg.242.0113