HEC MONTRÉAL

Le comportement sécuritaire pour la protection de l'actif informationnel : mieux comprendre et définir le concept

Par

Layla Jasic

Sciences de la gestion
(Spécialisation Transformation numérique)

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

Décembre 2021
© Layla Jasic, 2021

Sommaire

Avec le nombre grandissant d'incidents survenus au cours des dernières années, la sécurité de l'information a commencé à devenir un enjeu de plus en plus important pour les organisations. Afin de protéger leur actif informationnel, celles-ci investissent des sommes considérables dans des solutions technologiques, alors que la littérature scientifique et professionnelle révèle que c'est le facteur humain qui représente la cause d'incidents la plus fréquente. Ainsi, on mentionne le comportement sécuritaire des employés comme un moyen efficace pour atténuer l'impact des incidents de sécurité. Toutefois, un survol des écrits ne permet pas de comprendre clairement ce qu'est un comportement sécuritaire, tant il y a de variété dans la définition et la description de ce concept.

Devant ce constat, ce mémoire s'intéresse à clarifier et à définir ce qu'est un comportement sécuritaire pour la protection de l'actif informationnel. Pour ce faire, une revue de littérature systématique a été effectuée dans le but de recueillir et mettre en commun les connaissances existantes, et faire ressortir les éléments essentiels à la compréhension et à la définition du comportement sécuritaire. Au terme de cet exercice rigoureux, plusieurs constats émergent : (1) le comportement sécuritaire est un concept flou qui souffre de l'absence d'une définition claire, (2) il n'y a pas de terme commun pour désigner le concept, (3) plusieurs contradictions existent dans la manière de l'étudier et (4) le concept de comportement sécuritaire comporte plusieurs dimensions. La présente recherche a également permis d'identifier les principales caractéristiques du comportement sécuritaire, déterminer les relations entre ses dimensions et, finalement, proposer une définition claire et concise du concept. D'autres chercheurs pourront ensuite valider empiriquement cette définition et développer un instrument de mesure fiable.

Mots-clés : comportement sécuritaire, sécurité de l'information, protection de l'actif informationnel, définition, revue de littérature systématique

Remerciements

Je tiens tout d'abord à remercier ma directrice, Alina Dulipovici, pour sa générosité, sa patience et sa disponibilité tout au long de la rédaction de ce mémoire. Elle a toujours été de bon conseil et m'a proposé tant de bonnes idées pour me permettre d'avoir un travail à la hauteur de mes attentes. Grâce à elle, j'ai appris à appliquer la plus grande rigueur à ma recherche et j'ai pu faire de nombreux apprentissages en cours de route. Alina n'est pas seulement une professeure extraordinaire, c'est une femme au grand cœur et je me sens privilégiée d'avoir pu travailler avec elle.

J'aimerais également remercier Guy Paré, qui m'a été d'une aide précieuse au cours de ma toute première session à HEC. Il m'a d'abord permis de trouver ma directrice de mémoire, mais il a surtout su me transmettre sa passion pour la recherche et m'a fait réaliser que je pouvais accomplir de grandes choses dans le cadre de ma maîtrise.

Ensuite, un grand merci à tous les professeurs du département TI qui m'ont enseigné au cours des dernières années, ils ont contribué à faire de mon passage à la maîtrise une expérience hautement enrichissante. Merci aussi à mes collègues de la M.Sc. pour leurs encouragements.

Je veux également remercier mes amis pour leur soutien et leur curiosité à l'égard de mon mémoire. Un merci spécial à Lili pour sa compagnie et ses conseils, en mode virtuel ou en personne. Entre les discussions plus sérieuses et les fous rires, nos interactions ont contribué à faire de mon processus de rédaction une expérience encore plus agréable. Merci aussi à Sandra pour nos longues marches qui m'ont permis de m'aérer l'esprit.

Enfin, merci à ma famille pour son soutien et son aide durant cette aventure.

Table des matières

Sommaire ..... **i**
Remerciements ..... **ii**
Liste des tableaux ..... **v**
Liste des figures ..... **vi**
Chapitre 1. Problématique **1**
1.1 Présentation de la problématique 1
1.2 Pertinence de la problématique 3
1.3 Objectif et question de recherche 6
1.4 Structure du mémoire 7
Chapitre 2. État des connaissances autour du concept de comportement sécuritaire **8**
2.1 Le comportement sécuritaire et la protection de l'actif informationnel 9
2.2 Comportement sécuritaire : un concept flou 15
2.2.1 Termes utilisés 16
2.2.2 Définitions 17
2.2.3 Dimensions 18
2.2.4 Dimensions indépendantes ou interdépendantes? 20
2.3 Conclusion 22
Chapitre 3. Méthodologie de recherche **24**
3.1 Choix de la méthodologie de recherche 24
3.2 Étape 1 : Recherche de la littérature 25
3.3 Étape 2 : Tri des articles 27
3.4 Étape 3 : Extraction de données 30
3.5 Étape 4 : Analyse de données 32
Chapitre 4. Analyse et résultats **38**
4.1 Aspects fondamentaux du comportement 38
4.1.1 Termes utilisés et définitions 38
4.1.2 Actions du comportement 45
4.1.3 Intention vs comportement réel 49
4.2 Dimensions du comportement sécuritaire 53
4.2.1 Conformité 54
4.2.2 Éthique 55

4.2.3 Jugement 58
4.3 Relations entre les dimensions 60
4.4 Autres constats 67
Chapitre 5. Discussion 69
5.1 Retour sur les sous-objectifs de recherche 69
5.1.1 Identifier les thèmes dans la littérature au sujet du comportement sécuritaire 69
5.1.2 Autres constats importants avant la définition 76
5.2 Une interprétation dialectique du chaos 80
5.2.1 Présentation du modèle dialectique 80
5.2.2 Le comportement sécuritaire sous l'angle du modèle dialectique 81
5.3 Proposition d'une définition du comportement sécuritaire 88
Chapitre 6. Conclusion 92
6.1 Rappel de l'objectif de recherche et principaux résultats 92
6.2 Contributions de l'étude 93
6.3 Limites de l'étude 94
6.4 Pistes pour les recherches futures 96
Bibliographie 99
Annexe 1 – Guide de codage 105
Annexe 2 – Exemple d'un extrait du codage 107
Annexe 3 – Répartition des articles par publication 108
Annexe 4 – Définitions du comportement sécuritaire 109
Annexe 5 – Actions du comportement sécuritaire 113
Annexe 6 – Relations entre les dimensions 121
Annexe 7 – Liste des articles composant l'échantillon final 124

Liste des tableaux

Tableau 3.1 Critères utilisés pour le classement des articles selon le degré de pertinence 29
Tableau 3.2 Répartition des articles avant et après le codage 32
Tableau 3.3 Répartition des articles selon la méthodologie qu'ils emploient 33
Tableau 4.1 Identification du concept de comportement sécuritaire : termes utilisés et définitions 40
Tableau 4.2 Exemple d'un extrait du codage des définitions 41
Tableau 4.3 Principaux thèmes identifiés dans les définitions du comportement sécuritaire 43
Tableau 4.4 Exemple d'un extrait du codage des actions 46
Tableau 4.5 Classification des actions du comportement sécuritaire selon leur facilité d'observation 47
Tableau 4.6 Nombre d'articles selon la dimension étudiée 53
Tableau 4.7 Exemple d'un extrait du codage des liens entre les dimensions 61
Tableau 4.8 Types de relations entre les dimensions du comportement 62
Tableau 5.1 Vérification des critères de la définition 91

Liste des figures

Figure 2.1 Lien entre le comportement sécuritaire et la protection de l'actif..... 10
Figure 2.2 Lien entre le comportement non sécuritaire et la protection de l'actif 12
Figure 2.3 Rôles possibles de la sensibilisation, de l'éducation et de la formation sur le comportement et la protection de l'actif informationnel 13
Figure 2.4 Rôles possibles des politiques organisationnelles sur le comportement et la protection de l'actif informationnel..... 15
Figure 3.1 Démarche pour trier les articles et déterminer l'échantillon d'articles..... 27
Figure 3.2 Répartition des articles de l'échantillon par année de publication 35
Figure 5.1 Arbre de décision de l'adoption d'un comportement..... 74
Figure 5.2 Modèle dialectique du changement organisationnel, Van de Ven et Poole (1995, p.520) 80

Chapitre 1. Problématique

1.1 Présentation de la problématique

À mesure que les technologies deviennent de plus en plus sophistiquées, les méthodes utilisées pour perpétrer des cyberattaques le deviennent tout autant et les risques que cela pose à la sécurité de l'information continuent d'augmenter (Li *et al.*, 2019). À l'échelle mondiale, le coût moyen d'une brèche de données est évalué à 3,86 M$ et la plupart de ces brèches sont causées par des attaques malicieuses (IBM, 2020). Par ailleurs, les employés, par le biais des appareils qu'ils utilisent, constituent la principale voie d'accès pour les incidents de sécurité en permettant notamment à des types d'attaques comme l'hameçonnage, le piratage psychologique et les logiciels malveillants de se propager (PwC, s.d.). Les organisations investissent d'importantes sommes dans des solutions technologiques telles que des pare-feux ou des systèmes pour la gestion des accès et des mots de passe, mais la technologie à elle seule ne suffit pas pour assurer la protection de l'actif informationnel : il faut aussi porter attention aux employés et à leurs comportements, qui sont souvent la cause d'incidents (Ifinedo, 2014; Li *et al.*, 2019). Selon un rapport d'EY, 34% des organisations à échelle mondiale perçoivent les employés malhabiles ou insouciants comme leur principale vulnérabilité en matière de sécurité de l'information (EY, 2018). Ce chiffre s'élève à 39% au Canada (EY, 2020). Pourtant, les organisations s'en remettent encore beaucoup aux solutions technologiques quand il est question de sécurité, même si l'erreur humaine est l'une des sources les plus importantes d'incidents (Sampath, 2019).

L'importance de la dimension humaine, et plus précisément en ce qui a trait au comportement, est mentionnée tant dans la littérature académique que professionnelle. Par exemple, des comportements non sécuritaires de la part des employés, tels que la négligence, sont l'une des principales causes de brèches de données, ce qui entraîne des dépenses de millions de dollars pour les organisations (Herath et Rao, 2009b; Karjalainen *et al.*, 2020). Les brèches de mots de passe sont

également l'un des principaux facteurs de risque d'incident, ce qui démontre que le choix des mots de passe et leur protection constituent un autre aspect problématique en matière de sécurité lié au comportement des employés (Mamonov et Benbunan-Fich, 2018). De plus, l'hameçonnage constitue l'un des intermédiaires les plus fréquents pour perpétrer des attaques et une telle tentative réussit généralement à cause de l'erreur humaine, à la réception d'un courriel frauduleux, par exemple (Reed *et al.*, 2020; Sampath, 2019). En effet, les incidents de sécurité internes à l'organisation sont plus fréquents que ceux provenant de l'extérieur, ce qui met encore une fois l'accent sur le rôle du comportement des employés dans les incidents et sur l'importance de s'attarder à la dimension humaine de la sécurité informationnelle pour prévenir ces incidents (McCormac *et al.*, 2017).

Ainsi, pour mitiger les risques associés aux erreurs humaines, les études comportementales en Sécurité de l'information (Infosec) évoquent souvent l'idée d'un comportement sécuritaire, sans que l'on sache précisément de quoi il est question. Il faut dire que le terme employé pour désigner ce type de comportement varie d'un article à l'autre : comportement « sécuritaire » (p.ex. Karjalainen *et al.*, 2020; Ng *et al.*, 2009; Sampath, 2019), comportement souhaitable (p.ex. Huisman, 2018), sentiment d'auto-efficacité qui serait indicateur d'un comportement sécuritaire (p.ex. Parsons *et al.*, 2010; Rhee *et al.*, 2009) ou intention d'adopter un comportement sécuritaire (p.ex. Herath et Rao, 2009b; Ifinedo, 2014). Quant aux définitions proposées, plusieurs études décrivent qu'un comportement sécuritaire consiste en la conformité des employés aux pratiques de l'organisation, le plus fréquemment sous forme de politiques organisationnelles (p.ex. Herath et Rao, 2009b; Ifinedo, 2014; Parsons *et al.*, 2010) alors que d'autres évoquent que ce comportement relève d'un concept qui va au-delà de la conformité (p.ex. Ng *et al.*, 2009; Safa *et al.*, 2015; van Bavel *et al.*, 2019).

Outre le manque de consensus autour des termes employés et des définitions entourant le comportement sécuritaire, on retrouve également des divergences dans la manière dont le sujet est étudié : le comportement réel ou l'intention d'avoir un certain comportement. Il s'agit d'un choix méthodologique important puisque le but ultime

n'est pas de développer des intentions positives à l'égard de la sécurité de l'information chez les employés, mais bien de voir des changements réels s'opérer dans leur comportement (Boss *et al.*, 2015). Néanmoins, peu d'études s'intéressent au comportement sécuritaire réel et aux façons dont le comportement peut être modifié (Ng *et al.*, 2009).

Pour résumer, l'importance de la dimension humaine en Infosec, et plus spécifiquement l'importance du comportement des employés, est un élément couramment mentionné dans les recherches scientifiques comme dans les rapports professionnels, mais il se présente sous différents noms, avec différentes descriptions ou encore avec des disparités notables dans les moyens pour le mesurer. Nous constatons donc que le comportement sécuritaire est un concept[1] qui semble bien ancré dans la littérature Infosec, mais qui est ambigu. Une étude plus approfondie de ce concept est donc essentielle.

1.2 Pertinence de la problématique

Une définition claire du concept de comportement sécuritaire est essentielle autant pour la communauté scientifique que pour le milieu professionnel.

Tout d'abord, dans la littérature scientifique, plusieurs études quantitatives tentent de mesurer le comportement ou l'une de ses caractéristiques, mais toujours avec le même flou autour du concept (p.ex. Parsons *et al.*, 2017; Parsons *et al.*, 2015; Shropshire *et al.*,

[1] Nous avons choisi de traiter le comportement sécuritaire comme un concept dans le cadre de cette étude, à la différence d'un construit. Dans son étude, Chartrand (2010) fait la distinction suivante : « un concept est une expression ou abstraction d'un phénomène. Un construit nous amène à un niveau supérieur car il s'agit d'un concept déjà défini dans la communauté de recherche scientifique et prêt à être mesuré et analysé » (p.12, note en bas de page). Sachant que le comportement sécuritaire n'est pas clairement défini et qu'il est encore moins prêt à être mesuré et analysé, il nous paraît approprié de le considérer comme un concept. De plus, Barki (2008) précise que des concepts fréquemment mentionnés dans les études ou les rapports professionnels, mais qui sont peu précis ou ne sont carrément pas définis, constituent un bon point de départ pour identifier de futurs construits pertinents, ce qui confirme notre choix de traiter le comportement sécuritaire comme un concept.

2015), alors que certaines recherches comme celle de Rhee *et al.* (2009) ou celle de Safa *et al.* (2015) se basent sur une auto-évaluation pour établir des mesures. Ces éléments semblent confirmer que peu d'études sur le comportement ont été réalisées en utilisant des mesures objectives liées à l'aspect de sécurité (Mamonov et Benbunan-Fich, 2018). Le problème qui survient ici est que, sans une définition claire, on ne peut pas mesurer le construit précisément et objectivement. En effet, en l'absence de clarté dans la définition, il peut être difficile de comprendre ce à quoi un construit fait référence ou encore donner lieu à une confusion avec des construits similaires (MacKenzie *et al.*, 2011). De plus, si le concept et, conséquemment, le construit ne sont pas définis avec précision, les variables découlant du construit risquent fort d'être imprécises elles aussi. On peut ainsi se retrouver avec des résultats mitigés ou encore contradictoires quant à l'impact entre les variables (Barki, 2008).

Ensuite, un moyen efficace pour réduire les risques de sécurité liés aux facteurs humains se trouve dans la sensibilisation à la sécurité de l'information, en combinaison avec l'éducation et la formation (Parsons *et al.*, 2010). Il y a encore peu de données concrètes sur l'efficacité globale des programmes de sensibilisation, mais bon nombre d'organisations ont rapporté individuellement des effets positifs sur le comportement de leurs employés à la suite de ces formations (Korolov, 2015). Toutefois, pour élaborer un programme de sensibilisation efficace, c'est-à-dire qui aura un impact positif sur le comportement des employés, il est important de comprendre ce qui influence le comportement des employés (Ng *et al.*, 2009). Pour comprendre les influences, il faut définir ce qui est entendu par « comportement ». Outre la création des programmes de sensibilisation, d'éducation et de formation, il est également important d'évaluer ces programmes pour déterminer si les objectifs en matière de sécurité ont été communiqués adéquatement, voir comment ces programmes s'inscrivent par rapport aux objectifs et, éventuellement, y apporter des changements (Parsons *et al.*, 2010). L'évaluation de l'efficacité des programmes est un élément important pour les organisations, qui doit leur permettre d'avoir un portrait de leur performance en matière d'Infosec. Cependant, sachant que ces programmes visent avant tout le

changement des comportements des employés et que le comportement sécuritaire est un concept flou, il y a lieu de se demander comment on peut évaluer ces programmes de manière fiable. D'ailleurs, un rapport Gartner (Huisman, 2018) révèle que peu de gestionnaires en sécurité parviennent à décrire ou documenter des objectifs mesurables pour leurs programmes de sensibilisation. Cela implique qu'il est impossible de déterminer si ces programmes sont un succès ou non. Par exemple, utiliser la complétion d'une formation en Infosec comme métrique pour évaluer le comportement ou le changement de celui-ci, comme le font encore souvent des organisations, est insuffisant, car le simple fait que les employés aient suivi une telle formation ne signifie pas que cela a eu un impact positif sur leur comportement (Huisman et Carpenter, 2019). « Un programme efficace de sensibilisation à la sécurité de l'information commence par des objectifs clairement définis et des résultats mesurables» (Huisman, 2018, p.2, traduction libre).

Finalement, les études en Infosec comportementale s'intéressent fréquemment à comprendre pourquoi les employés ne respectent pas les politiques de sécurité de leur organisation ou pourquoi ils continuent d'adopter des comportements qui vont à l'encontre de la sécurité, malgré le fait qu'ils aient connaissance des pratiques et politiques. Pour tenter de mieux comprendre ce phénomène, les chercheurs en Infosec se basent sur des modèles provenant des disciplines connexes à l'Infosec, telles que la criminologie et, le plus fréquemment, la psychologie (Moody *et al.*, 2018). Néanmoins, ce recours aux autres disciplines pour emprunter des modèles crée une sorte de confusion, notamment parce qu'il est difficile d'appliquer efficacement ces modèles en Infosec lorsque des concepts apparemment similaires portent des noms différents ou lorsque des concepts apparemment différents portent des noms similaires. À titre d'exemple, Moody *et al.* (2018) mentionnent qu'il est difficile de discerner clairement la différence entre le concept d'attitude dans la Theory of reasoned action (TRA) et celui de motivation à la protection dans la Protection motivation theory (PMT), deux modèles couramment utilisés en Infosec comportementale. De plus, la Theory of planned

behavior (TPB), fréquemment employée elle aussi, contient le concept d'attitude et il y aurait lieu de se questionner si ce concept diffère de celui dans la TRA. Par exemple, Safa et al. (2015) ont utilisé de manière interchangeable la TPB et la TRA pour justifier l'utilisation de l'attitude dans leur modèle de recherche Infosec, mais il est difficile de comprendre si le concept réfère à la même idée ou à deux idées différentes. De plus, les emprunts des domaines connexes peuvent également soulever des questionnements quant au choix d'un modèle plutôt que d'un autre qui lui est semblable ou encore à savoir comment ces modèles se comparent en termes d'efficacité pour expliquer un phénomène Infosec.

Tous ces constats permettent de souligner l'importance des mesures précises pour évaluer le comportement, et donc le besoin d'une définition précise du concept de comportement sécuritaire à priori.

1.3 Objectif et question de recherche

Ce mémoire a comme objectif de proposer une définition conceptuelle du comportement sécuritaire pour la protection de l'actif informationnel, c'est-à-dire une description aussi précise que possible de ce qu'est un comportement sécuritaire, les caractéristiques qu'il possède et les dimensions qui le composent (MacKenzie *et al.*, 2011). Pour ce faire, nous effectuerons une revue systématique de la littérature afin d'examiner comment le comportement sécuritaire a été défini et employé antérieurement, autant dans des articles scientifiques que dans des rapports professionnels. Pour atteindre cet objectif général, nous avons deux sous-objectifs comme suit :

- Identifier les thèmes qui existent dans la littérature concernant le comportement sécuritaire;
- Proposer une définition « de dictionnaire », soit une définition claire, précise et concise.

Nous nous basons sur l'approche proposée par MacKenzie *et al.* (2011) afin de définir et décrire avec le plus de précision possible ce qui constitue un comportement sécuritaire. Plus précisément, nous allons, comme mentionné plus tôt, examiner la littérature afin de relever les définitions qui ont été données au comportement sécuritaire pour ensuite les regrouper et les comparer. Cela nous permet d'identifier des éléments communs entre les différentes définitions et aide à déterminer plus aisément les caractéristiques d'un comportement sécuritaire, ainsi que de vérifier s'il s'agit d'un concept multidimensionnel. Si tel est le cas, nous souhaitons mettre ensuite en commun les dimensions identifiées, proposer une définition pour chacune des dimensions et établir les relations existant entre ces dimensions. Tous ces éléments devraient, à la fin, nous permettre d'obtenir une définition du comportement sécuritaire qui soit claire, concise et sans ambigüité (MacKenzie *et al.*, 2011).

La question de recherche est donc : *Qu'est-ce qu'un comportement sécuritaire pour la protection de l'actif informationnel et comment se définit-il?*

1.4 Structure du mémoire

Le présent mémoire est structuré de la façon suivante. Le chapitre qui suit définit et décrit l'état des connaissances sur le comportement sécuritaire. Le troisième chapitre s'attarde à la démarche méthodologique suivie pour répondre à notre objectif de recherche. Le quatrième chapitre présente l'analyse des données et les résultats découlant de cette analyse. Le cinquième chapitre discute ces résultats et propose des pistes de réflexion. Enfin, le dernier chapitre fait état des principaux résultats de cette étude, de ses contributions et de ses limites, et propose des pistes pour de futures recherches.

Chapitre 2. État des connaissances autour du concept de comportement sécuritaire

L'objectif de ce mémoire est de proposer une définition conceptuelle du comportement sécuritaire pour la protection de l'actif informationnel. À cet effet, un survol de la littérature pertinente nous permet d'établir un portrait des connaissances déjà existantes en lien avec le comportement sécuritaire des employés et de mettre de l'avant le flou autour de la définition du concept, tant dans la littérature académique que dans la littérature professionnelle.

Pour entamer ce survol de la littérature, nous avons consulté les bases de données ABI/Inform, Science Direct, Sage et Springer, et utilisé les mots-clés « Infosec », « information security » ou Cybersecurity en combinaison avec les termes « Behavior », « secure behavior » et « safe behavior ». Aux mots-clés précédents, nous avons ensuite ajouté « ethics », « compliance » ou « awareness », car notre recherche initiale nous a permis de constater que ces termes étaient fréquemment associés au concept de comportement sécuritaire. Lors de notre recherche, nous avons mis l'emphase sur le sujet, sans égard à la qualité des revues et des conférences (Webster et Watson, 2002). Nous avons également fait une utilisation plus étendue de la littérature professionnelle dans le cadre de ce mémoire, notamment puisque celle-ci présente des enjeux similaires à ceux de la littérature académique à l'égard de l'importance du comportement sécuritaire et du manque de clarté dans sa définition. De plus, elle permet d'illustrer le flou sur le concept du comportement sécuritaire existant aussi dans la pratique professionnelle. Par ailleurs, comme la sécurité de l'information, et plus précisément l'aspect comportemental, est un champ d'étude relativement récent, la littérature professionnelle permet donc de bonifier les connaissances sur ce sujet pour l'instant moins étudié dans le domaine des TI.

Dans le présent chapitre, nous expliquons d'abord le rôle du comportement sécuritaire dans la protection de l'actif informationnel afin de montrer comment le comportement des employés peut contribuer à réduire les risques d'incidents au sein d'une

organisation. Ensuite, nous présentons plus en détail le flou existant autour du comportement sécuritaire, flou qui est à l'origine du manque de consensus entourant la définition et la nature de ce concept. Finalement, nous rappelons que plusieurs études soulignent qu'évaluer l'intention d'un comportement et évaluer le comportement réel ne s'équivalent pas, puisque le comportement réel permet de donner un portrait plus précis de l'efficacité des mesures prises pour modifier le comportement des employés. Ainsi, dans le cadre de ce chapitre, les études sur le comportement réel ont été favorisées à celles sur l'intention, afin de donner une image plus réaliste et plus claire de ce que représente le comportement dans un contexte de sécurité de l'information.

2.1 Le comportement sécuritaire et la protection de l'actif informationnel

La protection de l'actif informationnel d'une organisation passe par l'adoption d'un comportement sécuritaire de la part des employés. Dans la présente section, nous tenterons donc de mieux comprendre la relation entre le comportement sécuritaire et la protection de l'actif.

Lien entre le comportement des employés et la protection de l'actif informationnel

Même si le lien entre le comportement et la protection de l'actif informationnel y est parfois sous-entendu (p.ex. Parsons *et al.*, 2010; Safa *et al.*, 2015), la littérature aborde beaucoup plus souvent les antécédents d'un comportement sécuritaire tels que les traits individuels (McCormac *et al.*, 2017), l'attitude et l'intention (Shropshire *et al.*, 2015) ou encore le sentiment d'auto-efficacité (Rhee *et al.*, 2009; Safa *et al.*, 2015). La présente section ne vise cependant pas à traiter de ces antécédents, mais plutôt à mieux comprendre la relation entre le comportement sécuritaire et la protection de l'actif informationnel. Tel qu'illustré par la figure 2.1, la croyance générale est qu'un comportement sécuritaire a un impact positif sur la protection de l'actif informationnel.

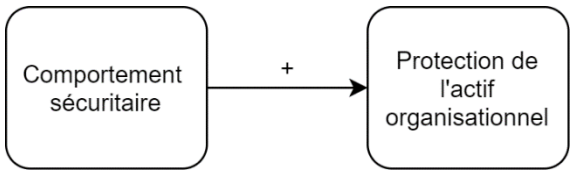

Figure 2.1 Lien entre le comportement sécuritaire et la protection de l'actif

Il est toutefois difficile de mesurer la variable « protection de l'actif informationnel » directement, puisque la notion de protection varie d'une organisation à l'autre, en fonction de leurs besoins, de leur contexte et de leurs contraintes. Ainsi, une organisation dans le milieu de la santé n'aura pas les mêmes besoins en matière de protection de l'actif qu'une organisation dans le secteur énergétique (EY, 2018). En raison de cela, certains chercheurs et professionnels préfèrent utiliser le risque (McMillan et Heiser, 2018; Watts, 2020) ou encore l'impact des incidents (EY, 2018) comme mesure. Par exemple, les organisations rédigent des politiques en matière de sécurité pour servir de lignes directrices afin de protéger l'actif informationnel, mais pour les aider à bien définir les objectifs de protection, elles peuvent utiliser le risque comme mesure de référence (McMillan et Heiser, 2018). Le risque s'avère une mesure pertinente, car il peut servir de langage commun entre les différents départements d'une organisation, tels que la direction et les gestionnaires TI, en permettant à chaque partie de mieux comprendre les risques auxquels est exposée l'autre partie et trouver un juste milieu pour intervenir sur ces risques. En ayant ce langage commun, les responsables TI peuvent communiquer plus aisément à la direction la manière dont les risques liés aux TI peuvent affecter le reste de l'organisation, dans le but de trouver un front commun d'intervention (Westerman, 2009).

La mesure de l'impact des incidents de sécurité, quant à elle, permet de comprendre l'importance de la protection de l'actif à travers un autre langage commun à l'organisation, celui des finances. En effet, les impacts financiers sont une mesure

fréquemment employée pour évaluer la protection de l'actif informationnel (p.ex. IBM, 2020). Si l'actif est adéquatement protégé, cela aura un effet positif sur le budget de l'organisation, car les risques d'incidents de sécurité seront réduits. Inversement, si une partie considérable du budget est allouée à la gestion post-incident, il y a lieu de questionner l'efficacité de la protection de l'actif (EY, 2018; IBM, 2020). Toutefois, la mesure du risque doit être revue régulièrement, puisque les risques et les besoins en gestion du risque changent au fil du temps et on ne peut pas être certain d'identifier tous les risques possibles (Watts, 2020; Westerman, 2009). Il en va de même pour la mesure de l'impact des incidents, car les sources d'incidents peuvent évoluer dans le temps et il devient nécessaire de réévaluer régulièrement les impacts possibles (Watts, 2020).

Concernant la variable indépendante de la figure 2.1., il est à noter que les comportements sécuritaires ou protecteurs sont considérés comme un succès lorsqu'il n'y a pas d'incident de sécurité qui survient (Ng *et al.*, 2009). Cette idée nous paraît importante, car elle propose une explication quant à la difficulté de trouver des études portant sur l'impact d'un comportement sécuritaire sur la protection de l'actif informationnel. En effet, il est impossible d'étudier ou d'observer l'absence d'un phénomène, en l'occurrence l'absence d'incidents de sécurité ici, ce qui fait en sorte qu'on doive plutôt examiner le lien inverse, c'est-à-dire l'impact d'un comportement non sécuritaire sur la protection de l'actif. Ainsi, le comportement non sécuritaire a un impact négatif sur la protection de l'actif (voir la figure 2.2), ce qui se traduirait notamment par la présence d'incidents (van Bavel *et al.*, 2019). Par exemple, certains articles (p.ex. Rhee *et al.*, 2009; Safa *et al.*, 2015; Warkentin *et al.*, 2016) montrent à partir des comportements non sécuritaires spécifiques tels que l'emploi de mots de passe faibles, le fait d'agir sans réfléchir aux conséquences pour l'Infosec ou le refus d'utiliser un logiciel *anti-malware*, qu'il y a un impact négatif sur la protection de l'actif informationnel.

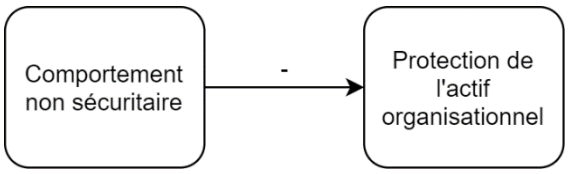

Figure 2.2 Lien entre le comportement non sécuritaire et la protection de l'actif

Nous avons également remarqué que certains auteurs examinent ce lien à travers l'angle d'une variable modératrice, principalement la sensibilisation, l'éducation et la formation (SEF). Les sous-sections qui suivent examineront le rôle de ces variables modératrices et la manière dont elles sont abordées dans la littérature.

Le rôle de l'éducation, la sensibilisation et la formation dans la protection de l'actif

Bon nombre d'études et de rapports professionnels s'intéressant au comportement sécuritaire pour la protection de l'actif informationnel mentionnent la sensibilisation, l'éducation et la formation (SEF) comme des facteurs favorisant l'adoption d'un comportement sécuritaire chez les employés. Ainsi, la sensibilisation des employés vise à mieux les préparer à prévenir les incidents et à savoir agir en cas de besoin (Furnell et Clarke, 2012). Ensuite, l'éducation, même si elle n'est pas la solution à tous les problèmes en Infosec, peut contribuer à mieux informer les gens, et plus elle est inculquée tôt, plus les notions clés concernant les menaces et les moyens de protection sont susceptibles de devenir naturellement une partie du bagage de connaissances des employés (Furnell et Clarke, 2012). Enfin, les formations en Infosec permettent de cultiver chez les employés les connaissances et les compétences nécessaires pour protéger efficacement l'actif informationnel. Par ailleurs, les connaissances acquises durant les formations ne seront efficaces que si la formation encourage et motive les employés à mobiliser ces connaissances (Furnell et Thomson, 2009).

La littérature présente ces trois éléments comme des antécédents d'un comportement sécuritaire sans les positionner clairement dans le réseau nomologique de la protection

de l'actif (p.ex. Parsons *et al.*, 2010; Safa *et al.*, 2016). Or, en examinant de plus près rapports et articles, la sensibilisation, l'éducation et la formation pourraient possiblement avoir un rôle modérateur (p.ex. van Bavel *et al.*, 2019) sur le lien entre le comportement et la protection de l'actif (voir figure 2.3). À titre d'exemple, les brèches de sécurité découlent souvent de la négligence humaine (c.-à-d. un « comportement non sécuritaire ») et cette négligence peut compromettre les meilleurs mécanismes de défense en matière d'Infosec. Les programmes de SEF devraient permettre de développer chez les employés les aptitudes à prendre des décisions éclairées en matière de sécurité informationnelle et prévenir la négligence (impact direct sur le comportement non sécuritaire) ainsi qu'à atténuer l'impact sur les mécanismes de défense (rôle modérateur de l'impact du comportement non sécuritaire sur la protection de l'actif) (Wu *et al.*, 2012).

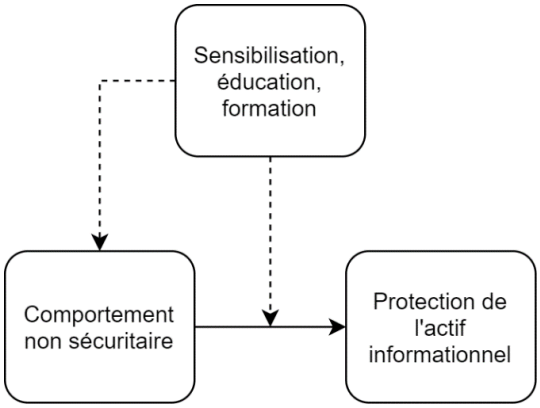

Figure 2.3 Rôles possibles de la sensibilisation, de l'éducation et de la formation sur le comportement et la protection de l'actif informationnel

Il est à noter que la sensibilisation est plus fréquemment mentionnée dans la littérature que l'éducation ou la formation (p.ex. Ng *et al.*, 2009; Safa *et al.*, 2015). En effet, les besoins des organisations en matière de protection de l'information grandissent sans cesse à mesure que les menaces croissent elles aussi et cela met encore une fois l'accent sur le fait que la technologie seule ne peut pas couvrir tous les aspects que représentent ces menaces. Cette réalité met de l'avant l'importance d'une sensibilisation continue. On suggère d'ailleurs que 40% du budget total pour la sécurité d'une organisation soit

alloué à la sensibilisation des employés en lien avec le rôle qu'ils ont à jouer dans la protection de l'actif informationnel (Furnell et Thomson, 2009). Idéalement, les programmes de sensibilisation devraient viser à faire passer l'employé d'un niveau d'ignorance à un niveau de conscience ou de connaissance en sécurité de l'information (Furnell et Thomson, 2009).

Nous constatons donc que les SEF peuvent jouer un rôle significatif dans la protection de l'actif informationnel. Par ailleurs, la littérature en Infosec examine les SEF surtout de manière conceptuelle en les positionnant autant comme antécédent du comportement sécuritaire que comme modérateur de la relation entre le comportement (non) sécuritaire et la protection de l'actif informationnel.

Le rôle des politiques organisationnelles

Dans le but de développer un comportement sécuritaire chez les employés, les organisations se fient souvent à des documents écrits, principalement des politiques organisationnelles en matière de sécurité, pour favoriser une meilleure compréhension des enjeux de protection (Furnell et Thomson, 2009). Cela permet donc de supposer que les politiques organisationnelles ont, comme les SEF, un rôle d'antécédent et un rôle de modérateur du lien comportement-protection. Le rôle modérateur (voir figure 2.4), à notre connaissance, n'a pas été démontré empiriquement. Néanmoins, à partir d'un exemple concret, dans ce cas la Politique de sécurité de l'information de HEC Montréal (*Politique de sécurité de l'information*, 2019), il est possible d'expliquer les liens. Ainsi, dans le but de mitiger les risques liés à l'Infosec, la Politique prescrit des rôles et des responsabilités pour les différentes parties impliquées, allant de la direction aux simples utilisateurs, en passant par les responsables TI et le conseil d'administration (lien direct). Elle indique également les sanctions possibles pour un non-respect des politiques afin de favoriser un comportement plus sécuritaire de la part des membres de HEC Montréal (lien modérateur).

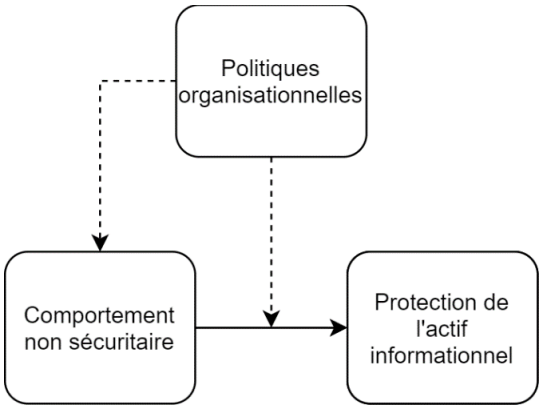

Figure 2.4 Rôles possibles des politiques organisationnelles sur le comportement et la protection de l'actif informationnel

Nous remarquons que les SEF, de même que les politiques organisationnelles, pourraient autant être un antécédent du comportement sécuritaire qu'avoir un rôle modérateur de la relation entre le comportement non sécuritaire et la protection de l'actif informationnel. Enfin, bien que la littérature empirique ne soit pas très riche, nous pouvons néanmoins conclure que le comportement sécuritaire (ou non sécuritaire) a un impact positif (ou négatif, respectivement) sur la protection de l'actif informationnel. Cependant, comme il n'est pas clair ce que l'on entend par comportement « sécuritaire » ou « non sécuritaire », la section qui suit examinera de plus près ce concept qui est au cœur du présent mémoire.

2.2 Comportement sécuritaire : un concept flou

Dans un rapport Gartner, Bazargan *et al.* (2020) posent la question suivante : « même si vous avez longuement réfléchi à la sécurité de l'information, avez-vous déjà spécifié à quoi ressemblent des comportements sécuritaires? » (p.2 traduction libre). En effet, un bref survol de la littérature existante sur la dimension comportementale de l'Infosec nous a d'abord permis de constater que le concept de « comportement sécuritaire » souffre d'un manque de consensus autour des termes employés pour s'y référer et autour de ses définitions. De plus, lorsque des articles font mention d'exemples de

comportements, il est possible de déduire si ces comportements sont sécuritaires ou non, mais il n'est toutefois pas possible d'établir une liste complète de comportements sécuritaires ou non sécuritaires. Nous discuterons plus en détail du flou entourant ce concept dans les paragraphes qui suivent.

2.2.1 Termes utilisés

Tout d'abord, en ce qui concerne l'utilisation variée des termes, on retrouve dans la littérature des expressions comme «*information security behavior*» (Karjalainen *et al.*, 2020; Parsons *et al.*, 2017), « *security practice behavior* » (Rhee *et al.*, 2009), « *online security behavior* » (van Bavel *et al.*, 2019), ou *« conscious care behavior*» (Safa *et al.*, 2015). Certains de ces termes réfèrent à une même idée, telle que l'adoption d'un comportement qui permet de protéger l'actif organisationnel et la compréhension des conséquences de ne pas le faire (p.ex. *online security behavior*, *conscious care behavior)* alors que d'autres portent sur une idée quelque peu différente comme la conformité aux pratiques ou aux politiques organisationnelles en matière d'Infosec (p.ex. *information security behavior*).

De plus, nous remarquons également une certaine disparité dans les manières de mesurer le comportement sécuritaire dans certaines études. Par exemple, Safa *et al.* (2015) ont mesuré le *conscious care behavior* avec des items qui renvoient à la capacité de employés de prendre conscience de leur comportement en contexte d'Infosec (p.ex. le fait de réfléchir et considérer les conséquences possibles avant de poser une action qui pourrait affecter la sécurité de l'information ou encore de se fier à ses expériences antérieures en Infosec pour réagir dans une situation donnée). Rhee *et al.* (2009), pour leur part, ont mesuré le concept de « *security practice behavior* » à partir d'items liés autant à un aspect technologique (p.ex. installer un antivirus et le mettre à jour régulièrement ou utiliser un filtre antipourriel) qu'à un aspect comportemental (p.ex.

faire des copies de sauvegarde de documents importants ou vérifier si un site crypte les données transférées avant d'y rentrer des renseignements personnels).

Par ailleurs, dans certains articles, on retrouve également des termes qui semblent référer à un aspect du comportement et y être étroitement reliés, mais sans être des termes désignant explicitement le comportement. Tel est le cas d'expressions comme *« privacy self-efficacy*» (Mamonov et Benbunan-Fich, 2018), ou « *accountability and responsibility* » (Buytendijk, 2017).

2.2.2 Définitions

Nous avons pu constater qu'en plus du manque d'un terme commun pour le désigner, le concept de comportement sécuritaire souffre également de l'absence d'une définition claire et partagée. On retrouve notamment des définitions du comportement aussi différentes que celles de Safa *et al.* (2015) et Warkentin *et al.* (2016). Le *conscious care behavior* de Safa *et al.* est défini comme un comportement où « les employés réfléchissent aux conséquences de leurs actions en matière d'Infosec lorsqu'ils utilisent un système, et plus particulièrement l'Internet » (p.66, traduction libre), alors que le *protective security behavior* de Warkentin *et al*. est décrit comme un « comportement associé à des actions protectrices dans un environnement à haut risque et visant à offrir un niveau d'assurance acceptable contre les menaces » (p.26, traduction libre).

Par ailleurs, certains articles mentionnent des termes référant au comportement sécuritaire, mais sans les définir (p.ex. Shropshire *et al.*, 2015), tandis que d'autres évoquent l'idée d'un tel comportement sans explicitement le nommer (p.ex. Albrechtsen, 2007). De plus, les articles qui définissent le concept proposent des éléments de définition souvent disparates, de manière qu'on puisse difficilement dégager une définition qui fasse consensus. Parmi les éléments mentionnés, nous retrouvons notamment le respect des politiques organisationnelles, le fait de poser des

gestes en pensant à la conséquence de ses actes, ou le fait de prendre des décisions et agir de manière à réduire le risque d'une attaque ou d'un incident.

Enfin, mentionnons que certains articles semblent confondre comportement et attitude. Par exemple, chez Boss *et al.* (2009) le comportement sécuritaire est défini comme la perception d'un individu qu'il prend les mesures adéquates afin de sécuriser son ordinateur et applique les principes en Infosec. Pourtant cette définition s'apparente davantage à une attitude c'est-à-dire l'« ensemble des opinions manifestées par un individu, un groupe social ou une institution, se traduisant par un comportement habituel ou circonstancié » (Larousse, 2020). Il faut dire qu'il y a des études (p.ex. Dinev et Hu, 2007; Safa *et al.*, 2015) qui ont examiné l'attitude comme un antécédent du comportement sécuritaire et qui l'ont généralement définie comme une opinion ou une perception favorable de l'adoption d'un comportement donné. Toutefois, dans ces études, la distinction entre les deux termes était suffisamment claire.

2.2.3 Dimensions

La différence dans les termes employés pour le désigner, ainsi que les nuances dans les définitions nous apparaissent comme des signes potentiels de la présence de différentes dimensions au comportement sécuritaire. Bien que cet aspect multidimensionnel ait été peu étudié, quelques chercheurs ont évoqué l'existence de plus d'une dimension du comportement sécuritaire.

Tout d'abord, la conformité semble souvent associée au concept de comportement sécuritaire (p.ex. Moody *et al.*, 2018; Yazdanmehr et Wang, 2016). Sans explicitement définir une dimension axée sur la conformité, ces études sous-entendent qu'un comportement conforme consisterait à suivre les règles et les principes inscrits dans la politique organisationnelle, avec des actions telles que l'utilisation de mots de passe robustes ou le signalement d'événements suspects (McCormac *et al.*, 2017; Parsons *et*

al., 2017). De plus, la conformité n'est pas un acquis permanent, car elle ne vise pas l'intention de l'employé de se conformer aux politiques, mais bien ses actions réelles. Or, Warkentin *et al.* (2016), mentionnent que même si les employés suivent les formations, respectent les règles et se servent des outils à leurs dispositions, ils finissent par les délaisser au bout d'un certain temps, principalement parce qu'ils ne perçoivent pas de danger immédiat pour la sécurité. Cela laisse donc supposer que la conformité ne devient pas un automatisme à long terme et serait plutôt le résultat d'une réflexion vis-à-vis de l'évaluation des risques de se conformer ou non, et de la concordance du fait de se conformer avec les valeurs de l'individu.

En effet, il est important que les employés comprennent pourquoi certains comportements sont bons et d'autres non, et non seulement qu'ils suivent ce que prescrivent les politiques organisationnelles (Ruighaver *et al.*, 2010). Dans ce contexte, le rôle de l'éthique dans le comportement sécuritaire peut être défini comme un ensemble de principes qui permettent « d'identifier les critères entre ce qui est bien et mal » (Ruighaver *et al.*, 2010, p. 732 - traduction libre) et les actions de « systématiser, défendre et recommander les concepts de bon et mauvais comportement » (Buytendijk, 2017, p.4 – traduction libre). De plus, un avantage considérable à l'adoption de principes éthiques serait le fait que les employés auront davantage conscience des conséquences possibles de leurs actions, de manière à être mieux outillés devant une situation inconnue (Ruighaver *et al.*, 2010).

Enfin, certaines études font mention d'une dimension du comportement qui va au-delà de la conformité et même de l'éthique. Cette dimension fait référence à la capacité de l'individu de s'adapter à une nouvelle situation. Nguyen (2017) l'a désignée par le terme « intelligence » et l'a définie comme « le réflexe d'assurer la protection de l'information en jugeant de manière éclairée les activités du quotidien et en prenant, au besoin, les mesures appropriées » (p.12). D'autres termes sont également utilisés pour désigner cette dimension, par exemple « *conscious care behavior*» chez Safa *et al.* (2015). Nous avons choisi de désigner cette dimension par le terme « jugement » pour faire référence aux réflexes individuels de protection découlant de l'évaluation d'une situation. Si la

conformité constitue une bonne prémisse de départ pour l'adoption d'un comportement sécuritaire, elle ne peut pas garantir le développement d'un tel comportement chez les employés (Huisman et Carpenter, 2019). Dans le même sens, le fait que les employés adoptent une approche éthique leur permettant d'avoir davantage conscience des conséquences de leurs actions n'implique pas une adaptation rapide aux situations imprévues (Ruighaver *et al.*, 2010). Ainsi, l'adaptation aux imprévus relève davantage du jugement.

Par ailleurs, l'étude de Hsu *et al.* (2015) évoque un comportement nommé « *extra-role behavior »* qui, à première vue, s'apparente au jugement, mais il pourrait aussi s'agir d'une dimension distincte qui met de l'avant un aspect coopératif, c'est-à-dire d'aider ses collègues ou de faire des suggestions dans le but d'améliorer les pratiques Infosec de l'organisation. Il serait donc pertinent d'investiguer davantage non seulement les dimensions de conformité, éthique et jugement, mais aussi la possibilité que d'autres dimensions existent (par exemple, la coopération).

2.2.4 Dimensions indépendantes ou interdépendantes?

Un survol des écrits nous a permis de discerner au moins trois dimensions du comportement sécuritaire : la conformité, l'éthique et le jugement. La littérature semble indiquer que chacune de ces trois dimensions est pertinente pour caractériser le comportement sécuritaire, mais prises une par une, en isolation, elles pourraient ne pas être suffisantes pour constituer un comportement sécuritaire. Pour cette raison, il est donc essentiel de clarifier les relations entre les dimensions qui le composent.

Pour ce faire, nous nous sommes tournés vers des théories issues de la psychologie, à savoir la théorie de la cohérence et de la dissonance cognitive et la théorie interpersonnelle du comportement (TIB - *Theory of interpersonal behavior*), afin de comprendre comment le comportement se forme, car aucune étude en Infosec ne semble adresser l'interdépendance des dimensions. À la base, il y a la supposition que

l'individu essaie de trouver une cohérence entre ses croyances et son comportement; c'est ce que l'on désigne par la cohérence cognitive. Lorsqu'un ou plusieurs éléments cognitifs deviennent incohérents chez l'individu, il survient alors une dissonance, qui se traduit souvent par un stimulus (causé par cette expérience « négative ») qui pousse l'individu à vouloir diminuer l'incohérence et à maintenir la cohérence à laquelle il est habitué (Gawronski, 2012).

Pour mieux clarifier ce phénomène, nous pouvons utiliser en exemple le cas du stratagème de la fraude du président, un type d'hameçonnage assez courant. Tout d'abord, rappelons que la fraude du président est une attaque malicieuse où un fraudeur se fait passer pour le président d'une compagnie dans un courriel où il demande à des employés une certaine faveur, le plus souvent un transfert d'argent[2]. Pour un employé qui reçoit ce courriel, il y aura vraisemblablement une dissonance cognitive, puisque ce n'est pas habituel que le président demande de l'argent ou encore qu'il communique directement avec un employé. Face à cette situation, l'employé cherchera alors à s'ajuster pour revenir à la cohérence, ce qui se fera par une tentative de changer l'élément de dissonance (Szajna et Scamell, 1993). Puisque l'état de dissonance est généralement désagréable, il constitue une motivation pour l'individu à enclencher un processus cognitif afin de le diminuer (Harmon-Jones et Harmon-Jones, 2007). Par ailleurs, l'incohérence qui en découle représente un signal d'erreur dans le système de croyances de l'individu et ce dernier doit y remédier. Puis, en nous basant sur la TIB, nous avançons que les croyances de l'employé et son évaluation de la situation influenceront son attitude, ce qui déterminera ensuite son comportement. Nous supposons donc que c'est le jugement qui déterminera comment l'employé agira.

Le jugement peut ainsi mener à plusieurs avenues. Par exemple, l'employé pourrait rapidement voir qu'il s'agit d'un hameçonnage et le signaler. Dans ce cas-ci, il s'est conformé aux principes qu'il aurait appris dans le cadre du SEF (c.-à-d. ne pas cliquer sur un lien) et s'est peut-être servi de son expérience (découlant du jugement) pour

[2] Banque Nationale (2020, 20 octobre). « Comment fonctionne la fraude du président? » Récupéré de : https://www.bnc.ca/particuliers/conseils/securite/fraude-du-president.html

déterminer qu'il s'agit bel et bien d'un courriel d'hameçonnage. D'autre part, un employé pourrait ne pas savoir qu'il s'agit d'un hameçonnage, mais choisira de ne pas cliquer, car il aura appris dans sa formation qu'il vaut mieux ne pas ouvrir de lien dans un courriel si l'on a un doute. Ainsi, il aura simplement opté pour la conformité aux principes SEF. Ensuite, l'employé pourrait également choisir de ne pas cliquer sur le lien en se basant sur l'idée qu'il n'est pas éthique de la part du président de demander de l'argent à un employé. Le résultat, ici, découlera donc de la dimension éthique. Enfin, il pourrait choisir de ne rien faire, auquel cas l'enjeu sera de minimiser les dommages et espérer que personne d'autre ne tombe dans le piège advenant que le courriel frauduleux ne soit pas signalé.

En empruntant à la psychologie des théories expliquant le développement d'un comportement et en les adaptant au contexte de sécurité de l'information, nous avons pu proposer une idée de liens logiques unissant les dimensions du comportement sécuritaire. La littérature Infosec tend, en effet, à montrer la pertinence d'étudier les dimensions comme étant interdépendantes plutôt qu'indépendantes sans toutefois offrir une validation empirique des relations entre ces dimensions. Cela soulève un intérêt à investiguer la littérature académique et professionnelle plus en profondeur afin de mieux comprendre le phénomène.

2.3 Conclusion

Ce chapitre nous a permis de mettre en lumière un lien clair entre le comportement sécuritaire et la protection de l'actif informationnel ainsi qu'un flou entourant le concept de comportement sécuritaire. Ce flou se manifeste notamment par le manque de consensus autour du terme désignant le concept et autour des définitions, qui varient grandement d'une étude à l'autre. Néanmoins certains points de convergence entre les études nous ont mené au constat que le comportement sécuritaire est probablement un concept multidimensionnel, mais les dimensions qui le constituent, leurs

caractéristiques et la manière dont elles sont reliées ne font pas consensus non plus. Tous ces éléments nous incitent à approfondir notre connaissance du phénomène afin de trouver un terme et une définition communs pour désigner le concept de comportement sécuritaire. Le prochain chapitre décrit la méthodologie qui nous permettra d'atteindre ce but.

Chapitre 3. Méthodologie de recherche

L'objectif du présent mémoire est de proposer une définition conceptuelle du comportement sécuritaire pour la protection de l'actif informationnel. Dans le chapitre précédent, nous avons relevé différents aspects flous du comportement sécuritaire, surtout en ce qui concerne les termes utilisés pour le désigner et ses définitions. Ainsi, pour y amener plus de clarté, il s'avère pertinent d'examiner en profondeur ce que la littérature contient sur le comportement sécuritaire, ses définitions et ses dimensions, afin de rassembler ces éléments en apparence disparates et obtenir une définition plus uniforme. Dans ce chapitre, nous expliquerons d'abord le choix d'employer la revue de littérature systématique comme méthode de recherche, puis nous détaillerons les différentes étapes de la démarche.

3.1 Choix de la méthodologie de recherche

Pour nous permettre de recueillir les données qui aideront à répondre à nos sous-objectifs de recherche, la revue de littérature effectuée dans le cadre de notre méthodologie correspond au type conceptuel, tel que décrit par de Guinea et Paré (2017). Ce type de revue systématique se concentre sur un seul concept, ici le comportement sécuritaire, et « implique l'identification des manières dont le concept a été défini et l'identification de ses principales caractéristiques » (de Guinea et Paré, 2017, p.75, traduction libre). De plus, ce type de revue étant généralement inclusif, il est possible d'étudier une grande variété de sources et faire preuve de plus de souplesse sur le critère de la qualité. Un assouplissement du critère de qualité des revues et des conférences est donc un avantage dans le cadre de ce mémoire puisque le domaine de la sécurité de l'information est relativement récent et ainsi nous aurons accès à un plus grand nombre d'articles. Bref, toutes ces caractéristiques viennent confirmer notre choix d'utiliser cette démarche pour guider la méthodologie du présent mémoire.

Le but de notre approche méthodologique est d'obtenir un vaste portrait de la manière dont le concept de comportement sécuritaire est défini et employé dans la littérature, des termes utilisés pour le désigner et des dimensions qui le constituent. L'objectif est d'avoir autant de données que possible pour établir des *patterns*, des similitudes et des différences entre les éléments relevés. Comme le sujet de cette étude est récent, il pourrait être plus difficile de trouver un nombre suffisant de sources pertinentes dans la littérature académique; c'est pourquoi nous examinons également la littérature professionnelle, dans ce cas-ci les articles de Gartner[3].

En nous basant sur les recommandations de Xiao et Watson (2019) et de Templier et Paré (2015), quatre principales étapes ont été identifiées dans le cadre de la présente revue systématique, à savoir la recherche de la littérature, le tri des sources, l'extraction des données et l'analyse des données. Ces étapes sont détaillées dans le présent chapitre.

3.2 Étape 1 : Recherche de la littérature

La recherche systématique d'articles a été effectuée en mars 2021. Pour la recherche de la littérature académique, les bases de données utilisées étaient ABI/Inform, Science Direct, Web of Science, IEEE Xplore, Sage et Springer. Nous avons débuté avec les mots-clés « cybersecurity », « information security », « infosec », « computer security » en combinaison avec « behavior ». Les quatre expressions en lien avec la sécurité ont également été combinées avec l'expression « ethics », qui n'a donné aucun résultat, puis avec les expressions « compliance » et « policy », qui ont pour la plupart généré des doublons des articles obtenus initialement. De plus, l'expression « security behavior », qui apparait dans la liste de mots-clés de plusieurs articles, a donné une grande quantité de sources de domaines autres que les TI, mais après avoir filtré le sujet, les résultats

[3] L'utilisation de l'expression « littérature professionnelle » dans ce chapitre, de même qu'au chapitre 4 réfère aux articles provenant de Gartner.

obtenus étaient à nouveau des doublons. Mentionnons que tous les résultats dans les bases de données consultées incluent autant « behaviour » que « behavior », peu importe l'orthographe employée dans la requête.

Les mots-clés ont été cherchés dans le résumé de l'article, lorsque la base de données permettait ce type de tri, afin d'assurer que le comportement sécuritaire pour la protection de l'actif informationnel soit l'un des principaux éléments de l'article. Les articles scientifiques, à savoir évalués par les pairs, ont été priorisés, mais des actes de conférences ont également été inclus afin d'enrichir notre connaissance sur le comportement sécuritaire.

Enfin, dans le but de nous assurer que notre échantillon est aussi complet que possible, nous avons fait une vérification au moyen de Google Scholar, en y cherchant les mêmes combinaisons de mots-clés mentionnées précédemment. La fonction de recherche de Scholar étant plus limitée que celle des autres bases de données utilisées, nous avons filtré les résultats en cherchant les mots-clés dans le titre. Nous avons cherché dans les dix premières pages de résultats. Par ailleurs, dès les cinq premières pages de résultats, nous avons constaté que toutes nos combinaisons de mots-clés avaient généré principalement des doublons des articles précédemment recueillis ou encore des articles non pertinents pour cette étude. À la fin, seuls quatre articles pertinents additionnels ont été trouvés.

Pour la recherche de la littérature professionnelle, la base de données de Gartner a été utilisée. Nous avons employé les mêmes combinaisons de mots-clés que pour les articles scientifiques. De plus, nous avons ajouté l'expression « digital ethics », qui désigne des principes et valeurs éthiques dans le cadre de l'utilisation des TI et qui semble être une expression propre à Gartner. En effet, une recherche de cette expression dans les autres bases de données (littérature scientifique ou professionnelle) n'a pas abouti à des résultats pertinents.

3.3 Étape 2 : Tri des articles

Une fois que la liste des sources a été recueillie, Xiao et Watson (2019) recommandent d'examiner chacun des articles afin de déterminer s'il doit faire l'objet des étapes d'extraction des données et d'analyse, et d'éliminer ceux dont le contenu n'est pas pertinent, c'est-à-dire applicable à la question ou aux sous-objectifs de recherche. Partant de cette recommandation, la figure 3.1 illustre la démarche suivie pour cette étape.

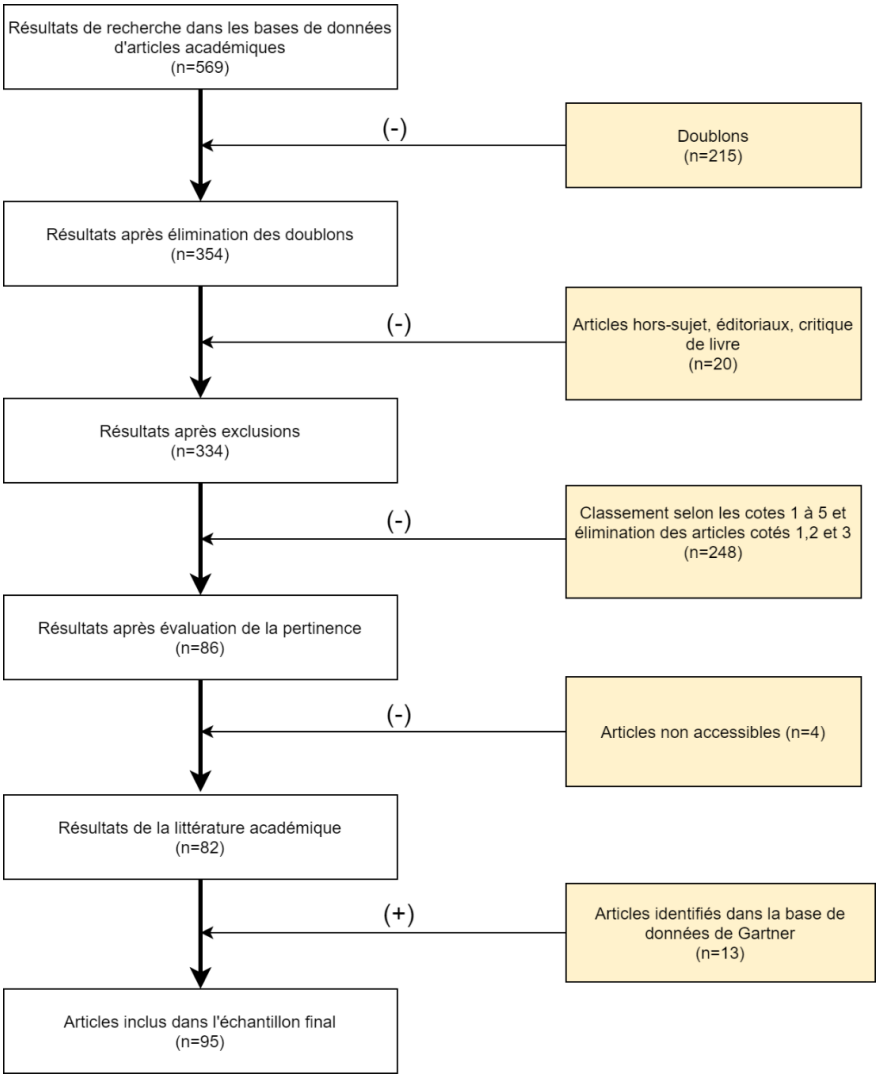

Figure 3.1 Démarche pour trier les articles et déterminer l'échantillon d'articles

Ainsi, lorsque notre recherche dans les bases de données était complétée, les résultats obtenus ont été exportés dans le logiciel de gestion bibliographique EndNote. Le nombre total d'articles se chiffrait initialement à 569 et, après avoir éliminé les doublons, on dénombrait 354 articles. Ce changement s'explique grandement par le fait que les résultats obtenus avec les mots-clés liés à la sécurité combinés avec « compliance » ont retourné essentiellement des doublons des résultats obtenus auparavant avec les mots-clés liés à la sécurité en combinaison avec « behavior ». Puis, nous avons exclu les articles qui étaient visiblement hors sujet par leur titre, les éditoriaux et les critiques de livres, pour arriver à 334 articles.

Par la suite, nous avons entrepris de trier ces articles selon leur pertinence, afin de ne conserver que ceux dont la pertinence est la plus élevée pour la présente étude. Suivant la recommandation de Xiao et Watson (2019), le tri des articles a été fait à partir de leur résumé et de leur liste de mots-clés. Ainsi, un système de classement coté de 1 (pas pertinent) à 5 (très pertinent) a été créé pour trier les articles, selon les critères présentés dans le Tableau 3.1. Une fois ce classement effectué, les 248 articles correspondant aux cotes 1, 2 et 3 ont été exclus en raison de leur faible degré de pertinence pour notre objectif général. En effet, les critères de ces trois catégories (voir le Tableau 3.1) laissaient déjà présager un faible niveau de pertinence pour la présente recherche. Enfin, quatre autres articles ont été enlevés parce que nous n'avons pas réussi à avoir accès au texte complet.

Tableau 3.1 Critères utilisés pour le classement des articles selon le degré de pertinence

Cote	Description des critères
5	• Le comportement sécuritaire ou l'une de ses dimensions est le sujet principal de l'étude.
4	• Le comportement sécuritaire (ou l'une de ses dimensions) n'est pas le sujet principal de l'étude, mais y est abordé de manière assez élaborée • Contient des éléments connexes pertinents pour mieux comprendre le concept de comportement sécuritaire
3	• Traite du comportement sécuritaire, mais ce n'est pas le sujet principal • Aborde le concept de comportement, mais de manière limitée
2	• Mentionne seulement le comportement ou traite d'un concept associé au comportement sécuritaire (p.ex. sensibilisation Infosec) mais le comportement lui-même n'est pas abordé, ni le lien entre le comportement et le concept connexe • Étendue de l'étude trop restreinte (p.ex. mots de passe seulement)
1	• Non relié au comportement ou cite seulement le comportement, mais porte sur un autre sujet • Porte sur un sujet trop général ou trop vague (p.ex. les sciences cognitives en cybersécurité) • Le sujet de l'étude est trop restreint (p.ex. une technologie spécifique seulement, un groupe démographique particulier)

Quant à la littérature professionnelle, étant donné les fonctionnalités limitées du moteur de recherche de Gartner, nous avons effectué le tri des articles manuellement, à la source. Puisque les titres sont habituellement explicites, nous nous sommes d'abord basés sur le titre des rapports, puis avons lu leurs résumés afin de les trier. Seuls les articles correspondant aux critères des cotes 4 et 5 (voir le tableau 3.1) ont été retenus. De plus, lorsqu'une version d'un même article a été mise à jour, la version la plus récente a été sélectionnée. Enfin, puisque la page de résultats de Gartner en est une de type défilement continu (*endless scroll*) et que les résultats sont classés par ordre de pertinence, nous avons arrêté la recherche lorsque les résultats n'étaient plus jugés pertinents dans le cadre du présent mémoire, à savoir lorsqu'au moins une dizaine d'articles consécutifs ne contenaient pas les informations clés nécessaires pour

atteindre nos deux sous-objectifs de recherche. Au total, 13 articles provenant de Gartner ont été ajoutés à notre échantillon.

L'échantillon obtenu à la fin de cette étape de tri était donc constitué de 95 articles académiques et professionnels (voir Figure 3.1), à savoir ceux qui avaient reçu une cote 4 ou 5.

3.4 Étape 3 : Extraction de données

L'extraction des données dans le cas d'une revue de littérature se base sur le codage minutieux des articles identifiés à l'étape précédente. Pour ce faire, chaque article a été lu attentivement et a été codé au moyen d'une grille de codage (voir Annexe 2, qui présente un extrait du tableau Excel utilisé). Nous avons suivi une logique déductive, à savoir que nous nous sommes basés sur un guide (voir Annexe 1) contenant des catégories déjà établies (Xiao et Watson, 2019). Cela a permis notamment de faire ressortir les différents termes et définitions du comportement utilisés, les actions du comportement, les dimensions étudiées, les cadres théoriques ainsi que des informations sur les méthodologies de recherche telles que les méthodes employées, les mesures utilisées, l'échantillon à l'étude et l'utilisation du concept comme variable. Les différents sujets étudiés étaient représentés dans les colonnes et les articles dans les rangées. L'objectif était de recueillir autant d'informations pertinentes que possible, dans chaque colonne et en portant une attention particulière au nom donné au concept du comportement sécuritaire, à la définition et aux dimensions étudiées. De la même manière que pour le tri des articles (l'étape 2), une information est jugée pertinente si elle contribue à atteindre les deux sous-objectifs de recherche.

Le codage des articles était plutôt aisé avec les articles cotés 5, soit les plus pertinents, cependant, pour la plupart des articles cotés 4, il était souvent difficile de trouver des éléments de réponse suffisamment complets pour atteindre les deux sous-objectifs de recherche. Dans les cas où le texte de l'article ne nous permettait pas de trouver les

informations recherchées, nous consultions alors les items des questionnaires ou les annexes afin d'y trouver plus d'indices. Il est à noter que le codage des articles a été effectué par une seule personne, il n'y a donc pas lieu de calculer le taux de fiabilité intercodeur (Okoli et Schabram, 2010). Nous sommes conscients que cela augmente le risque de biais et, afin de l'atténuer, des rencontres régulières ont été tenues avec la directrice de recherche afin de discuter du processus de codage et des articles codés. D'ailleurs, cette explication s'applique aussi au tri des articles de l'étape 2.

Lors du tri des articles à l'étape précédente, pour qu'un article reçoive une cote 4 ou 5, on devait au moins pouvoir retrouver facilement le nom du concept, une définition sinon des actions d'un comportement sécuritaire, ainsi que la dimension étudiée. Toutefois, la lecture plus détaillée effectuée lors du codage des articles, nous a menés à rétrograder 12 articles de la cote 4 à la cote 3. Ces articles ont été donc exclus de l'échantillon final puisqu'ils ne contenaient pas des informations clés et n'étaient donc pas considérés comme pertinents dans le cadre de la présente recherche.

De plus, six articles cotés 4 initialement ont reçu une cote « 4+ », car ils étaient jugés plus pertinents que les autres articles de la même catégorie, mais pas suffisamment pertinents pour être classés dans la cote 5. Nous avons décidé de garder une trace de ces articles « cote 4+ » au cas où il y aurait lieu de mettre davantage d'attention par rapport aux autres articles de la cote 4 dans le cadre de l'analyse des données.[4]

Par ailleurs, un article de la cote 4 a été reclassé dans la cote 5 en raison de son niveau de pertinence très élevé, car même si le comportement sécuritaire n'y est pas le sujet principal, le sujet qui y était étudié a une influence importante sur le comportement et nous a permis de recueillir un grand nombre d'informations essentielles.

Le Tableau 3.2 présente les changements effectués au cours de cette étape. L'échantillon obtenu à la fin du codage (l'échantillon final) est de 83 articles, soit les articles cotés 4, 4+ et 5. La décision d'exclure de l'échantillon les cotes 1, 2 et 3 (voir le

[4] La cote 4+ n'a finalement pas été pertinente. L'analyse séparée des articles de la cote 4+ n'a révélé aucune particularité ou tendance digne de mention dans le chapitre 4.

tableau 3.1 pour les critères de ces catégories) a d'ailleurs été indirectement confirmée lors de cette étape de codage. En effet, les articles de la cote 4 se sont révélés « passablement » pertinents et toute catégorie inférieure à la cote 4 aurait été peu pertinente.

Tableau 3.2 Répartition des articles avant et après le codage

Catégorie	Nombre d'articles après le tri (à la fin de l'étape 2)	Nombre d'articles après le codage (à la fin de l'étape 3)*
Cote 1	86	86
Cote 2	83	83
Cote 3	79	**91**
Cote 4	58	**39**
Cote 4+		**6**
Cote 5	24	**25**
Littérature professionnelle (Gartner)	13	13
Nombre d'articles inclus dans l'échantillon retenu pour l'étape suivante	95	**83**

*Les chiffres en gras indiquent les changements qui ont eu lieu lors de l'étape de l'extraction des données.

3.5 Étape 4 : Analyse de données

Afin d'analyser les données recueillies selon notre grille de codage, nous avons effectué un processus en deux temps, soit une préanalyse pour relever les éléments qui ressortent à ce stade-là, suivie d'une analyse détaillée par thèmes pour nous permettre d'atteindre les deux sous-objectifs de recherche. Les sous-sections qui suivent décrivent ces analyses.

Préanalyse de l'échantillon d'articles et le profil général de l'échantillon

Dans un premier temps, la préanalyse nous a donné une description de l'échantillon et un premier regard sur le contenu de la littérature au sujet du comportement sécuritaire. Cette étape nous a ensuite permis de dresser un profil bibliométrique des articles à l'étude, au moyen de données quantitatives recueillies à partir de la grille de codage.

Les grilles respectives des articles cotés 4 et 5 (y compris 4+) nous ont servi lors de l'étape de préanalyse. Tout d'abord, puisque la grille de codage prend la forme d'un vaste tableau, nous faisions d'emblée une analyse intra-article en le remplissant lors de chaque lecture. Lors de cette étape, des données quantitatives ont été recueillies afin de comparer distinctement le contenu des cotes 4 et 5 pour nous permettre de voir si ces catégories se ressemblent ou encore se démarquent de façon significative. Les chiffres représentent le nombre d'articles correspondant aux différentes caractéristiques du comportement et la manière dont elles sont étudiées. Cette étape a notamment mené au constat que les articles de la cote 5 avaient tendance à fournir davantage d'informations sur le comportement sécuritaire que ceux de la cote 4.

Par la suite, les deux catégories ont été mises en commun afin de nous donner un portrait général de l'échantillon de littérature académique (voir le Tableau 3.3). Un constat qui a rapidement émergé de cette préanalyse était la prédominance des études quantitatives. Sur les 70 articles académiques, 49 ont eu recours à une méthodologie quantitative, 10 ont utilisé une méthodologie qualitative, 10 sont de nature conceptuelle et un article utilise une méthode mixte.

Tableau 3.3 Répartition des articles selon la méthodologie qu'ils emploient

Type de méthodologie employée	Nombre d'articles
Méthode quantitative (p.ex. enquête par sondage, recherche expérimentale, méta-analyse)	49
Méthode qualitative (p.ex. étude de cas, *case survey*, enquête qualitative)	10
Article conceptuel	10
Méthode mixte (quantitatif et qualitatif)	1

Par la suite, le même type de données a été recueilli dans la grille des articles de la littérature professionnelle (à l'exception des informations sur la méthodologie qui n'apparaissent pas habituellement dans ce type d'article), mais ces données ont été traitées distinctement de celles de la littérature académique afin de nous permettre de

voir comment ces deux types de littérature se comparent. Cela a notamment fait ressortir un écart entre les aspects du comportement abordés dans la littérature académique et ceux de la littérature professionnelle.

Lors de la préanalyse, nous avons pu faire deux constats intéressants concernant le profil bibliométrique de notre échantillon d'articles (voir Annexe 3). Premièrement, les articles composant l'échantillon final proviennent d'un grand nombre de revues différentes et parmi les publications qui reviennent le plus fréquemment on retrouve Computers and Security (14), Information and Computer Security (8), Computers in Human Behavior (5), Information Technology and People (5) et Journal of the Association for Information Systems (4). La vaste majorité des articles académiques (57) proviennent du domaine des TI, et un de ces articles utilise également des éléments de la psychologie comportementale. Les autres articles, pour leur part, sont issus du domaine du management (9) et de *health informatics* (2). Toutefois, peu d'articles à ce jour ont été publiés dans les revues les plus influentes en TI, telles que celles listées dans le « Senior Scholar's Basket of Eight [5] » de l'*Association for Information Systems.* Quatre d'entre eux proviennent du *Journal of the Association for Information Systems*, deux proviennent du *European Journal of Information Systems* et un article provient de *Information Systems Research.*

Deuxièmement, les articles de l'échantillon couvrent la période de 2007 à 2021, avec la majorité d'entre eux datant de 2015 et après (voir la figure 3.2). Puisque le sujet étudié ici est plutôt récent, nous n'avons pas limité l'année de publication des articles, car il était question d'avoir le plus de sources pertinentes possible, mais aussi de voir comment le comportement sécuritaire a été étudié au fil du temps.

[5] Association for Information Systems, « Senior Scholars' Basket of Journals ». Récupéré de https://aisnet.org/page/SeniorScholarBasket

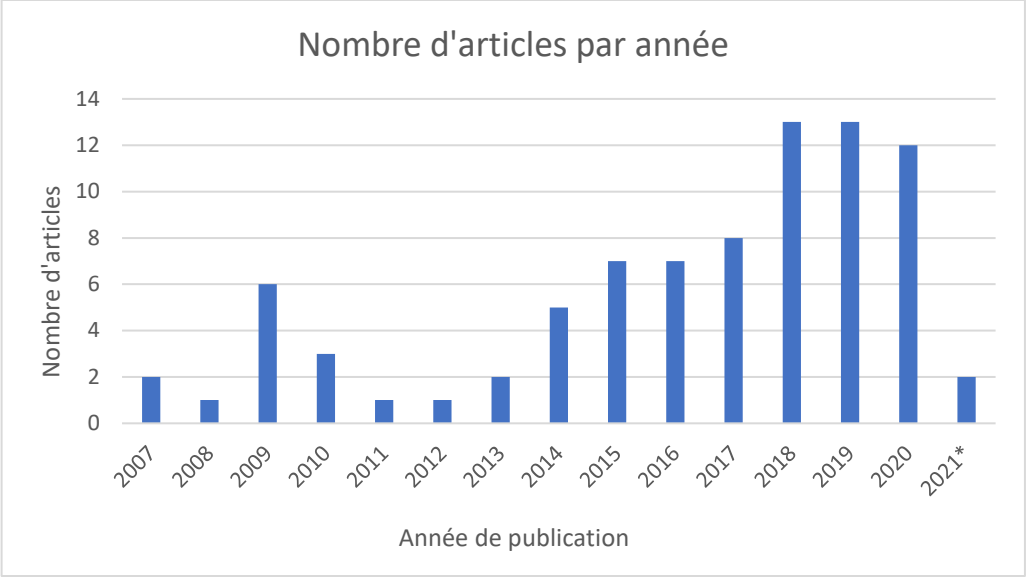

Figure 3.2 Répartition des articles de l'échantillon par année de publication

* La recherche d'articles a été faite en mars et ce chiffre ne reflète pas l'ensemble des articles qui ont été ou qui seront publiés en 2021.

En somme, les données quantitatives recueillies dans la phase de préanalyse nous ont permis de jeter un premier regard sur des aspects fondamentaux du comportement sécuritaire et sur la manière dont le concept est étudié. La préanalyse a, par ailleurs, fait ressortir que notre échantillon est majoritairement constitué d'articles récents du domaine des TI. De plus, les données quantitatives ont également servi de point de départ pour l'analyse qualitative qui a suivi, puisqu'elles ont permis de faire ressortir certaines pistes à analyser.

Analyse détaillée de l'échantillon d'articles

Nous avons ensuite procédé à l'analyse principale des données recueillies, qui en est une de nature qualitative interarticles. Le but de celle-ci est de nous permettre de recueillir et rassembler les informations nécessaires pour atteindre nos deux sous-objectifs de recherche. Dans un premier temps, il a fallu identifier les principaux éléments de réponses requis. Ainsi, pour répondre à l'objectif général, celui de proposer une définition conceptuelle du comportement sécuritaire, il faut d'abord voir quelles

définitions existent déjà et quelles appellations du concept sont utilisées dans la littérature, de même que les actions qui constituent un tel comportement. Ensuite, on doit pouvoir identifier les caractéristiques de chaque dimension et voir si des articles étudient plus d'une dimension et la manière dont ces dimensions sont liées.

Afin de recueillir les données mentionnées, des tableaux thématiques ont été créés. Par exemple, à la suite de la préanalyse qui nous a permis d'identifier 23 articles proposant une définition du comportement sécuritaire, nous avons conçu un tableau contenant ces définitions et les noms de concepts correspondants (Annexe 4). La préanalyse a également fait ressortir qu'un plus grand nombre d'articles mentionnaient des actions plutôt que des définitions. Alors, un tableau regroupant les actions proposées par les articles, ainsi que les noms de concepts et les dimensions étudiées a été créé (Annexe 5). Enfin, un tableau contenant les liens entre les dimensions a également été créé (Annexe 6).

À partir des données contenues dans ces tableaux, nous avons procédé à un codage des informations qu'ils contiennent, en attribuant un code (en lettres) et une couleur correspondant à un thème ayant émergé des données. Nous avons analysé les articles de la littérature académique et de la littérature professionnelle dans un même tableau, mais les deux catégories étaient placées l'une à la suite de l'autre pour les distinguer, au cas où des différences significatives entre les deux ressortiraient.

Par ailleurs, au cours de l'analyse interarticles, nous avons relevé des contradictions entre les propos de certains chercheurs, les avons notés en commentaire dans la grille de codage et avons identifié les sujets qui pouvaient donner lieu à un débat. Une analyse de discours (Wall *et al.*, 2015) a été effectuée à partir de ces sujets, qui se présentaient souvent sous la forme « thèse - antithèse ». Les arguments de chaque parti ont été recensés, puis mis en comparaison.

En somme, la revue de littérature systématique présentée dans ce chapitre nous a permis d'examiner d'une manière rigoureuse la littérature académique et professionnelle afin de trouver des éléments qui devraient nous permettre de répondre

à notre objectif général de recherche. L'examen de ces deux types de littérature nous a fait état des connaissances actuelles sur le comportement sécuritaire et a confirmé l'existence d'un flou autour du concept. Enfin, l'analyse en deux temps nous a permis d'identifier et de rassembler les éléments nécessaires à la compréhension du comportement sécuritaire dans le but de pouvoir proposer une définition plus claire et uniforme. Les résultats de l'analyse principale sont consignés dans le chapitre 4.

Chapitre 4. Analyse et résultats

Ce chapitre présente les résultats de l'analyse des articles issus de la revue de littérature systématique et explique comment nous avons identifié les éléments de réponse clés à nos deux sous-objectifs de recherche. Rappelons que devant le flou et le manque de consensus existant autour du concept de comportement sécuritaire dans la littérature, notre objectif général est de proposer une définition conceptuelle du comportement sécuritaire pour la protection de l'actif informationnel. Ainsi, nous débutons ce chapitre en présentant l'analyse des aspects fondamentaux du comportement sécuritaire, soit les noms donnés au concept, les définitions et les actions. Par la suite, nous nous attarderons aux dimensions qui constituent le comportement sécuritaire et, enfin, nous examinerons les relations entre les dimensions évoquées dans la littérature.

4.1 Aspects fondamentaux du comportement

4.1.1 Termes utilisés et définitions

Pour débuter notre analyse, nous avons d'abord tenté de comprendre les termes utilisés dans la littérature pour désigner le concept de comportement sécuritaire. Pour ce faire, nous avons utilisé les filtres d'Excel dans notre tableau contenant le codage (voir un extrait à l'annexe 2) pour faire ressortir certaines catégories, telles que les noms de concept, les définitions ou les dimensions. Ensuite, nous avons cherché les termes dans les colonnes des catégories concernées (p.ex. « security » et/ou « behavior » dans le nom de concept) et avons compté les entrées correspondantes. Pour identifier le nombre d'articles proposant ou non une définition, ainsi que pour identifier les dimensions qui y sont associées, nous avons filtré les codes correspondants (p.ex. code pour la présence d'une définition, code pour la définition d'un concept connexe, code pour l'absence de définition) et avons compté les résultats. À première vue, les résultats se présentaient comme un ensemble plutôt disparate, mais nous avons été en mesure

d'identifier plusieurs thèmes communs (voir le tableau 4.1). Nous avons ainsi pu identifier que les mots « security » et « behavior » se retrouvent dans la majorité des termes utilisés pour désigner le comportement. L'expression la plus fréquente est « information security » (32 articles sur 83 ou 39%) et elle est le plus souvent combinée à « behavior » ou parfois « compliance ». Alors que « information security compliance » désigne, comme son nom l'indique, des comportements conformes, l'expression « information security behavior », quant à elle, englobe autant des comportements relevant de la conformité, de l'éthique et du jugement. Il faut dire que la majorité des articles utilise un nom de concept n'identifiant pas explicitement la dimension du comportement. Toutefois, certains articles emploient des noms contenant « compliance », « ethics » ou « judgement », de manière à identifier la dimension étudiée. Par ailleurs, nous considérons une dimension explicitement identifiée lorsque le nom du concept contient le terme correspondant (soit compliance, ethics ou judgement) ou lorsque le terme correspondant n'est pas présent dans le nom du concept, mais que la dimension étudiée est identifiable dans le texte, immédiatement après la mention du concept. Ainsi, les termes *Computer security behavior* et *Conscious care behavior*, bien qu'ils ne contiennent pas le mot « judgement », ont été associés au jugement, car leur description permettait une identification rapide de la dimension, dès leur première mention.

Tableau 4.1 Identification du concept de comportement sécuritaire : termes utilisés et définitions

Caractéristiques	Nombre d'articles (sur 83)	Exemples
Termes utilisés		
Contient au moins « security »	57	Online security behavior, Information security compliance, Computer security behavior
Contient au moins « behavior »	52	Information protection behavior, Safe behavior, Privacy-protective behavior
Contient l'expression « information security »	32	Information security behavior, Information security compliance, Information security role of users
Contient un terme désignant un comportement non-sécuritaire	6	Non compliance with information security policy, Unethical information security behavior, Information security policy violation behavior
Ne permet pas d'identifier la dimension du comportement	51	Information security behavior, Computer security behavior, Secure employee behavior
Identifie la dimension *conformité*	23	Security compliance behavior, Information security policy compliance
Identifie la dimension *éthique*	7	Ethical behavior, Digital ethics
Identifie la dimension *jugement*	3	Cybersecurity judgement
Définitions		
Définition du comportement sécuritaire	28	"the behaviors of individuals which relate to protecting information and information systems assets" (Crossler et al., 2019, p.344)
Définition d'un concept connexe	11	Self-efficacy in information security: "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability" (Rhee et al., 2009, p.818)
Aucune définition	43	n/a

Outre l'ambigüité entourant les noms de concept, un autre point de départ ayant motivé la rédaction du présent mémoire a été l'observation d'un manque de consensus assez évident autour de la définition du comportement sécuritaire dans la littérature en sécurité de l'information. L'analyse des définitions contenues dans notre échantillon permet en effet de confirmer ce constat, d'une part à cause d'une absence fréquente de définition (voir Tableau 4.1), d'autre part à cause de la variété d'éléments contenus dans les définitions (voir Tableau 4.3). En effet, parmi tous les articles analysés, près de la moitié (43 articles sur 83 ou 52%) ne donne pas de définition, seulement 28 sur 83 proposent une définition du comportement sécuritaire et quelques articles donnent la définition d'un concept connexe. Nous entendons par « concept connexe » un concept

qui ne désigne pas directement le comportement sécuritaire, mais qui y est étroitement lié, tel que l'auto-efficacité (p.ex. *self-efficacy* dans Rhee et al., 2009). De plus, parmi les articles ne donnant aucune définition, certains (19 sur 43) donnent au moins quelques indices quant à ce qui pourrait constituer un comportement sécuritaire, mais ce n'est pas le cas pour la majorité des articles. De manière générale, les constats sont très similaires entre la littérature académique et la littérature professionnelle, c'est-à-dire que la plupart des articles ne donne pas de définition et quelques-uns offrent une définition soit du comportement sécuritaire soit d'un concept connexe.

Ensuite, nous avons procédé à une analyse plus détaillée des définitions au moyen d'un codage thématique, à partir duquel nous avons pu identifier certains éléments récurrents, qui ont été identifiés au moyen d'un code, comme l'illustre l'exemple du tableau 4.2. Il est à noter que lors du codage complet, nous avions utilisé des couleurs par la suite pour faciliter le comptage, lorsque nécessaire.

Tableau 4.2 Exemple d'un extrait du codage des définitions

Auteur	Nom du concept	Définition
Crossler et al. (2019)	Security behavior	"the behaviors of individuals which relate to protecting information and information systems assets" (p.344) **[P]**
Hsu et al. (2015)	In-role behavior Extra-role behavior	"in-role behaviors, which are required or expected organizational behaviors that are the basis of regular and ongoing job performance evaluations and are linked to rewards and punishments" **[C]** "Accordingly, mindful employees should be motivated to pay attention to others' behaviors in an interdependent context and thus engage in extra-role behaviors such as performing altruistic behaviors to aid others [...]and speaking up with the intent to improve organizational functioning" (p.283) **[Eval]**
Khatib et Barki (2020)	Information security noncompliance	"Information security violations occur when employees contravene an organization's ISP, which provides them with instructions about what they should do to safeguard their organization's information and technology resource" (p.486) **[NS]**
Vedadi et Warkentin (2020)	Secure behavior	Définition de la variable behavioral intention: "Users' intention to use a particular security solution" (p.450) **[I]**

Légende : **[P]** Idée de protection des systèmes et/de l'actif informationnel; **[Eval]** Idée de songer aux conséquences, évaluer la situation, s'adapter, prendre des initiatives; **[C]** Idée de conformité/suivre les politiques; **[NS]** Comportement non sécuritaire; **[I]** Intention seulement

Cette analyse plus approfondie des articles académiques proposant une définition du comportement sécuritaire a fait émerger trois thèmes principaux présents dans les définitions : (1) protéger les systèmes ou l'actif organisationnel, (2) suivre les politiques et les recommandations de l'organisation, et (3) évaluer une situation, songer aux conséquences de ses actions, s'adapter à une nouvelle situation ou prendre des initiatives pour favoriser la sécurité (voir le tableau 4.3). Mentionnons également que quelques définitions correspondent à un comportement non sécuritaire, alors que certaines définitions renvoient à l'intention d'un comportement (voir les lignes (4) et (5) dans le tableau 4.3).

D'autre part, dans la littérature professionnelle, les cinq articles proposant une définition du comportement sécuritaire mentionnent tous explicitement un aspect éthique au comportement, ou au moins l'idée de réfléchir à ses propres actions et aux conséquences qui pourraient en découler. Par ailleurs, dans cette catégorie de la littérature, il n'y a aucune utilisation de l'intention du comportement, c'est toujours le comportement réel qui constitue la variable dépendante (VD).

Tableau 4.3 Principaux thèmes identifiés dans les définitions du comportement sécuritaire

Aspect du comportement sécuritaire contenu dans la définition	Auteurs
(1) Idée générale de protection des systèmes et/ou de l'actif informationnel	**Littérature académique** : Burns et al. (2019); Crossler et al. (2019); Hwang et Cha (2018); Kim et Kim (2017); Omidosu et Ophoff (2016); Rhee et al. (2009); Safa et al. (2016); Williams et al. (2014); Zauwiyah et al. (2019)
	Littérature professionnelle : aucun
(2) Idée de conformité/suivre les politiques	**Littérature académique** : Boss et al. (2009); Doherty et Tajuddin (2018); Donalds et Osei-Bryson (2020); Hsu et al. (2015); Omidosu et Ophoff (2016)
	Littérature professionnelle : Kim et al. (2020)
(3) Idée de songer aux conséquences, évaluer la situation, s'adapter, prendre des initiatives	**Littérature académique** : Boss et al. (2009); Dang-Pham et al. (2017); Hsu et al. (2015); Lin et Wittmer (2017); Ng et al. (2009); Safa et al. (2015)
	Littérature professionnelle : Buytendijk (2017); Buytendijk et al. (2020b); den Hamer et al. (2020); Scholtz et al. (2015)
(4) Comportement non sécuritaire	**Littérature académique** : Chu et So (2020); Khatib et Barki (2020)
	Littérature professionnelle : aucun
(5) Comportement défini par une intention	**Littérature académique** : Abraham et Chengalur-Smith (2019); Hwang et Cha (2018); Kim et Kim (2017); Vedadi et Warkentin (2020); Williams et al. (2014)
	Littérature professionnelle : aucun

Par ailleurs, lors du codage des articles académiques, il a été constaté que la majorité des études proposant une définition au comportement sécuritaire utilisent une approche quantitative, en l'occurrence une enquête par questionnaire et quelquefois une recherche expérimentale. De plus, seuls deux articles sur les dix utilisant une méthodologie qualitative (dans ce cas-ci une enquête qualitative) offrent une définition et deux articles sur les dix de nature conceptuelle font de même. Ce constat est quelque peu étonnant, car les études qualitatives et conceptuelles sont très propices pour le

développement de définitions (MacKenzie *et al.*, 2011) et cet atout ne semble pas avoir été exploité dans la littérature Infosec.

Il a également été observé que les articles utilisant l'intention du comportement comme VD avaient tous recours à une méthodologie quantitative, mais que tous les articles qualitatifs et conceptuels utilisaient le comportement réel comme VD. Selon notre revue systématique, ces éléments donnent l'impression que des étapes auraient été sautées puisque la majorité des termes utilisés ou des définitions n'ont pas été validés empiriquement dans ces études quantitatives. De plus, ces dernières ont tendance à tout de suite établir un lien de causalité, sans que l'on sache précisément comment les variables ont été mesurées. Partant de ce constat et du fait que l'emploi de l'intention comme VD au détriment du comportement réel a été critiqué par plusieurs auteurs, les études qualitatives font un pas en avant en utilisant le comportement réel comme VD. Cependant il y manque une définition du concept la plupart du temps.

En somme, l'analyse des définitions proposées par les 28 articles permet de faire ressortir la multidimensionalité du concept de comportement sécuritaire. En effet, il est déjà possible de distinguer des comportements relevant de la conformité, ainsi que des comportements allant au-delà de la conformité, c'est-à-dire basés sur des principes éthiques et allant même au-delà de l'éthique. Par ailleurs, peu importe la dimension évoquée, bon nombre de définitions nous indiquent qu'un comportement sécuritaire en est un qui consiste à protéger l'actif informationnel d'une organisation, mais aucune définition ne mentionne concrètement les moyens pour y parvenir. Pour cette raison, il devient pertinent d'examiner les actions du comportement sécuritaire dans la littérature. Il faut dire que la majorité des articles qui offrent une définition proposent également des actions associées à un comportement sécuritaire. De plus, la grille contenant le codage nous a permis d'observer que plusieurs articles ne donnant pas de définition du comportement sécuritaire ou définissant seulement un concept connexe proposent en contrepartie des actions correspondant à un tel comportement. Ces informations supplémentaires aideront à améliorer la compréhension de ce qui

constitue un comportement sécuritaire et serviront à mieux décrire les dimensions du comportement plus loin dans ce chapitre.

4.1.2 Actions du comportement

Afin de mieux comprendre ce que désigne le concept de comportement sécuritaire, nous avons analysé comment il se manifeste, c'est-à-dire de voir les actions qui, selon la littérature, peuvent constituer un tel comportement. Ainsi, l'examen de notre échantillon a permis de déceler initialement deux catégories d'actions : celles qui sont liées à des pratiques de sécurité non techniques, telles que suivre des formations ou rapporter des incidents et celles qui sont liées à des pratiques de sécurité techniques comme l'utilisation d'un logiciel antivirus. Il faut néanmoins mentionner que certaines actions comme le choix d'un mot de passe fort ou l'installation d'une application de sécurité pouvaient autant être considérées comme des pratiques techniques que des pratiques non techniques dépendamment des études. Pour cette raison cette manière de classer les actions a été rejetée. Le manque de clarté entre les frontières de ces catégories nous a donc poussés à examiner les actions du comportement sous d'autres angles, ce qui nous a permis d'identifier une autre classification des actions, à savoir selon leur observabilité.

Nous avons ainsi tenté de déterminer les actions observables, c'est-à-dire pouvant être perçues par autrui, qui s'inscrivent dans un comportement sécuritaire. Celles-ci offrent notamment davantage d'objectivité que des actions rapportées par un individu, dans le cadre d'une auto-évaluation, par exemple. Nous avons procédé à un codage thématique des actions selon leur facilité d'observation, un peu de la même manière que pour le codage des définitions (voir l'exemple du tableau 4.4). Le tableau 4.5 présente ensuite la répartition des articles selon l'observabilité des actions qu'ils présentent.

Tableau 4.4 Exemple d'un extrait du codage des actions

Article	Concept utilisé dans l'article	Actions observables du comportement
Burns et al. (2019)	Protection motivated behaviors	Se rappeler entre collègues les pratiques à adopter, reconnaitre et rapporter un comportement suspect d'un employé **[AO]** être sensibilisé aux politiques de sécurité, se conformer aux politiques **[F]**
Khatib et Barki (2020)	Information security non compliance	(actions d'un comportement non sécuritaire) **[NS]**: copier des données confidentielles sur une clé USB non sécurisée pour pouvoir travailler de la maison, laisser son ordinateur ouvert pour ne pas perdre de temps avec le démarrage, partager un mot de passe avec un collègue pour pouvoir terminer une tâche urgente plus rapidement **[AO]**
Ng et al. (2009)	Computer security behavior	Mots de passe forts, faire régulièrement des copies de sauvegarde, précautions et vérification avec les pièces jointes des courriels, s'informer sur les pratiques de sécurité **[DO]**

Légende : **[AO]** Actions aisément observables; **[DO]** Actions difficilement observables; **[NS]** Actions non-sécuritaires; **[F]** Actions floues/mal définies ou impossibles à observer

Tableau 4.5 Classification des actions du comportement sécuritaire selon leur facilité d'observation

Types d'actions selon leur observabilité	Auteurs
(1) Actions aisément observables Exemples : suivre des formations, rapporter des incidents de sécurité, verrouiller son ordinateur, ne pas laisser d'informations sensibles sur son bureau	**Littérature académique** : Albrechtsen (2007); Burns et al. (2019); Chowdhury et al. (2018)*****; Chu et So (2020)*****; Da Veiga et Eloff (2010); Hsu et al. (2015); Karjalainen et al. (2020); Khatib et Barki (2020)*****; Kim et Kim (2017); Li et al. (2019); Lin et Wittmer (2017); Safa et al. (2015); Sommestad (2018)*****; Takemura (2011); Van Slyke et Belanger (2020)*****
	Littérature professionnelle : Buytendijk et al. (2020a)
(2) Actions plus ou moins observables Exemples : gestion des mots de passe, prudence avec les courriels, copies de sauvegarde régulières, utilisation de technologies de protection	**Littérature académique** : Albrechtsen (2007); Connolly et al. (2017); Karjalainen et al. (2020); Klein et Luciano (2016); Li et al. (2019); Mamonov et Benbunan-Fich (2018); Ng et al. (2009); Parsons et al. (2010); Rhee et al. (2009); van Bavel et al. (2019); Van Slyke et Belanger (2020)*****; Weems et al. (2018); Williams et al. (2014)
	Littérature professionnelle : Buytendijk (2017); Buytendijk et al. (2020a); Buytendijk et al. (2020b); den Hamer et al. (2020); Huisman (2018a)
(3) Actions difficilement observables ou floues/mal définies Exemples : suivre les politiques organisationnelles en matière de sécurité, se conformer aux lois et aux règlementations, être sensibilisé à la sécurité de l'information	**Littérature académique** : Boss et al. (2009); Burns et al. (2019); Cavallari (2012); Chowdhury et al (2020)*****; Herath et Rao (2009a); Herath et Rao (2009b); Hsu et al. (2015); Hwang et Cha (2018); Kajtazi et al. (2018)*****; Kim et Han (2019); Kim et Kim (2017); Safa et al. (2015); Safa et al. (2016); Sommestad et al. (2015b); Wall et al. (2013); Yan et al. (2018); Yazdanmehr et Wang (2016)
	Littérature professionnelle : Buytendijk (2017); Buytendijk et al. (2020a); Noakes-Fry et Carpenter (2008); Reed et al. (2020)

Note : Les références contenant le symbole « * » mentionnent des actions d'un comportement non-sécuritaire

Ainsi, la plupart des actions que nous avons jugées aisément observables (voir la ligne (1) dans le tableau 4.5) relèvent d'une interaction avec un autre individu, par exemple rapporter des comportements suspects ou des incidents, aider ses collègues à appliquer des pratiques de sécurité, consulter des experts en sécurité, suivre des formations ou faire preuve d'initiative en émettant des suggestions pour améliorer la sécurité. On retrouve également certaines actions observables ne nécessitant pas d'interaction, telles que verrouiller son ordinateur ou ne pas laisser d'informations sensibles sur son

bureau. De plus, parmi les articles identifiant des actions non-sécuritaires, la même tendance est observée, à savoir que les actions les plus facilement observables découlent d'une interaction. Ainsi, on relève le partage de mots de passe, le fait de donner un accès non autorisé à autrui, l'évitement des formations ou le fait de ne pas rapporter les incidents comme principales actions non-sécuritaires. D'autre part, parmi les actions où il n'y a pas d'interaction figurent l'omission de verrouiller son ordinateur, les mots de passe écrits sur un papier et le fait de laisser des informations sensibles sans surveillance à son poste de travail.

Néanmoins, si bon nombre d'articles nous informent sur des actions concrètement observables du comportement sécuritaire (ou non sécuritaire), il y en a tout autant qui décrivent ce type de comportement avec des actions difficilement perceptibles (voir la ligne (2) dans le tableau 4.5), dans la mesure où il s'agit d'actions que l'on ne peut observer simplement dans le cadre des tâches quotidiennes des employés. Les actions les plus fréquemment mentionnées sont de choisir des mots de passe forts, faire attention avec les courriels et surtout avec leurs pièces jointes, effectuer régulièrement des copies de sauvegarde, faire preuve de prudence avec les téléchargements et utiliser des technologies de protection (p.ex. les antivirus, les pare-feux et les bloqueurs de *pop-ups*).

Enfin, plusieurs articles mentionnent des actions du comportement sécuritaire qui sont très vagues, voire impossibles à observer (voir la ligne (3) dans le tableau 4.5). On parle ici d'actions telles que suivre les politiques en matière de sécurité de l'organisation, se conformer aux lois et aux règlementations et être sensibilisé à la sécurité ou aux politiques de sécurité. Ces actions sont jugées imprécises, car les politiques de sécurité peuvent grandement varier d'une organisation à l'autre et on ne peut pas vraiment savoir ce qui constitue le respect des politiques. Il est difficile de dire s'il s'agit, par exemple, de suivre les consignes à la lettre ou d'appliquer les lignes directrices de la politique selon le cas. De plus, quelques articles étudiant les dimensions « éthique » ou « jugement » mentionnent des actions vagues telles qu'évaluer les risques, s'adapter à une situation, réfléchir aux conséquences et prendre responsabilité de ses actes.

Néanmoins, la majorité des articles mentionnant des actions vagues étudient l'aspect de la conformité et ils utilisent, pour la plupart, *Information Security Policy Compliance* ou une variation similaire comme nom de concept. Il est intéressant, par ailleurs, de constater que bon nombre d'articles qui emploient *Information Security Policy Compliance, ISP Compliance* ou une variation semblable ne proposent pas de définition (p.ex. Herath et Rao, 2009a; Sommestad *et al.*, 2015), ou alors ils donnent une définition tautologique du concept de comportement sécuritaire ou d'un concept connexe (p.ex. Wall *et al.*, 2013). De plus, certains de ces articles ne donnent ni définition ni actions du comportement sécuritaire (p.ex. Siponen *et al.*, 2014). Bref, ces articles semblent tenir pour acquis que la définition est connue et acceptée par tous et que tous s'entendent qu'un comportement de conformité équivaut à un comportement sécuritaire. Il est à noter que ces articles proviennent tous de la catégorie Cote 4 (c.-à-d. des articles dont le comportement sécuritaire n'est pas le sujet principal, mais qui contiennent des éléments connexes pertinents permettant de comprendre ce concept).

Le codage détaillé des définitions du comportement a ainsi permis d'identifier des thèmes communs dans un ensemble de données plutôt disparates à première vue et le codage des actions a fait ressortir l'importance d'avoir des repères concrets quant à ce qui constitue un comportement sécuritaire. De plus, un examen plus approfondi a mis en lumière l'existence d'arguments divergents concernant l'utilisation de l'intention du comportement comme mesure et l'utilisation du comportement réel, notamment avec certains chercheurs remettant en question la pertinence de l'intention seule. Les paragraphes qui suivent détaillent davantage ces arguments.

4.1.3 Intention vs comportement réel

En examinant de plus près les noms de concepts ainsi que les définitions, il est possible d'observer une certaine dichotomie entre les études qui s'intéressent à l'intention d'un

comportement sécuritaire et celles qui s'intéressent au comportement réel. Comme le soulèvent Crossler *et al.* (2013), il est compréhensible que les chercheurs aient parfois recours à l'intention comme mesure du comportement en raison des « difficultés liées à l'observation et à la collecte de données sur le comportement réel en contexte de sécurité de l'information » (p.95, traduction libre). Cependant, nous avons pu remarquer que certains auteurs sont persuadés de l'efficacité de l'intention comme mesure, tandis que d'autres critiquent cette approche et appellent à l'utilisation du comportement réel comme mesure.

D'une part, les chercheurs qui prônent l'utilisation de l'intention se basent principalement sur l'idée que des théories bien établies sur le comportement ont démontré l'efficacité de cette approche. Par exemple, certains auteurs soutiennent que la *Theory of planned behavior* (TPB) permet d'expliquer le lien entre l'intention du comportement et le comportement réel (Kim et Kim, 2017) ou encore que cette théorie est suffisante à elle seule pour expliquer l'intention de se conformer (Sommestad 2015b). De plus, Sommestad (2018) affirme que la TPB a donné les résultats les plus constants dans la littérature et explique le mieux le comportement via l'intention. En somme, ces auteurs avancent que la TPB démontrerait bel et bien que l'intention mène au comportement. Par ailleurs, une autre théorie fréquemment citée en Infosec, la *Protection motivation theory* (PMT), expliquerait adéquatement elle aussi l'intention de suivre les pratiques et politiques (Abraham et Chengalur-Smith, 2019). Enfin, selon Williams *et al.* (2014) le Health Belief Model (HBM) explique et prédit bien les comportements préventifs, surtout lorsqu'on y ajoute l'auto-efficacité et l'intention. Cependant, il est à noter que deux autres études dans notre échantillon se basent sur le HBM (c.-à-d. Li *et al.*, 2019; Ng *et al.*, 2009) et mesurent le comportement réel plutôt que l'intention. Il est également intéressant de constater que tous ces articles avaient reçu une Cote 4, ce qui donne l'impression que les études qui se concentrent sur l'intention d'un comportement ne font pas partie des plus pertinentes.

En contrepartie aux arguments soutenant l'utilisation de l'intention comme mesure, plusieurs chercheurs ont soulevé l'idée qu'il faut plutôt mesurer le comportement réel

puisque l'intention seule ne suffit pas. En effet, les théories et les modèles couramment utilisés dans la littérature Infosec ont tendance à évaluer l'intention plutôt que le comportement, mais en réalité, les actions des employés peuvent différer de leurs intentions (Alohali *et al.*, 2017). D'autre part, Li *et al.* (2019) soutiennent que le comportement rapporté par les employés dans le présent est un meilleur indicateur que d'éventuelles actions futures. Selon ces auteurs, certains résultats ambigus dans la littérature entre la PMT et les comportements sécuritaires surviennent à cause de l'utilisation de l'intention comme mesure. Ainsi, les liens entre les variables qui influencent l'intention ne sont vraisemblablement pas les mêmes que les liens entre les variables qui influencent le comportement réel, d'où une remise en question de l'utilisation de la PMT telle quelle (Li *et al.*, 2019). Par ailleurs, Mamonov et Benbunan-Fich (2018) soutiennent un argument similaire au sujet de cette théorie en évoquant le fait que les liens entre les variables découlant de la PMT et l'intention d'un comportement sécuritaire n'ont pas été cohérents au fil des études.

De plus, les intentions ne sont pas toujours suivies du comportement et le lien entre l'intention et l'exécution d'un comportement s'est souvent avéré faible dans la littérature (Shropshire *et al.*, 2015). En effet, dans le cadre de l'étude de Shropshire *et al.* (2015), la majorité des participants a affirmé avoir l'intention d'adopter une mesure de sécurité donnée, mais moins du quart l'a réellement fait par la suite. Les auteurs ont ainsi conclu qu'il y a d'autres facteurs que l'intention qui influencent le comportement et qu'en fait le lien intention-comportement n'est pas direct parce qu'il existe vraisemblablement d'autres variables entre ces deux-là. Cela contribuerait à expliquer la faible fiabilité de la prédiction de l'intention du comportement par d'autres chercheurs (Shropshire *et al.*, 2015).

Enfin, mesurer le comportement réel fonctionne mieux que l'intention, car lorsqu'il est question de sécurité et de protection de l'information, ce sont avant tout les actions et non les intentions qui comptent (van Bavel *et al.*, 2019). Par ailleurs, van Bavel *et al.* (2019) mentionnent que quelques études ont tenté de mesurer le comportement réel, mais que ces études avaient surtout recours à l'auto-évaluation pour mesurer le

comportement. En effet, bon nombre d'études en Infosec comportementale utilisent l'intention ou l'auto-évaluation pour mesurer le comportement et peu d'études, en fait, ont utilisé des mesures objectives (Mamonov et Benbunan-Fich, 2018). Cette observation est également évoquée par Crossler *et al.* (2013) qui soulignent que « les recherches ont démontré que les données provenant d'une auto-évaluation ou celles sur l'intention d'un comportement sont moins précises et fiables que les données provenant de l'observation d'un comportement réel » (p.95, traduction libre).

Ce débat entre l'utilisation du comportement réel par rapport à l'intention du comportement a mis en lumière qu'en plus d'un manque de consensus entourant les définitions du comportement sécuritaire, il ne semble pas y avoir non plus de consensus quant à la manière d'opérationnaliser le concept. En effet, certains articles (p.ex. Safa *et al.*, 2016) définissent leur concept comme un comportement réel, mais mesurent l'intention. D'autres articles (p.ex. Herath et Rao, 2009a) ne définissent pas explicitement le concept et proposent plutôt quelques caractéristiques du comportement sécuritaire qui renvoient à un comportement réel, mais les items du questionnaire mesurent, quant à eux, une intention.

Un examen approfondi des autres aspects fondamentaux, tels que les noms de concept, les définitions et les actions du comportement sécuritaire, a contribué à confirmer le flou autour du concept, mais il a également permis de faire ressortir une caractéristique commune importante, à savoir le but du comportement sécuritaire, qui est d'assurer la protection des systèmes et de l'actif informationnel. Par ailleurs, si les études s'entendent généralement sur ce but, ce qui varie, ce sont les manières de l'atteindre, comme l'illustrent les définitions et les actions proposées par les différents auteurs. Toutefois, cela nous a donné plusieurs indices quant à la multidimensionalité du comportement sécuritaire, tels que les différences de termes utilisés dans les noms de concept et les différents angles abordés dans les définitions, c'est pourquoi nous en avons fait l'objet de la prochaine section de notre analyse.

4.2 Dimensions du comportement sécuritaire

À partir de l'analyse interarticles, nous avons été en mesure de déterminer que le comportement sécuritaire est bel et bien un concept multidimensionnel, c'est-à-dire qu'il contient plus d'une facette distincte qui le caractérise (MacKenzie *et al.*, 2011). En effet, MacKenzie *et al.* (2011) expliquent qu'un concept ou un construit est multidimensionnel si ses facettes sont différentes les unes des autres et si l'élimination de l'« une d'entre elles restreint de manière significative le domaine du construit » (p.301, traduction libre). Ainsi, à la lumière de notre analyse, nous avons conclu que les facettes du comportement, comme la conformité, l'éthique et le jugement, sont des dimensions distinctes et constituent des éléments clés pour la compréhension du concept de comportement sécuritaire (voir Tableau 4.6).

Tableau 4.6 Nombre d'articles selon la dimension étudiée

Dimension	Nombre d'articles (sur 83)	Quelques exemples
Conformité	63	Karjalainen et al. (2020); Noakes-Fry et Carpenter (2008); Parsons et al. (2014); Warkentin et al. (2016)
Éthique	14	Buytendijk (2017); den Hamer et al. (2020); Lankton et al. (2019); Ruighaver et al. (2010)
Jugement	16	Ng et al. (2009); Safa et al. (2015); Walls (2015); Yan et al. (2018)

La présente section s'intéresse donc à décrire chacune des dimensions, de même que leurs caractéristiques. Vers la fin du chapitre, nous abordons également la possibilité que le comportement sécuritaire présente d'autres dimensions que la conformité, l'éthique et le jugement.

4.2.1 Conformité

L'examen systématique de la littérature permet de constater que la conformité est couramment associée au concept de comportement sécuritaire et est parfois décrite comme étant la principale dimension de celui-ci (p.ex. Safa *et al.*, 2016; Warkentin *et al.*, 2016; Yazdanmehr et Wang, 2016). La conformité est par ailleurs fréquemment associée aux politiques organisationnelles, avec 16 articles qui utilisent des expressions telles que « information security policy compliance behavior » (Yazdanmehr et Wang, 2016) ou « information security policy compliance » (p.ex. Sommestad, 2018; Wall *et al.*, 2013). Sans explicitement la définir, les études mentionnées ci-dessus sous-entendent qu'un comportement de conformité consisterait à suivre les règles et principes inscrits dans la politique organisationnelle. En effet, les politiques organisationnelles sont un moyen fréquemment utilisé par les organisations dans le but de former ou d'influencer le comportement de leurs employés à l'égard de la sécurité de l'information (Ifinedo, 2014). Bien que l'importance pour les organisations d'avoir des politiques en matière d'utilisation des technologies a été établie, leur efficacité et leur impact sur les employés ne sont pas toujours clairs, notamment parce que les employés ne s'y conforment pas (Herath et Rao, 2009b).

Plusieurs études se sont intéressées aux facteurs favorisant ou influençant la conformité aux pratiques ou aux politiques organisationnelles (p.ex. Safa *et al.*, 2016; Shropshire *et al.*, 2015; Yazdanmehr et Wang, 2016) sans précisément exposer les avantages qu'apporte l'adoption d'un comportement conforme. Mentionnons que ces études peuvent employer explicitement le terme « conformité » (*compliance*) ou encore des variations de l'expression « comportement sécuritaire » où ce comportement en est principalement un de conformité. Toutefois, l'étude de Safa *et al.* (2016) soulève un avantage aux comportements conformes en mentionnant que l'amélioration du comportement des employés conformément aux politiques organisationnelles constitue un moyen efficace pour mitiger les risques associés à l'erreur humaine, mais

la manière dont un comportement conforme contribue à la réduction des risques n'est pas détaillée.

Enfin, Hsu *et al.* (2015) ont identifié la dimension de conformité avec les *in-role behaviors*, qui sont définis comme des comportements « spécifiés par les politiques de sécurité, incluant l'adoption des comportements attendus ou l'adaptation de son style de travail de manière à satisfaire ces attentes » (p.282, traduction libre). De plus, tel qu'évoqué au chapitre 2, Hsu *et al*. ont également identifié une autre dimension (les *extra-role behaviors*) confirmant ainsi l'importance d'investiguer le comportement sécuritaire sous d'autres angles que seulement celui de la conformité.

4.2.2 Éthique

Outre la conformité, on retrouve dans la littérature Infosec la dimension éthique comme élément du comportement sécuritaire. Il est à noter que six des articles abordant cette dimension sont de nature académique, mais seul celui de Ruighaver *et al.* (2010) décrit en détail le rôle de l'éthique, son importance et ses avantages pour le comportement sécuritaire. Il s'agit également du seul article qualitatif. Les cinq autres articles sont quantitatifs et n'examinent pas en profondeur le rôle de l'éthique. Ils mesurent généralement l'impact de certains facteurs liés à l'éthique sur le comportement, mais sans expliquer le rôle que joue cette dimension.

Nous avons vu au chapitre 2 que l'éthique est un ensemble de principes permettant d'identifier ce qui est bien ou mal en termes de comportements liés à la sécurité de l'information. Ainsi, Ruighaver *et al.* (2010) proposent une réflexion sur le rôle de la dimension éthique dans le développement et l'adoption de comportements sécuritaires et estiment que le comportement des employés ne peut plus être déterminé seulement par le respect des règles établies, notamment par le biais de politiques organisationnelles. Ils soutiennent que les employés doivent comprendre pourquoi certains comportements sont bons et d'autres non. De plus, l'évaluation des enjeux

moraux ou éthiques d'une situation peut favoriser l'adoption d'un comportement sécuritaire (Lankton *et al.*, 2019). En ce sens, plus l'employé a conscience des impacts possibles de la situation, plus il risque d'entreprendre des actions pour assurer la sécurité de l'information.

Par ailleurs, les organisations ne devraient plus s'attendre à ce que leurs employés suivent aveuglément les prescriptions organisationnelles en matière de comportement sécuritaire, et les employés sont sans doute prêts à faire leur part et réfléchir aux conséquences possibles de leurs actes, au-delà de ce qu'on leur recommande (Ruighaver *et al.*, 2010; Sampath, 2019). À cet effet, les organisations gagneraient à aller au-delà des politiques organisationnelles, qui guident les comportements à adopter, et établir des principes éthiques qui permettraient de favoriser le changement comportemental des employées en les sensibilisant aux conséquences possibles de leurs actions (Ruighaver *et al.*, 2010).

À titre d'exemple, Ruighaver *et al.* (2010) ont mené une étude de cas auprès d'une entreprise publique australienne de taille moyenne qui a décidé d'intégrer une sorte de charte éthique à leur politique organisationnelle en matière de sécurité, qui se veut à la fois un complément à celle déjà existante et une manière de l'améliorer. La politique organisationnelle en place était de nature prescriptive et énonçait ce que les employés avaient le droit de faire ou non en matière de sécurité de l'information. En raison de cette nature prescriptive, le document contenant la politique était souvent laissé sur les tablettes par les employés car il établissait les comportements à suivre, mais sans fournir les raisonnements derrière les directives, par exemple en relatant les menaces potentielles pouvant survenir ou les risques que les employés peuvent causer en ne suivant pas les recommandations. Par ailleurs, les employés eux-mêmes avaient admis ne pas nécessairement respecter la politique en place, puisqu'ils ne voyaient pas les impacts de ne pas s'y conformer. La refonte de la politique organisationnelle a donné lieu à un document qui relevait davantage d'un guide que d'une politique et qui a été nommé *Acceptable use guidelines*. Ce nouveau guide, plutôt que de prescrire des comportements comme la version précédente, identifiait plutôt les risques et les

conséquences possibles si les employés ne suivent pas les recommandations. Certes, ces derniers ont toujours le choix de décider comment ils se comportent, mais grâce à ces nouvelles lignes directrices, ils ont pu mieux constater la responsabilité et l'imputabilité qui leur revient selon leurs actions. Ainsi, les employés sont devenus plus conscients des conséquences de leurs actes, ce qui leur a permis de prendre des décisions plus éclairées, favorisant ainsi une meilleure sécurité informationnelle au sein de l'organisation (Ruighaver *et al.*, 2010).

Bien qu'il y existe un corpus littéraire académique portant sur la sécurité TI et l'éthique, nous avons trouvé que la littérature provenant de Gartner offre une perspective nettement plus claire de la mise en pratique de principes éthiques en gestion de la sécurité de l'information. Un concept en particulier a retenu notre attention, celui de « *digital ethics* », qui est défini comme « des valeurs et des principes moraux servant à guider les interactions numériques » (Buytendijk, 2017, p.3 – traduction libre). Selon Gartner, ce concept s'annonce comme une tendance majeure pour les prochaines années (Buytendijk, 2017; Cearley et Burke, 2018) et son importance a été davantage amplifiée à la suite des couvertures médiatiques sur divers incidents de fuites de données, qui ont eu pour effet de réveiller la conscience collective sur la sécurité de l'information (Hare *et al.*, 2018). Le concept de *digital ethics* est inspiré du courant de pensée *Care ethics*, décrit comme l'art de « prendre la responsabilité des conséquences de ses actes, même si elles ne sont pas intentionnelles » et repose donc sur le principe que l'utilisation des technologies et les conséquences qui en découlent se trouvent entre les mains des utilisateurs (Buytendijk, 2017, p.8).

Bien que la majorité des articles de notre échantillon porte sur la conformité, l'éthique propose une vision bien différente et pertinente pour décrire le comportement sécuritaire. Elle implique une réflexion de la part des employés face aux actions qu'ils posent et à leurs conséquences. Cela expliquerait pourquoi cette dimension est utilisée chez certains auteurs qui prônent l'étude du comportement sécuritaire au-delà de la conformité. Quant aux autres auteurs qui prônent l'étude du comportement sécuritaire

au-delà de la conformité, ils abordent une dimension qui semble différente de l'éthique et qui est décrite plus en détail dans la section qui suit.

4.2.3 Jugement

On retrouve dans la littérature portant sur la dimension comportementale en Infosec des études qui font mention d'un aspect du comportement qui va au-delà de la conformité et de l'éthique, comme l'illustrent 16 articles de notre échantillon. Ce concept, dont la dénomination varie d'un article à l'autre, fait généralement référence à l'idée que les utilisateurs réfléchissent aux conséquences en termes de sécurité informationnelle avant de poser une action, développent des réflexes pour mieux protéger l'information et acquièrent une capacité à évaluer les situations avant d'agir ou encore s'adapter à de nouvelles situations dans un contexte Infosec. Des expressions telles que « *computer security behavior* », « *conscious care behavior* », « *cybersecurity judgement* » ou « *proactive information security behavior* » sont employées pour désigner cette idée. Comme il n'y a pas de définition ni de terme commun pour la désigner, nous avions identifié plusieurs liens et similitudes dans la littérature et avions traduit cette dimension par le terme « jugement » au chapitre 2. Ainsi, la présente section vise à présenter les différents concepts provenant de la littérature en lien avec cette dimension du comportement qui va au-delà de la conformité et de l'éthique.

Tout d'abord, un comportement sécuritaire nécessite que l'utilisateur d'une technologie fasse consciemment le choix d'entreprendre des actions supplémentaires dans le but d'assurer la sécurité informationnelle et prévenir des incidents comme une perte de données (Ng *et al.*, 2009). Plus spécifiquement, Ng *et al.* (2009) font une distinction entre les technologies positives, c'est-à-dire celles dont on se sert à des fins pour lesquelles elles ont été conçues et les technologies protectrices, c'est-à-dire celles qui servent à prévenir des conséquences négatives. Ainsi, une utilisation judicieuse des technologies protectrices peut constituer un comportement sécuritaire. Cependant, un

bon usage technologique n'est pas garant d'un comportement sécuritaire, car ce dernier nécessite également des actions de la part des employés qui requièrent un certain jugement, et ne nécessite aucun usage particulier de la technologie.

D'autre part, Safa *et al.* (2015) introduisent l'idée d'une sensibilisation accrue aux enjeux de la sécurité de l'information et à l'importance de cette dernière pour l'organisation, comme pour les individus. Les auteurs proposent le concept de *conscious care behavior* qu'ils définissent comme le comportement où « les utilisateurs réfléchissent aux conséquences de leurs actions en matière de sécurité de l'information lorsqu'ils travaillent avec un système et particulièrement sur Internet » (p.66). De plus, étant donné le dynamisme et l'évolution continuelle du domaine Infosec, les individus ont besoin des mises à jour fréquentes et d'une grande capacité d'adaptation (Safa *et al.*, 2015). Les employés doivent donc faire preuve de jugement, puisque le fait de se conformer à des politiques ou de suivre des principes éthiques ne peut pas constituer une solution à chaque nouvelle situation rencontrée. Sans le nommer explicitement, van Bavel *et al.* (2019) évoquent un comportement relevant du jugement des utilisateurs et consistant à choisir les actions en lien avec la sécurité qui leur semblent appropriées, sans d'autres directives spécifiques. Autrement dit, un comportement sécuritaire en est un qui réduit les risques de cyberattaques et le choix d'une action sécuritaire est habituellement plus complexe et requiert plus de temps et d'efforts cognitifs.

Finalement, que peut-on faire lorsque la menace devant laquelle on se trouve n'est pas encadrée par les politiques organisationnelles? Hsu *et al.* (2015) ont identifié ce comportement par le terme *extra-role behavior*. Ce type de comportement possède un caractère social, dans la mesure où il consiste à être attentif aux comportements des autres employés et se servir de son expérience pour les aider à améliorer lesdits comportements. Les auteurs distinguent deux idées principales liées aux *extra-role behaviors* : l'aide (*helping*), c'est-à-dire un comportement de coopération qui peut permettre à d'autres d'améliorer leurs compétences en Infosec et l'expression (*voicing*), c'est-à-dire faire part de commentaires ou de suggestions afin d'améliorer les pratiques Infosec dans l'organisation, ce qui peut permettre d'améliorer les politiques et mettre

en lumière d'éventuelles lacunes (Hsu *et al.*, 2015). Ce comportement relève donc de l'initiative personnelle et requiert certaines connaissances et expériences qui vont au-delà de ce qui est écrit dans les politiques. Nous estimons, en raison de cela, que le concept d'*extra-role behavior* s'apparente au jugement, mais avec un aspect social.

À la suite de l'analyse de tous ces concepts allant au-delà de la conformité et de l'éthique, nous avons été en mesure d'identifier et de réunir leurs principales caractéristiques afin de construire une définition pour la dimension « jugement ». Nous proposons donc de définir le jugement comme *les réflexes individuels de protection découlant de l'évaluation d'une situation et le fait d'agir ou prendre des décisions en ayant conscience des conséquences possibles de ses gestes.*

Cette sous-section sur les trois dimensions du comportement sécuritaire (conformité, éthique, jugement) confirme la pertinence d'aborder ce concept de la perspective d'un concept multidimensionnel. En effet, chacune des dimensions présentées contribue à améliorer la compréhension du comportement sécuritaire, mais notre analyse nous porte également à croire que l'étude de ces dimensions ensemble donnera une vision beaucoup plus complète du concept. Bien que peu d'articles abordent plus d'une dimension, nous avons pu en identifier suffisamment pour nous permettre d'avoir une idée des principales relations entre les dimensions existant dans la littérature, tel que le présente la section qui suit.

4.3 Relations entre les dimensions

L'analyse approfondie des dimensions du comportement nous a permis d'observer que la majorité des articles de l'échantillon n'étudiaient qu'une seule dimension et donc qu'un nombre relativement faible d'études traite d'une possible relation entre les dimensions. Néanmoins, de tous les articles analysés, nous en avons identifié 20 qui évoquaient l'existence d'une relation entre les dimensions du comportement, dont 13 provenaient de la littérature académique et sept de la littérature professionnelle. Ils

relevaient toujours une relation entre deux des trois dimensions à l'étude dans ce mémoire; aucun n'établissait de rapport entre les trois. De plus, tous ces articles datent de 2015 ou après, à l'exception de deux d'entre eux, datant respectivement de 2009 et 2010, ce qui nous indique que l'étude des relations entre les dimensions n'est que très récente.

Afin de mieux comprendre la manière dont ces dimensions sont reliées, nous avons procédé à un codage thématique à partir des 20 articles mentionnés ci-haut, un peu de la même façon que nous avons procédé pour les définitions et les actions (voir tableau 4.7).

Tableau 4.7 Exemple d'un extrait du codage des liens entre les dimensions

Article	Concept utilisé dans l'article	Lien mentionné dans l'article avec d'autres dimensions
Chen et al. (2019)	Information security policy violation behavior	Suggestion que l'éthique serait un antécédent de la conformité, car l'étude avance que c'est un manque de considération éthique qui mène à la violation des politiques de sécurité **[A]**
Herath et al. (2018)	IS Security Policy Violation Likelihood	Le désengagement moral favorise une violation des politiques; par contre une sensibilisation aux politiques réduit le risque de désengagement moral **[IR]**
van Bavel et al. (2019)	Online security behavior	L'étude suggère que le jugement seul ne suffit pas toujours, qu'une composante de la conformité (ici une suggestion d'actions à entreprendre) permet de diminuer le risque de subir une cyberattaque **[P]**

Légende : **[P]** Les dimensions vont de pair; **[A]** Une dimension est l'antécédent d'une autre; **[IR]** Les dimensions ont une interdépendance réciproque (p.ex la conformité est l'antécédent du jugement; mais le jugement est aussi l'antécédent de la conformité)

Ainsi, trois types de relations ont pu être identifiés, soit l'idée (1) que deux dimensions vont de pair, (2) qu'une dimension est l'antécédent d'une autre ou (3) que les deux dimensions ont une interdépendance réciproque (voir le tableau 4.8). Le premier type désigne simplement l'idée que les deux dimensions étudiées ne sont pas dissociables et

constituent ensemble un comportement sécuritaire. Le second type représente le fait qu'une dimension précède l'autre, dans la mesure où elle permet de développer ou renforcer l'autre. Enfin, le dernier type désigne que la première dimension précède la deuxième et inversement, selon la situation. Le tableau 4.8 présente ces résultats plus en détail.

Tableau 4.8 Types de relations entre les dimensions du comportement

Types de relations entre dimensions	Auteurs
(1) Dimensions qui vont de pair Exemples : conformité et jugement; conformité et éthique	**Littérature académique** : Burns et al. (2019); Hong et Furnell (2021); Hsu et al. (2015); van Bavel et al. (2019); Van Slyke et Belanger (2020)
	Littérature professionnelle : Buytendijk (2017); Buytendijk et al. (2020a); den Hamer et al. (2020); Huisman (2018b); Kim et al. (2020); Reed et al. (2020)
(2) Une dimension est l'antécédent d'une autre Exemples : l'éthique précède la conformité; le jugement précède la conformité, la conformité précède le jugement, l'éthique précède le jugement	**Littérature académique** : Chen et al. (2019); Dang-Pham et al. (2017); Hadlington et al. (2021); Rhee et al. (2009); Ruighaver et al. (2010); Safa et al. (2015); Tsohou et Holtkamp (2018)
	Littérature professionnelle : Buytendijk et al. (2020b)
(3) Les dimensions ont une interdépendance réciproque Exemple : l'éthique influence la conformité et la conformité, à son tour, favorise l'éthique	**Littérature académique**: Herath et al. (2018)
	Littérature professionnelle : aucun

Parmi les articles proposant l'idée que des dimensions vont de pair, les relations mentionnées sont celles entre la conformité et le jugement (7 articles) et entre la conformité et l'éthique (4 articles). Aucun de ces articles ne traite d'une relation entre l'éthique et le jugement. De manière générale, les dimensions sont clairement mentionnées, mais certains articles mettent davantage l'accent sur le fait que la conformité ne suffit pas et évoquent un peu plus vaguement l'autre dimension concernée. Néanmoins, les explications fournies étaient suffisamment claires pour nous aider dans notre classification.

Ensuite, parmi les articles suggérant qu'une dimension est l'antécédent d'une autre, les trois types de relations soit conformité-jugement, conformité-éthique et éthique-

jugement se retrouvent dans la littérature. Toutefois, la direction de l'antécédence ne fait pas de consensus. Par exemple, deux articles présentent l'éthique comme antécédent de la conformité car ce serait un manque de considération éthique, voire un désengagement moral, qui mènerait à une sensibilisation plus faible envers les pratiques et politiques organisationnelles et ultimement à la violation des politiques de sécurité (Chen *et al.*, 2019; Hadlington *et al.*, 2021). Un autre article argumente la relation inverse parce que la conformité est la base sur laquelle on peut développer des principes éthiques en ce qui concerne l'utilisation des technologies, mais qu'il faut aller au-delà de ce seuil (Buytendijk *et al.*, 2020b). Ces deux arguments opposés se retrouvent également dans l'étude de Herath *et al.* (2018) qui avancent ainsi l'idée d'une interdépendance réciproque : un désengagement moral, c'est-à-dire un manque de considération pour les conséquences de ses actes, favorise la non-conformité aux politiques et une meilleure sensibilisation, et donc une meilleure conformité, diminue en retour le désengagement moral.

En ce qui concerne les études abordant la conformité et le jugement, deux articles sur les quatre évoquent le jugement comme antécédent de la conformité (Rhee *et al.*, 2009; Tsohou et Holtkamp, 2018) et les deux autres mentionnent la relation inverse (Dang-Pham *et al.*, 2017; Safa *et al.*, 2015). D'abord, l'idée que le jugement précède la conformité pourrait s'expliquer par le fait que les employés chez qui l'auto-efficacité (ici liée au jugement) est plus développée sont généralement portés à adopter les comportements recommandés en matière de sécurité par leur organisation (Rhee *et al.*, 2009). Par ailleurs, la décision de se conformer (ou non) découlerait de l'évaluation d'une situation et de l'évaluation de la pertinence des actions en fonction de la situation (Tsohou et Holtkamp, 2018). D'autre part, la relation inverse, soit que la conformité précède le jugement, pourrait notamment s'expliquer par l'idée que le comportement sécuritaire se manifeste par le partage de connaissances liées à la sécurité. Ce partage de connaissances serait en quelque sorte associé au jugement et relèverait de motivations découlant de la conformité, mais il se peut aussi que les employés partagent leurs connaissances de leur propre gré, selon le contexte, s'ils évaluent que c'est

pertinent à la situation (Dang-Pham *et al.*, 2017). Par ailleurs, la conformité en combinaison avec des éléments du jugement formés à partir d'expériences antérieures contribuerait à développer davantage le jugement (Safa *et al.*, 2015). Enfin, un seul article prend une direction différente et propose l'idée que l'éthique permet de développer le jugement, dans la mesure où les employés seront mieux préparés à des situations inconnues s'ils ont une meilleure sensibilisation aux conséquences possibles de leurs actions (Ruighaver *et al.*, 2010).

L'analyse des relations proposées entre les dimensions a permis de constater que la littérature académique mentionne le plus fréquemment une relation entre la conformité et le jugement, tandis que la littérature professionnelle fait davantage ressortir la relation entre l'éthique et la conformité. D'ailleurs, parmi les huit articles mentionnant une relation d'antécédence entre les dimensions, les rapports éthique-conformité (3) et jugement-conformité (3) reviennent le plus souvent, mais il faut prendre ces résultats avec un grain de sel parce que d'une part, il y a très peu d'études et d'autre part, certaines de ces études ne sont pas empiriques. Ces résultats ne sont pas surprenants si l'on considère que le discours dominant dans la littérature positionne la conformité comme l'élément principal du comportement sécuritaire (p.ex. Donalds et Osei-Bryson, 2020; Herath et Rao, 2009a). Les auteurs qui estiment que ce type de comportement devrait aller bien au-delà de la simple conformité (soit avec l'éthique, soit avec le jugement) ne constituent, pour l'instant, qu'un discours plutôt marginal (p.ex. Buytendijk, 2017; Ng *et al.*, 2009). Ce constat est particulièrement évident dans la littérature académique où 47 des 70 articles (67%) examinent seulement la conformité, tandis 23 d'entre eux (33%) étudient soit d'autres dimensions du comportement, soit la conformité en combinaison avec une autre dimension. Cependant, dans la littérature professionnelle, c'est le phénomène inverse qui a été observé : la majorité des articles (11 sur 13 ou 85%) aborde plus d'une dimension du comportement (en combinaison ou non avec la conformité). Ce résultat, quant à lui, est quelque peu surprenant, parce qu'il

donne l'impression que la théorie ne rend pas très bien compte de la réalité sur le terrain.

Les auteurs qui définissent le comportement sécuritaire uniquement par la conformité croient généralement que le simple fait de suivre les politiques organisationnelles permet de protéger l'actif informationnel contre la plupart des incidents, mais ils n'offrent pas de justification très élaborée au sujet de leur position (p.ex. Omidosu et Ophoff, 2016; Safa *et al.*, 2016; Siponen *et al.*, 2014). Certains associent la conformité à la mitigation des risques d'incidents (Donalds et Osei-Bryson, 2020) et vont jusqu'à dire que la présence d'incidents serait un échec de la gouvernance de la sécurité, car l'organisation n'a pas trouvé moyen d'encourager les employés à se conformer aux politiques (Herath et Rao, 2009a). Il est à noter qu'il existe des articles qui s'attardent à la conformité, mais qui ne prétendent pas explicitement qu'il s'agit de la seule dimension du comportement sécuritaire; ces articles ne font pas partie du discours décrit ici.

En contrepartie, la position des auteurs prônant un comportement sécuritaire multidimensionnel se base sur l'insuffisance d'une seule dimension à assurer un comportement sécuritaire chez les employés. Par exemple, nous avons vu que l'article de Hsu *et al.* (2015) présente le comportement sécuritaire comme ayant deux dimensions, avec l'*in-role behavior* (lié à la conformité) et l'*extra-role behavior* (lié au jugement). Les auteurs estiment que ces deux éléments sont complémentaires et indissociables pour que les politiques de sécurité soient pertinentes et efficaces, et donc pour favoriser un comportement sécuritaire. De plus, Ng *et al.* (2009), disent explicitement que le comportement sécuritaire est « plus vaste que la conformité aux politiques organisationnelles » (p.816, traduction libre). Les programmes de sensibilisation devraient donc viser à exercer une influence positive sur l'attitude et le comportement des employés afin de les rendre plus conscients des enjeux de sécurité, de manière à développer leur jugement, et pas nécessairement de les influencer à se conformer. Ainsi, un comportement sécuritaire devrait idéalement relever davantage d'un choix individuel que d'une exigence organisationnelle (Ng *et al.*, 2009). Du côté de

la pratique professionnelle, les programmes de sensibilisation sont souvent uniquement axés sur la conformité et se concentrent principalement à transmettre de l'information au sujet des enjeux de sécurité, au lieu de mettre l'accent sur une manière d'inciter un comportement sécuritaire chez les employés (Walls, 2013). Selon Walls (2013), en raison de cette emphase sur la conformité, les investissements dans ces programmes de sensibilisation ne donnent pas d'amélioration tangible dans la sécurité de l'organisation.

Par ailleurs, le discours de certains auteurs met explicitement l'accent sur l'éthique, qui serait indissociable du comportement sécuritaire. Chez Hadlington *et al.* (2021) il y a deux dimensions à la sensibilisation des employés et par conséquent à leur comportement : d'une part la compréhension de la pertinence des politiques organisationnelles, et d'autre part l'engagement de l'employé par rapport aux principes de sécurité. Ce deuxième aspect est étudié par les auteurs dans sa forme négative, c'est-à-dire à travers le désengagement moral des employés et est présenté comme un antécédent indirect ayant une influence négative sur la sensibilisation à la sécurité. En somme, le comportement sécuritaire dépend notamment du sens moral ou éthique qu'ont les employés, dans la mesure où c'est une évaluation de ce qui est bien ou mal qui permettra aux employés de décider d'adopter les pratiques recommandées (Hadlington *et al.*, 2021). De plus, le comportement sécuritaire contiendrait nécessairement une dimension éthique, qui doit compléter la conformité, car « ce ne sera jamais le rôle des politiques organisationnelles d'enseigner un comportement éthique » (Ruighaver *et al.*, 2010, p.733, traduction libre).

En outre, plusieurs articles de Gartner traitant du concept de *digital ethics* (p.ex. Buytendijk *et al.*, 2020a; den Hamer *et al.*, 2020) avancent que la sécurité de l'information et la confidentialité des données nécessitent une approche qui va au-delà de la conformité. Ce qui distingue le *digital ethics* de l'éthique évoquée par d'autres articles (surtout académiques) est l'idée que la sécurité de l'information ne passe pas seulement par le comportement sécuritaire des employés, mais également par la manière dont une organisation utilise son actif technologique. Ainsi, le *digital ethics* peut aider les membres d'une organisation à faire une utilisation éthique et juste de cet

actif (Buytendijk, 2017). Par exemple, l'organisation peut aussi bien compromettre la sécurité des membres ou de ses clients si elle vend des données de clients à de tierces parties inconnues ou si elle utilise l'intelligence artificielle pour recueillir des données confidentielles. En raison de cela, Buytendijk (2017) estime que les principes de sécurité ne sont plus une question de conformité et nécessitent une prise de position éthique de la part des organisations.

En somme, la grande majorité des articles qui évoquent des relations entre les dimensions mettent de l'avant que la conformité seule est insuffisante pour assurer un comportement sécuritaire. Même s'il y a relativement peu d'études sur le sujet, il est assez clair au terme de cette analyse que chacune des dimensions joue un rôle significatif dans le comportement sécuritaire et qu'il est non seulement pertinent, mais nécessaire de les mettre en relation pour mieux comprendre ce qu'est un tel comportement.

4.4 Autres constats

L'analyse des données issues de la revue de littérature systématique nous a permis de recenser trois principales dimensions au comportement sécuritaire, soit la conformité l'éthique et le jugement, et a fait ressortir un lien possible d'interdépendance entre elles. Ainsi, nous n'avons pas identifié d'autres dimensions ou d'autres relations qui ressortent, outre celles déjà mentionnées tout au long de ce chapitre. Cependant, il est impossible de dire qu'il n'en existe pas d'autres, surtout compte tenu du fait que l'Infosec comportementale est un champ d'étude très récent. Par exemple, les concepts d'*extra-role behavior* et de *digital ethics* vont un peu plus loin que la définition de leurs dimensions respectives, mais la faible quantité d'information ne permet pas de tirer des conclusions solides sur le sujet. De plus, un élément difficilement classifiable, à savoir la pression temporelle, a été recensé, or il n'est pas clair comment il s'inscrit dans le réseau nomologique du comportement sécuritaire. Il est à noter que les trois seules études de

notre échantillon évoquant cet élément sont particulièrement récentes (c.-à-d. Chowdhury *et al.*, 2018; Chowdhury *et al.*, 2020; Kajtazi *et al.*, 2018) et d'autres informations seraient nécessaires pour mieux comprendre son rôle.

Ce chapitre d'analyse a contribué à rassembler les informations nécessaires pour formuler des réponses à nos deux sous-objectifs de recherche dans le prochain chapitre.

Chapitre 5. Discussion

Le présent mémoire a été réalisé dans le but de proposer une définition conceptuelle du comportement sécuritaire pour la protection de l'actif informationnel, concept dont l'importance a été reconnue dans la littérature, mais qui demeure encore flou. À partir des données recueillies au moyen d'une revue de littérature systématique, nous avons trouvé des éléments pour répondre à notre premier sous-objectif, à savoir d'identifier les thèmes qui existent dans la littérature concernant le comportement sécuritaire. Le deuxième sous-objectif, soit de proposer une définition « de dictionnaire » du comportement sécuritaire, découlera ensuite de la mise en commun des éléments trouvés en réponse au sous-objectif précédent.

5.1 Retour sur les sous-objectifs de recherche

Tout d'abord, pour atteindre le premier sous-objectif de recherche, nous avons synthétisé les principaux résultats obtenus au chapitre précédent concernant les caractéristiques du comportement sécuritaire, ses dimensions et les relations entre les dimensions. Les paragraphes qui suivent présentent donc les réponses à ce sous-objectif.

5.1.1 Identifier les thèmes dans la littérature au sujet du comportement sécuritaire

Identifier les principales caractéristiques du concept

Afin de répondre au premier sous-objectif de recherche, soit d'identifier les thèmes qui existent dans la littérature concernant le comportement sécuritaire, nous avons recueilli dans un premier temps les informations clés provenant de l'analyse des éléments fondamentaux identifiés au chapitre 4, soit les noms de concept, les définitions et les

actions du comportement. L'analyse de ces éléments fondamentaux nous a donc permis d'identifier certains aspects importants qui devraient se refléter dans la définition du comportement sécuritaire.

Ainsi, parmi les noms de concept relevés, examinons d'abord celui qui est le plus fréquemment utilisé, soit *information security behavior* (ou *Infosec behavior*) en anglais ou *comportement lié à la sécurité de l'information* (ou *comportement Infosec*) en français, et qui donne un bon aperçu de ce en quoi la définition devrait consister, dans la mesure où il implique qu'il s'agit d'un comportement qui est lié à la sécurité de l'information et il ne met pas l'emphase sur une dimension en particulier, de manière à pouvoir inclure toutes les dimensions. Une précision s'impose, toutefois, quant à la distinction entre ce terme et le terme beaucoup plus répandu parmi les professionnels francophones : *comportement sécuritaire*. Le terme anglais fréquemment utilisé a une connotation neutre et il peut désigner autant un comportement positif que négatif. Ainsi, afin de préserver la logique sémantique, le terme anglais correspondant au *comportement sécuritaire pour la protection de l'actif informationnel* serait *protective information security behavior* (ou *protective Infosec behavior)*, qui contient la même connotation positive. Étant donné que l'objectif de ce mémoire est de définir un comportement sécuritaire pour la protection de l'actif informationnel, ce qui connote qu'il s'agit d'un comportement positif, notre définition doit le refléter adéquatement. Ainsi, le **but de ce type de comportement***,* ici de protéger l'actif informationnel, devrait être explicitement énoncé dans la définition proposée.

Un autre détail qui nous paraît important pour la définition est l'utilisation d'**un terme qui inclut toutes les dimensions**. Tel que constaté lors de notre analyse systématique de la littérature, une définition n'incluant pas toutes les dimensions peut devenir trop restrictive et non représentative. De plus, malgré la variété et la disparité des définitions recensées, nous avons retenu qu'un comportement sécuritaire devrait être **défini par des gestes réels** et non par des intentions.

Enfin, selon notre analyse, les actions du comportement sécuritaire devraient être **objectivement observables**, donc pouvoir être perceptibles par autrui et ne pas pouvoir être seulement déterminées au moyen d'une auto-évaluation. La définition du comportement sécuritaire devrait donc mettre l'emphase sur cet aspect. Précisons également que, puisque la définition d'un concept a une incidence sur la mesure de variables qui pourraient en découler (MacKenzie *et al.*, 2011), il nous paraît pertinent d'insister sur le caractère objectif des actions.

En somme, l'analyse des noms de concept, des définitions et des actions du comportement sécuritaire dans la littérature a fait ressortir les éléments qui doivent impérativement être présents dans la définition qui sera proposée :

- La définition doit explicitement faire part du but du comportement sécuritaire, soit de protéger l'actif informationnel;
- La définition doit pouvoir inclure toutes les dimensions qui constituent le comportement sécuritaire;
- Le comportement doit être défini par des gestes réels et non par des croyances ou des intentions;
- Le comportement sécuritaire doit être perceptible à travers des actions objectivement observables.

Maintenant que nous avons clarifié les caractéristiques du comportement sécuritaire, la prochaine étape consiste à discuter des principaux constats sur les trois dimensions du comportement sécuritaire identifiées dans la littérature.

Identifier et définir les dimensions du concept

D'après l'analyse de notre échantillon, la littérature tend à démontrer l'existence des trois dimensions principales, soit la conformité, l'éthique et le jugement. Nous avons déjà identifié les définitions correspondant à chacune de ces dimensions au chapitre 4. À ce stade-ci, nous avons pu observer un point commun entre les dimensions, soit le fait

qu'elles relèvent toutes d'un **degré d'initiative différent de la part de l'individu.** La conformité nécessite le moins d'initiative, car il s'agit simplement de suivre ce que recommandent les pratiques et politiques. L'éthique en requiert un degré un peu plus élevé dans la mesure où, même si l'individu peut apprendre certains principes éthiques dans le cadre d'une formation par exemple, ultimement c'est lui-même qui doit évaluer si ses actions constituent le « bien » dans une situation donnée pour assurer la protection de l'actif informationnel. Enfin, le jugement est la dimension qui relève du plus haut degré d'initiative, car il nécessite que l'individu évalue une situation, qui est parfois nouvelle, et en se basant sur cette évaluation, il détermine les actions à poser. De plus, selon certains chercheurs (p.ex. Hsu et al., 2015), le jugement consiste également à avoir l'initiative de proposer des idées pour améliorer les pratiques de sécurité.

Bien qu'il semble y avoir un consensus dans la littérature quant aux dimensions constituant un comportement sécuritaire, la manière dont ces dimensions sont reliées et la manière dont un comportement se crée ne sont pas claires. Les paragraphes qui suivent présentent nos constats et nos réflexions à ce sujet.

Déterminer les relations entre les dimensions

Nous avons vu au chapitre précédent que les articles traitant des relations entre les dimensions étaient relativement peu nombreux et très récents pour la plupart. Il n'est donc pas étonnant que ce sujet soit encore à un stade exploratoire et qu'on ne puisse affirmer avec certitude les relations qui existent entre les dimensions. La plupart de ces relations ont été validées empiriquement, mais on retrouve encore de nombreuses contradictions entre les études, surtout concernant les liens d'antécédence entre la conformité et l'éthique, et entre la conformité et le jugement. Par ailleurs, comme le domaine de recherche de la sécurité de l'information comportementale est si récent, il est également possible qu'un nombre significatif de chercheurs ne soit pas encore rendu au stade de déterminer et valider les liens d'antécédence. Pourtant, il serait logique de

penser qu'une telle investigation pourrait contribuer à mieux définir le concept de comportement sécuritaire et à clarifier les relations entre ses dimensions.

Afin de présenter et de synthétiser les principales relations entre les dimensions relevées, nous les avons traduites sous la forme d'un modèle de type « arbre de décision » (Figure 5.1). Comme tout modèle, celui-ci ne se veut pas une représentation entièrement réaliste, il s'agit d'une simplification résumant certaines tendances ressortant de la littérature. Il ne représente donc pas tous les cas de figure. De plus, il est à noter que la littérature Infosec s'intéresse surtout aux antécédents du comportement sécuritaire ou aux facteurs favorisant ce dernier et n'aborde pratiquement pas la manière dont un tel comportement se forme. Ainsi, pour tenter de faire du sens de ces informations et les rendre plus complètes, nous avons consulté les théories issues de la psychologie relevées au chapitre 2 (c.-à-d. la théorie de la dissonance cognitive et la théorie du comportement interpersonnel) afin de proposer une manière plus cohérente d'illustrer le développement du comportement.

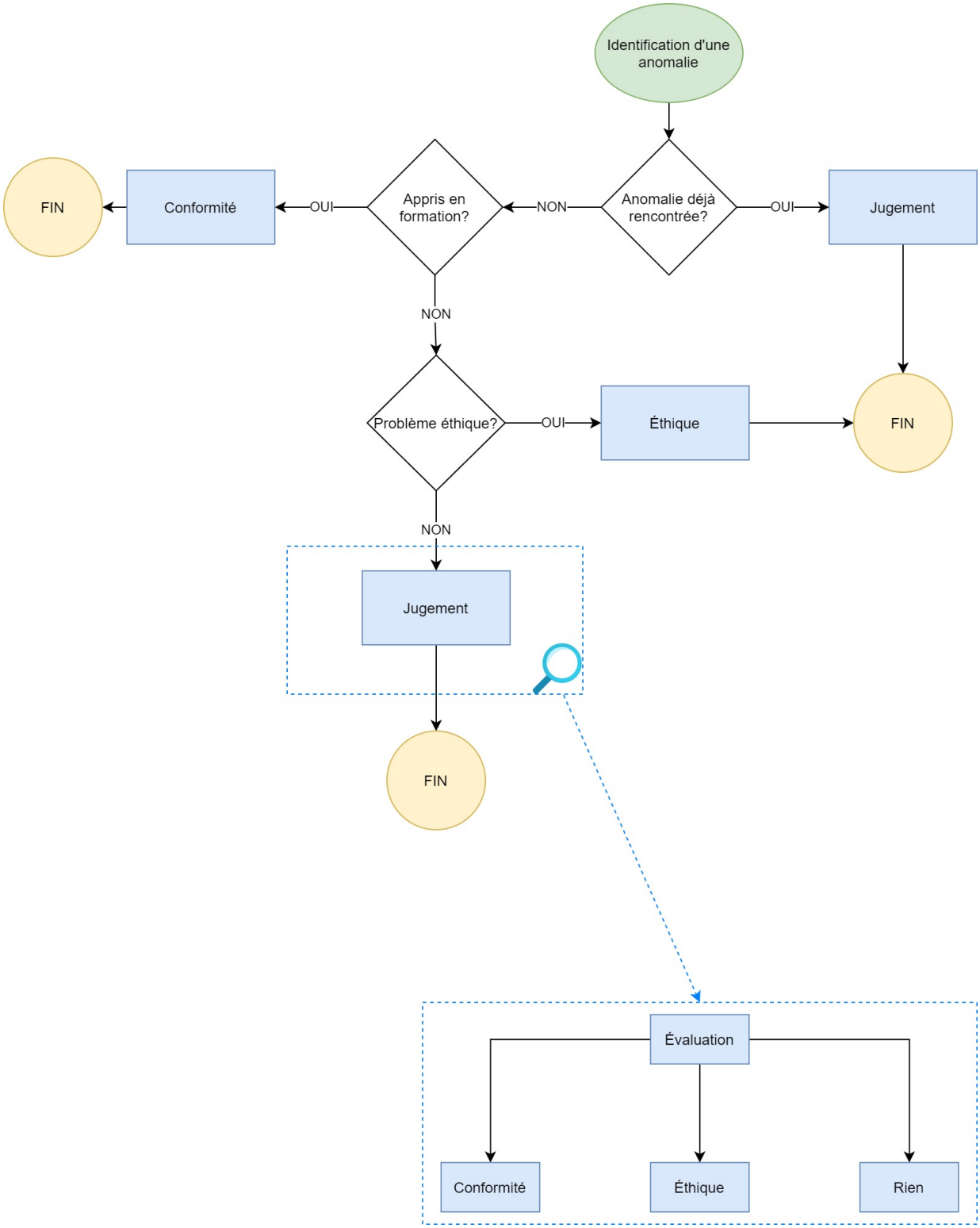

Figure 5.1 Arbre de décision de l'adoption d'un comportement

La figure 5.1 illustre ainsi une situation débutant avec l'identification d'une anomalie par un employé :

- Tout d'abord, la théorie de la dissonance cognitive nous indique que l'identification de l'anomalie crée une incohérence (ou dissonance) dans l'esprit de l'employé par rapport à sa situation habituelle. La théorie explique également que l'être humain est naturellement porté à vouloir se débarrasser de cette dissonance, puisqu'elle génère un sentiment désagréable.
- Si l'employé a déjà rencontré ce type d'anomalie auparavant, la littérature Infosec suggère qu'il va se fier à son jugement, et donc à son expérience antérieure pour la résoudre.
- Si l'employé n'a jamais rencontré l'anomalie, la dissonance persiste. S'il identifie qu'il a déjà vu un tel cas dans le cadre d'une formation, il appliquera la conformité en mettant en œuvre ce qu'il a appris pour éliminer la dissonance.
- Si le cas n'a pas été vu en formation, la dissonance persiste encore. Toutefois, si l'employé identifie qu'il s'agit d'un problème éthique, il résoudra l'anomalie en appliquant des principes éthiques.
- S'il ne s'agit pas d'un problème éthique non plus, la dissonance persiste toujours et, face à cette nouvelle situation, l'employé n'aura d'autre choix que d'avoir recours à son jugement. De cette utilisation du jugement découlera une évaluation de la situation qui déterminera la manière de résoudre l'anomalie :
    - Soit en faisant des parallèles avec des notions apprises en formation et en appliquant la conformité, même si ce cas spécifique n'a pas été appris;
    - Soit en déterminant ce qu'il est « bien » de faire en se basant sur des principes éthiques, même si la nature de l'anomalie n'est pas forcément éthique;
    - Soit en ne faisant rien, auquel cas il faut espérer pouvoir minimiser les dommages.

En empruntant des théories au domaine de la psychologie et en les appliquant à l'Infosec, nous avons proposé une manière différente de considérer les relations entre les dimensions du comportement sécuritaire et la façon dont ce comportement pourrait se former. Ces théories nous suggèrent que le comportement devrait se former tel que l'illustre la figure 5.1, or la littérature Infosec présente quelques différences. Ainsi, dans notre figure, toutes les branches au-dessus de l'agrandissement ainsi que celles des liens « jugement-éthique » et « jugement-rien » dans l'agrandissement découlent d'un raisonnement logique, mais ne sont pas abordées dans la littérature Infosec. La relation entre le jugement et la conformité (dans l'agrandissement), quant à elle, est abordée dans la littérature et est la seule à avoir été validée empiriquement (c.-à-d. Rhee *et al.*, 2009; Safa *et al.*, 2015). Ces flous dans la littérature pourraient d'ailleurs appuyer l'argument de certains auteurs affirmant que les théories les plus utilisées actuellement en Infosec comportementale ne sont pas suffisantes à la compréhension du comportement sécuritaire et qu'il faudrait les adapter ou les combiner à d'autres théories. D'ailleurs, ce ne serait pas inhabituel ou spécifique à l'Infosec comportementale, l'emprunt aux domaines connexes est en effet une phase normale de l'évolution d'un domaine donné (Dulipovici et Baskerville, 2015).

L'examen des éléments fondamentaux, des dimensions et des relations entre les dimensions du comportement sécuritaire nous a permis d'atteindre notre premier sous-objectif de recherche et à mieux clarifier ce qu'est un tel comportement. Le deuxième sous-objectif consistera donc à proposer une définition plus uniforme de ce concept.

5.1.2 Autres constats importants avant la définition

Le deuxième et dernier sous-objectif de cette recherche est de présenter une définition dite « de dictionnaire » du concept de comportement sécuritaire. Toutefois, nous constatons à ce stade-ci que ce n'est pas encore possible, notamment en raison de certaines contradictions et d'un flou qui persistent. Dans l'ensemble, l'importance de la

composante humaine en sécurité de l'information a été mise de l'avant dans tous les articles analysés dans le cadre de notre revue systématique et le comportement sécuritaire y est habituellement présenté comme la solution la plus efficace pour prévenir les incidents. Même si ces études nous donnent une idée générale du comportement sécuritaire, en raison de la variété de définitions recensées dans la littérature, il est toujours difficile de comprendre en quoi il consiste précisément. Les paragraphes suivants s'attarderont à présenter et expliquer les plus importants flous et contradictions qui demeurent même après notre analyse.

Contradictions et flou dans l'étude du concept

La sécurité de l'information, et particulièrement l'aspect comportemental, étant des domaines de recherche récents, il est normal que certains des sujets étudiés soient encore à un stade exploratoire. Cependant, puisque le comportement sécuritaire est largement utilisé dans la littérature, il y aurait un intérêt à clarifier ce concept fondamental. À cet effet, nous avons identifié dans la littérature TI certaines bonnes pratiques qui pourraient contribuer à dissiper le flou autour du comportement sécuritaire. Dans un premier temps, MacKenzie *et al.* (2011) notent que « le chercheur devrait préciser la nature du construit et son thème conceptuel avec des termes dépourvus d'ambigüité et en cohérence avec les études antérieures » (p.298, traduction libre). Toutefois, la variété et les variations des définitions recensées au chapitre précédent nous indiquent que l'opérationnalisation est peu uniforme. En effet, les termes composant les définitions ne sont pas toujours précis et il n'a pas été observé que les définitions soient cohérentes avec des recherches précédentes, ni même qu'elles y font référence.

Par la suite, MacKenzie *et al.* (2011) mentionnent que les premiers pas dans le processus de conceptualisation d'un construit consistent à examiner dans un premier temps comment le construit a été défini précédemment au moyen d'une revue de littérature, puis de mener des entrevues auprès de praticiens ou d'autres experts. Cependant, il a

été observé qu'aucun article de notre échantillon ne s'est penché spécifiquement sur la question de la définition du comportement sécuritaire et aucune revue de littérature sur ce sujet n'a pu être identifiée. Sans prétendre qu'il s'agisse de la seule façon de faire, cela pourrait néanmoins constituer une explication quant à la persistance du flou et au manque de cohérence entre les études. Par ailleurs, d'autres chercheurs n'ont pas manqué de souligner le flou dans l'étude du comportement sécuritaire et ses impacts sur les résultats. On retrouve notamment l'idée qu'il y a dans la littérature des résultats de recherche contradictoires et une terminologie portant à confusion, de même qu'une multitude de facteurs influençant le comportement (Topa et Karyda, 2019). De plus, quelques rares auteurs (p.ex. Weems *et al.*, 2018) ont explicitement insisté sur le fait qu'il est essentiel d'avoir d'abord une définition du comportement sécuritaire avant même de songer à le mesurer.

Contradictions et flou autour des dimensions du concept

En plus des contradictions liées à l'étude du comportement sécuritaire découlant en partie du manque de définition claire, nous croyons qu'il serait possible que cette absence de définition contribue également à cultiver un flou autour des dimensions du concept. Plus précisément, le *manque de définition claire* pourrait empêcher de déterminer exactement ce qui constitue une dimension par rapport à d'autres aspects tels qu'un antécédent, une caractéristique ou un facteur favorisant le comportement sécuritaire. En effet, nous avons relevé au chapitre 4 deux éléments dans la littérature qui nous apparaissent comme de possibles dimensions du comportement sécuritaire, mais elles ont été très peu étudiées à ce jour.

Tout d'abord, nous avons vu l'*extra-role behavior* de Hsu *et al.* (2015), qui contenait certes des éléments de la dimension jugement, mais mettait aussi l'emphase sur la collaboration entre employés pour favoriser la sécurité de l'information organisationnelle. Ensuite, nous avons identifié certains aspects du concept de *digital ethics* dans la littérature de Gartner, qui pourraient également laisser présager une

nouvelle dimension au comportement sécuritaire. Certains articles (p.ex. Buytendijk, 2017; den Hamer *et al.*, 2020) suggèrent que l'éthique consiste aussi à songer à la manière dont les technologies sont utilisées au sein d'une organisation, dans la mesure où une utilisation négligente (p.ex. vendre des données à de tierces parties) pourrait constituer une source d'incidents. Enfin, au terme de notre analyse, nous avons identifié un autre élément qui, sans s'apparenter explicitement à une dimension, pourrait être une caractéristique servant à décrire le comportement sécuritaire, à savoir *la pression temporelle*. L'étude de Chowdhury *et al.* (2020) a révélé qu'une des raisons pour lesquelles les employés n'appliquent pas certaines mesures de sécurité est en fait le caractère chronophage de ces dernières, car ils se préoccupent davantage d'accomplir leurs tâches à temps que de penser aux principes de sécurité.

Enfin, nous avons relevé des contradictions concernant les liens d'antécédence entre les dimensions, qui découleraient possiblement aussi du manque de définition claire du comportement sécuritaire. La littérature a fait ressortir cette relation d'antécédence entre l'éthique et la conformité, et entre le jugement et la conformité. Cependant il n'est pas encore possible de déterminer quelle dimension est l'antécédent de l'autre, surtout considérant que ce champ d'étude est récent.

En somme, cette section fait ressortir les contradictions et le flou, que nous désignons par le terme « chaos », que notre analyse du chapitre 4 n'a pas permis de clarifier. Le terme « chaos » désigne habituellement un désordre précédant la création, ce qui paraît approprié dans ce contexte, dans la mesure où nous faisons face à un désordre autour du comportement sécuritaire et à la suite duquel nous nous affairerons à créer une définition. Même si le mot « chaos » peut sembler fort, il s'agit d'un choix intentionnel de notre part pour souligner le grand désordre présent dans la littérature et la criticité de résoudre les contradictions et le flou qui le composent. Ainsi, la section suivante tente d'apporter un peu plus de clarté à ce chaos.

5.2 Une interprétation dialectique du chaos

Afin de mieux comprendre les contradictions et le flou autour du concept de comportement sécuritaire, nous nous sommes basés sur le modèle de développement et changement organisationnel de Van de Ven et Poole (1995) pour adapter le moteur dialectique de ce modèle à l'étude du comportement sécuritaire. Une approche relativement similaire a été utilisée par Moeini et Rivard (2019) pour étudier la littérature sur la gestion du risque dans les projets TI.

5.2.1 Présentation du modèle dialectique

Le modèle de Van de Ven et Poole (1995) propose quatre moteurs de changement, dont le moteur dialectique (Figure 5.2) qui correspond le mieux au cas étudié ici.

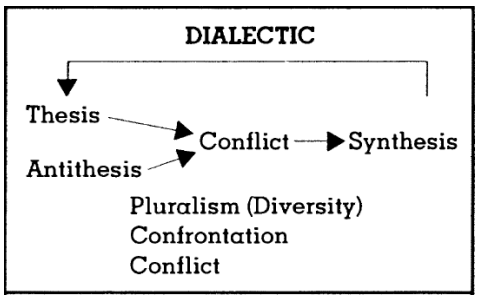

Figure 5.2 Modèle dialectique du changement organisationnel, Van de Ven et Poole (1995, p.520)

Ainsi, le modèle de changement dialectique est caractérisé par l'existence d'un conflit entre deux entités, sous la forme « thèse – antithèse ». Nous entendons par « thèse » la position initiale ou encore la plus répandue dans un débat donné et par « antithèse » la position opposée, qui vient contredire la thèse. Van de Ven et Poole (1995) expliquent qu'il y a deux issues possibles à ce conflit. D'une part, la situation la plus fréquente est

que la thèse et l'antithèse vont se combiner pour former une synthèse, qui n'est ni la thèse, ni l'antithèse, mais bien un hybride des deux. D'autre part, il est possible qu'une des deux entités entre la thèse et l'antithèse soit assez forte pour défaire l'autre et devenir la thèse principale. Enfin, les trois mots au bas de la figure 5.2 (*pluralism*, *confrontation* et *conflict*) représentent les concepts qui régissent ce moteur dialectique, dans la mesure où ce dernier contient au moins deux perspectives (*pluralité*) opposées (ou en *confrontation*), ce qui génère un *conflit*.

5.2.2 Le comportement sécuritaire sous l'angle du modèle dialectique

Afin de tenter de faire du sens du chaos mentionné ci-haut, nous l'avons examiné à travers le modèle dialectique afin d'identifier pour chaque contradiction et flou la thèse et l'antithèse, de même qu'une résolution (cf. à la figure 5.2). Les paragraphes qui suivent s'attardent à ces résultats plus en détail et présentent quelques propositions de recherche.

Cas #1 : intention d'un comportement et comportement réel

Dans le cas de la question de l'étude de l'intention du comportement par rapport au comportement réel, nous pouvons considérer que l'utilisation de l'intention constitue la thèse, car elle était mentionnée dans les études plus anciennes en Infosec datées d'avant 2010. Comme nous l'avons mentionné au chapitre précédent, certaines études utilisaient l'intention du comportement pour des raisons pragmatiques telles que la difficulté de collecter des données sur le comportement réel; elles ne font pas partie du cas décrit ici. Ce conflit entre l'intention et le comportement réel survient vraisemblablement en raison du flou dans l'étude du concept. Plus précisément, il s'agirait d'un résultat du manque d'une définition claire du comportement sécuritaire, en ce sens où la littérature n'indique pas sans ambigüité si le comportement est défini uniquement par des gestes réels ou par des intentions aussi. Par ailleurs, nous avons

également soulevé au chapitre précédent que certains articles définissaient ou caractérisaient le comportement sécuritaire par des gestes réels, mais le mesuraient comme une intention, ce qui met encore une fois l'accent sur l'ambigüité entourant la définition.

Thèse : Les chercheurs prônant l'intention comme mesure du comportement soutiennent que l'intention prédit efficacement les actions. Leur argumentaire se base sur l'idée que les théories sur lesquelles leur recherche est fondée telles que la Protection motivation theory (PMT) ou la Theory of planned behavior (TPB) avaient bien prédit des comportements dans des études en psychologie, et que par conséquent elles devraient bien s'appliquer au comportement en contexte Infosec. Ces études utilisant l'intention, prises séparément, semblent avoir donné des résultats pertinents, mais certains chercheurs (p.ex. Mamonov et Benbunan-Fich, 2018) ont observé que les résultats pouvaient, en fait, être incohérents au fil des études.

Antithèse : Parmi les principaux arguments soutenant l'antithèse, c'est-à-dire l'utilisation du comportement réel, on retrouve les idées que les intentions ne sont pas toujours suivies du comportement et que dans le contexte Infosec il y aurait d'autres variables entre l'intention et le comportement, d'où pourquoi les théories faisant un lien direct entre comportement et intention ne s'appliquent pas aussi bien. De plus, des chercheurs comme van Bavel *et al.* (2019) soulèvent qu'en sécurité de l'information ce sont les actions réelles et pas uniquement de bonnes intentions qui comptent afin de protéger les systèmes.

Conflit et sa résolution : Nous avons observé que, malgré le fait qu'un bon nombre d'études ne donne pas de définition du comportement sécuritaire, il y en avait beaucoup plus qui faisaient part d'actions s'inscrivant dans un tel comportement, dont certaines étaient directement observables. Cela nous porte à croire que les actions concrètes sont effectivement un indicateur d'un comportement sécuritaire et que les résultats découlant de celles-ci peuvent montrer si l'actif informationnel a été protégé, ou du moins qu'il n'a pas fait l'objet d'une attaque.

Il est à noter que tous les articles de notre échantillon critiquant l'utilisation de l'intention comme mesure sont récents, le plus ancien datant de 2015. Cela nous mène donc à croire que le comportement réel comme mesure découle de l'évolution de la recherche en Infosec et de l'analyse des études antérieures. Ainsi, ce qui émerge dans ce débat est que c'est l'antithèse qui prévaut sur la thèse, car des études (p.ex. Shropshire *et al.*, 2015) ont démontré que l'intention n'est pas toujours une bonne prédiction du comportement et que les données provenant de l'intention ne sont pas aussi fiables ou précises (Crossler *et al.*, 2013). Ainsi, nous considérons ce débat comme étant résolu.

Cas #2 : les dimensions et la relation entre les dimensions

En ce qui concerne la question de l'étude d'une seule dimension, soit la conformité par rapport à l'étude de dimensions combinées, nous considérons que la conformité comme composante première du comportement sécuritaire constitue la thèse. En effet, la conformité est la dimension la plus fréquemment mentionnée dans les articles de notre échantillon et elle est également abordée dans les articles plus anciens. Ainsi, l'idée que la conformité seule ne suffit pas pour déterminer un comportement sécuritaire constitue l'antithèse, car elle provient principalement des études ultérieures qui ont relevé de potentielles lacunes à l'utilisation de la conformité. Ce conflit semble d'abord découler du manque d'une définition claire, qui aurait permis de mieux identifier ce qu'est un comportement sécuritaire et déterminer avec moins d'ambigüité les dimensions qui le constituent. Ensuite, c'est ce même manque de clarté autour des dimensions qui alimente davantage le conflit comme nous le verrons à la fin de ce cas avec des concepts pour lesquels il n'est pas possible de déterminer s'il s'agit de nouvelles dimensions ou simplement d'antécédents ou de facteurs favorables au développement du comportement sécuritaire.

Thèse : La plupart des études étudiant la conformité comme composante essentielle du comportement sécuritaire font habituellement référence au fait de se conformer aux

pratiques et politiques organisationnelles. On y avance généralement que les politiques constituent en quelque sorte une base d'apprentissage et une ligne directrice pour favoriser l'adoption d'un comportement sécuritaire. Les études qui soutiennent que la conformité permet d'assurer un comportement sécuritaire se basent sur l'idée que si les employés font ce qui est prescrit dans les politiques organisationnelles, l'actif informationnel devrait être protégé (p.ex. Donalds et Osei-Bryson, 2020; Omidosu et Ophoff, 2016).

Antithèse : En contrepartie, les études affirmant que la conformité ne suffit pas évoquent le fait que les employés ne vont pas nécessairement faire ce que l'on demande d'eux (au moyen des politiques notamment), et qu'il faut également les sensibiliser aux conséquences possibles de leurs actions, voire de leur inaction. Par ailleurs, comme les politiques en matière de sécurité sont principalement des lignes directrices pour assurer un certain comportement sécuritaire, elles ne peuvent pas couvrir toutes les situations possibles qui pourraient survenir. Ainsi, certains auteurs (p.ex. Safa *et al.*, 2015) avancent qu'un comportement sécuritaire implique une capacité à évaluer une situation, surtout si elle est nouvelle, et s'y adapter.

Il semble y avoir une sorte d'écart entre la théorie et la pratique dans la mesure où la littérature académique s'intéresse surtout à la conformité tandis que la littérature professionnelle (Gartner) insiste sur la nécessité d'aller au-delà de la conformité en raison de l'insuffisance de cette dernière.

Conflit et sa résolution : Dans ce cas-ci, c'est un hybride entre la thèse et l'antithèse qui détermine l'issue du conflit, dans la mesure où ce n'est ni l'une ni l'autre qui contient la réponse, car cette dernière se situe quelque part entre les deux. Puisque le comportement humain est très complexe, il serait un peu simpliste de résumer le comportement sécuritaire comme consistant seulement à suivre les prescriptions des politiques organisationnelles. Yan *et al.* (2018) soulignent que les employés sont un groupe diversifié et que la recherche en Infosec a établi que certains facteurs individuels peuvent avoir un impact sur le comportement. Partant de ce constat, les auteurs

demandent donc à quel point le comportement sécuritaire pourrait prendre différentes formes chez les individus.

Ensuite, plusieurs auteurs, tel que relevé au chapitre 4, soutiennent que la conformité ne suffit pas pour que les employés comprennent leurs responsabilités vis-à-vis de la sécurité de l'information (p.ex. Buytendijk, 2017; den Hamer *et al.*, 2020). Ainsi, la compréhension des employés quant à leurs responsabilités est fondamentale pour qu'ils acquièrent un niveau de sensibilisation qui leur permette de comprendre comment protéger les systèmes, mais aussi de comprendre le rôle qu'ils jouent dans cette protection. Par ailleurs, l'adoption du comportement sécuritaire passe en partie par la communication du risque et les moyens habituellement utilisés (c.-à-d. les politiques et autres documents officiels) ne sont pas suffisants. Une approche plus ciblée devrait donc être favorisée, plutôt qu'une approche dite universelle (*one-size-fits-all*) (Alohali *et al.*, 2017). Cet argument renforce l'idée que la conformité et les politiques organisationnelles ne suffisent pas pour assurer un comportement sécuritaire et que d'autres éléments sont nécessaires.

De plus, les politiques organisationnelles comportent souvent des failles et ne peuvent pas servir à prévenir la plupart des incidents. Bon nombre de brèches de sécurité sont causées par des erreurs ou des accidents de la part des employés et non par une violation des politiques. La conformité aux politiques reste un élément important pour la sécurité de l'information, mais une de ses plus grandes lacunes résiderait dans le fait que les politiques n'évoluent pas avec les menaces; elles sont toujours un pas en arrière, puisqu'elles sont généralement mises à jour à la suite d'une menace ou d'un incident (Burns, 2019). Cette idée contribue à mettre de l'avant l'importance de l'éthique et du jugement, notamment pour renforcer le comportement sécuritaire là où la conformité ne suffit plus. Comme nous l'avons vu, ces deux dimensions, et en particulier le jugement, peuvent être d'utilité face à une situation nouvelle. Burns (2019) mentionne d'autant plus que les organisations qui réussissent à développer chez leurs employés une capacité à identifier les particularités des menaces potentielles et qui acquièrent une capacité à y répondre rapidement subissent moins d'incidents, car elles sont

capables de reconnaître et évaluer les menaces, et de faire preuve de flexibilité et de discernement pour y répondre, ou tout au moins pour réduire les impacts. Ceci nous permet de formuler une proposition de recherche qui vise à orienter les recherches futures.

***Proposition 1** : Le comportement sécuritaire gagne à être étudié en combinant les dimensions de la conformité, de l'éthique et du jugement.*

Le cas présenté ici est partiellement résolu, dans la mesure où il est clair que les autres dimensions en plus de la conformité sont essentielles pour étudier le comportement sécuritaire. Néanmoins, une incertitude persiste en ce qui concerne l'existence de possibles dimensions supplémentaires, encore à cause du manque de clarté par rapport à ce qui constitue le comportement sécuritaire, ainsi que ses dimensions.

Par exemple l'*extra-role behavior* (Hsu *et al.*, 2015) porte à croire que le comportement sécuritaire pourrait avoir une dimension collaborative en plus des trois déjà abordées dans la littérature. À partir de ce constat, il y aurait lieu de se demander, d'une part, si cette composante sociale fait partie intégrante du jugement, mais n'a pas encore été suffisamment étudiée ou, d'autre part, s'il s'agit d'une autre dimension du comportement sécuritaire ou même d'une sous-dimension du jugement. Par ailleurs, cet aspect social n'est pas négligeable, puisque l'analyse du chapitre précédent nous a indiqué que certaines interactions avec autrui constituaient les actions les plus facilement observables du comportement sécuritaire, et pourraient donc servir de point de départ pour le développer des mesures plus objectives.

Ensuite, le *digital ethics* dans Gartner, pousse plus loin la réflexion sur la dimension éthique. Buytendijk (2017) et den Hamer *et al.* (2020) nous disent qu'il faudrait songer à la façon dont une organisation se sert des données, ou des technologies en général, et qui pourrait être négligente, voire compromettante pour la sécurité de son actif informationnel. Cependant, un peu comme l'aspect social au paragraphe précédent, il n'est pas encore possible de déterminer si l'utilisation des technologies constitue une

nouvelle dimension ou s'il s'agit d'une composante de la dimension éthique. Il est à noter qu'aucun article académique dans notre échantillon ne traite de ce sujet ou d'un concept similaire.

Enfin, on retrouve le concept de pression temporelle, qui pourrait être important pour l'étude du comportement sécuritaire, mais dont le rôle exact demeure inconnu. Le peu de recherches à ce sujet propose toutefois des pistes de réflexions pertinentes. Par exemple, dans l'étude de Chowdhury *et al.* (2020), les participants avaient expliqué que d'effectuer certaines actions de sécurité (p.ex. utiliser des outils technologiques de sécurité, faire des copies de sauvegarde, crypter des documents ou des données contenues dans des appareils) leur enlevait du temps pour faire des tâches liées à leur travail principal. Dans un ordre d'idées similaire, une autre étude (Kajtazi *et al.*, 2018) a montré que lorsque les employés ne suivaient pas les politiques de sécurité, c'était principalement pour pouvoir accomplir une tâche à temps, car ils estimaient que suivre ces politiques constituait un obstacle à la complétion de leur travail. Bien qu'il ne semble pas y avoir beaucoup d'études sur la pression temporelle et le comportement sécuritaire, cette piste nous laisse croire qu'un tel comportement pourrait se caractériser par des actions qui ne prennent pas trop de temps à effectuer ou qui constitueraient un compromis raisonnable en termes de temps pour les employés. Cet élément nous paraît donc important, car les mesures de sécurité n'ont aucune pertinence si les employés ne les appliquent pas. Ceci nous permet donc de formuler une autre proposition de recherche, qui, comme la précédente, vise à orienter les recherches futures.

***Proposition 2** : Le comportement sécuritaire peut avoir d'autres dimensions que la conformité, l'éthique et le jugement.*

Cas #3 : les relations d'antécédence entre les dimensions

Le cas des relations d'antécédence entre les dimensions ressort comme une contradiction assez évidente dans la littérature et pourrait donner lieu à un conflit.

Cependant, l'étude de ce sujet est, à ce jour, à un stade embryonnaire, ce qui ne permet pas encore d'identifier ni une thèse ni une antithèse. En effet, nous avons relevé au chapitre précédent que les relations éthique-conformité (et son inverse) et jugement-conformité (et son inverse) ressortaient le plus souvent, mais il y a si peu d'études qu'il n'est pas possible de déceler une position dominante pour constituer la thèse. Certes, il s'agit de positions opposées, mais elles ne sont pas rendues à l'étape de la confrontation.

En conclusion, l'utilisation du modèle de changement organisationnel de Van de Ven et Poole (1995) adapté au contexte Infosec nous a aidé identifier et proposer des pistes pour clarifier deux contradictions importantes dans la littérature. Cela a notamment permis de mieux comprendre le flou qui persistait autour du comportement sécuritaire et de mieux compléter notre compréhension du concept. Maintenant que nous avons atteint le premier sous-objectif de recherche et que nous avons trouvé un certain sens dans le « chaos » autour du comportement sécuritaire, nous pouvons proposer une définition plus uniforme de ce concept et ainsi atteindre notre deuxième sous-objectif.

5.3 Proposition d'une définition du comportement sécuritaire

Il avait déjà été observé au chapitre 2 que le comportement sécuritaire pour la protection de l'actif informationnel souffrait du manque d'une définition claire et l'analyse des données provenant de notre revue systématique ne fait qu'appuyer davantage ce constat. Toutefois, cette même analyse nous a permis de recueillir et mettre en commun des informations clés permettant de proposer une définition plus uniforme du concept. Maintenant que nous avons apporté un peu de clarté au chaos entourant le comportement sécuritaire, nous pouvons revenir à notre dernier sous-objectif, soit de proposer une définition « de dictionnaire ». Ainsi, afin de formuler cette définition, nous nous sommes basés sur les recommandations de MacKenzie *et al.*

(2011) qui proposent des critères pour aider à définir un concept de manière claire, concise et précise.

Selon Mackenzie et al. (2011), pour que la définition d'un concept ou d'un construit soit dépourvue d'ambigüité elle devrait répondre aux critères suivants :

1. être claire et concise
2. ne pas être sujette à de multiples interprétations
3. ne pas contenir trop de termes techniques
4. définir le concept / construit par ce qu'il est et non par ce qu'il n'est pas
5. ne pas être tautologique ou auto-référentielle

Il a été constaté que la plupart des définitions recensées dans le cadre de la revue systématique ne répondaient pas entièrement à ces critères (1, 2 et 5 en particulier), d'où l'importance d'en proposer une qui pourrait remédier à cette situation. Ainsi, à partir des éléments recueillis tout au long de ce mémoire et spécifiquement en nous basant sur les réponses trouvées à notre premier sous-objectif de recherche, nous rappelons également les éléments essentiels de cette définition (cf. les résultats du chapitre 4):

- La définition doit explicitement faire part du but du comportement sécuritaire, soit de protéger l'actif informationnel;
- La définition doit pouvoir inclure toutes les dimensions qui constituent le comportement sécuritaire;
- Le comportement doit être défini par des gestes réels et non par des croyances ou des intentions;
- Le comportement sécuritaire doit être perceptible à travers des actions objectivement observables.

Par conséquent, nous proposons la définition du comportement sécuritaire dans l'encadré ci-dessous, suivie d'un rappel des définitions des trois principales dimensions.

Comportement sécuritaire pour la protection de l'actif informationnel : ensemble d'actions objectivement observables qu'adopte un individu afin de prévenir des incidents de sécurité et, ultimement, de protéger l'actif informationnel.

> **Actions objectivement observables:** les actions doivent relever de différents degrés d'initiative de la part de l'individu, correspondant aux différentes dimensions du comportement. Seules des actions objectives et perceptibles par autrui constituent un comportement. Les actions non observables ne s'inscrivent pas dans un comportement (il s'agirait plutôt d'attitudes ou de croyances, par exemple).

Dimensions du comportement sécuritaire

- **Conformité :** le fait d'appliquer les règles et les principes inscrits dans la politique organisationnelle**;**
- **Éthique :** ensemble de critères permettant de distinguer ce qui est bien de ce qui est mal, de manière à pouvoir en assumer les conséquences;
- **Jugement :** les réflexes individuels de protection découlant de l'évaluation d'une situation et le fait d'agir ou prendre des décisions en ayant conscience des conséquences possibles de ses gestes.

Enfin, pour vérifier notre définition, nous l'avons confronté à la liste de critères établis par MacKenzie *et al.* (2011), ainsi qu'aux critères que nous avons identifiés précédemment dans ce chapitre, tel que le présente le tableau 5.1.

En conclusion, ce chapitre nous a permis de rassembler les informations essentielles à l'élaboration d'une définition conceptuelle du comportement sécuritaire, puis de vérifier qu'elle répond à certains critères clés d'une définition efficace.

Tableau 5.1 Vérification des critères de la définition

Critères	Manière dont la définition y répond
La définition doit être claire et concise*	À notre avis, la formulation proposée respecte ces critères. Toutefois, notre définition devra être soumise au test d'une validation empirique.
La définition ne doit pas être sujette à de multiples interprétations*	
La définition ne doit pas contenir trop de termes techniques*	Elle est rédigée dans un langage usuel et ne comporte pas de jargon trop spécifique à un domaine.
La définition doit définir le concept / construit par ce qu'il est et non par ce qu'il n'est pas*	Elle décrit directement ce que le comportement sécuritaire est, à savoir des actions observables servant ultimement à protéger l'actif informationnel.
La définition ne doit pas être tautologique ou auto-référentielle*	Elle ne répète pas une même idée en termes différents et ne contient pas de termes qui réfèrent à un autre terme dans la définition.
La définition doit explicitement faire part du but du comportement sécuritaire, soit de protéger l'actif informationnel	Cette information est explicitement énoncée dans la définition
La définition doit pouvoir inclure toutes les dimensions qui constituent le comportement sécuritaire	Elle ne mentionne aucune dimension spécifique, ce qui la rend inclusive. De plus la précision sur les actions objectivement observables fait mention de degrés d'initiative, ce qui permet de suggérer plusieurs dimensions.
Le comportement doit être défini par des gestes réels et non par des croyances ou des intentions	Cette information est présente dans la précision sur les actions objectivement observables
Le comportement sécuritaire doit être perceptible à travers des actions objectivement observables	Cette information est explicitement énoncée dans la définition

Note : les critères marqués d'un « * » correspondent à ceux identifiés dans l'article de MacKenzie *et al.* (2011)

Chapitre 6. Conclusion

Le présent chapitre clôt ce mémoire en rappelant d'abord l'objectif général et les deux sous-objectifs de recherche, puis en présentant les principaux résultats et les contributions qui en découlent. Il fait mention ensuite des principales limites de l'étude et propose des pistes pour des recherches futures.

6.1 Rappel de l'objectif de recherche et principaux résultats

Devant le constat que la plupart des incidents de sécurité étaient causés par l'erreur humaine, l'emphase est mise sur l'importance de la composante humaine en sécurité de l'information, tant dans la littérature académique que professionnelle. Un des éléments clés qui y est soulevé est le comportement sécuritaire des employés. Or, ce concept pourtant répandu demeure encore flou et mal défini dans les deux catégories de littérature. Le présent mémoire s'intéresse donc à clarifier ce qu'est le comportement sécuritaire en contexte de protection de l'actif informationnel en proposant une définition conceptuelle du comportement sécuritaire, c'est-à-dire une description aussi précise que possible de ce qu'est un comportement sécuritaire, les caractéristiques qu'il possède et les dimensions qui le composent. Ainsi pour atteindre cet objectif, nous avons d'abord atteint les deux sous-objectifs suivants, qui ont permis de mieux comprendre en quoi consiste ce concept :

- Identifier les thèmes qui existent dans la littérature concernant le comportement sécuritaire;
- Proposer une définition « de dictionnaire », soit une définition claire, précise et concise.

Afin de trouver les réponses à ces sous-objectifs, une revue systématique de la littérature académique et professionnelle du domaine des TI a été effectuée et l'analyse principale a été faite à partir d'un échantillon composé des 83 articles jugés comme

étant les plus pertinents. Cette démarche a permis dans un premier temps d'illustrer clairement le manque de consensus autour du comportement sécuritaire et de sa définition et, dans un second temps de recueillir un plus grand nombre d'éléments qui, mis en commun au terme d'une analyse rigoureuse, nous ont permis d'identifier les principales composantes du comportement sécuritaire.

6.2 Contributions de l'étude

Les contributions de cette recherche sont principalement de nature théorique, mais elles permettent d'établir de nouvelles bases pour des recherches futures qui pourront, à leur tour, apporter des nouvelles contributions à la pratique.

Dans un premier temps, le présent mémoire propose une définition plus uniforme et complète du concept de comportement sécuritaire. Il a notamment rendu possible l'identification d'éléments clés qui ont permis de construire la définition, mais aussi de mieux comprendre ce qui constitue un comportement sécuritaire. Ces éléments clés ont notamment contribué à identifier le but du comportement sécuritaire, à souligner l'importance des actions observables et ont aidé à spécifier le nom du concept qui devrait être utilisé.

De plus, cette définition pourra servir à développer un instrument de mesure uniforme pour le comportement sécuritaire. D'ailleurs, à cause du manque d'une définition claire, plusieurs études avaient développé des instruments de mesure différents, et ce, pour des concepts similaires. Un instrument uniforme permettrait donc d'éviter des incohérences dans les mesures des construits, ainsi que des résultats contradictoires, ce qui contribuerait à dissiper une autre partie du chaos entourant le comportement sécuritaire.

Ensuite, la présente recherche a également permis d'identifier au moins trois dimensions importantes du comportement sécuritaire et de décrire des manières dont chacune de ces dimensions pourrait contribuer à ce comportement. Elle a également

fait ressortir la pertinence de considérer ces dimensions toutes ensemble plutôt que séparément afin de mieux comprendre le comportement sécuritaire. De plus, nous avons pu proposer un modèle représentant les relations entre les dimensions et, même si notre modèle n'a pas été validé empiriquement, il peut néanmoins constituer un point de départ pour une éventuelle investigation plus approfondie de ces relations. Enfin, nous avons identifié deux propositions de recherche en lien avec les dimensions et leurs relations qui peuvent alimenter de nouvelles recherches, soit :

Proposition 1 : Le comportement sécuritaire gagne à être étudié en combinant les dimensions de la conformité, de l'éthique et du jugement.

Proposition 2 : Le comportement sécuritaire peut avoir d'autres dimensions que la conformité, l'éthique et le jugement.

En ce qui concerne le milieu professionnel, il est pertinent pour les praticiens d'avoir une définition claire de ce qu'est un comportement sécuritaire, car cela peut permettre à la direction d'établir plus précisément des objectifs et des indicateurs de performance SMART, ainsi que des politiques en matière de sécurité de l'information. Cela permettra ensuite à l'ensemble des employés de mieux comprendre ce qui est attendu d'eux à cet égard. Si chaque individu dans l'organisation comprend clairement ses responsabilités dans la protection de l'information organisationnelle, il pourrait ne plus agir comme un maillon faible de la sécurité de l'information. En effet, la sécurité de l'information relève d'une responsabilité collective de tous les employés d'une organisation, qu'ils soient des employés TI ou non-TI.

6.3 Limites de l'étude

Cette étude comporte plusieurs limites concernant les aspects méthodologiques. Tout d'abord, une des principales limites de notre étude se trouve dans le fait que le codage

et le tri des articles ont été effectués par une seule personne. Cela augmente de façon significative le risque de biais puisque le point de vue du codeur n'est pas confronté à celui d'autres chercheurs, ce qui ne permet pas d'avoir un consensus et de garantir l'objectivité totale de la démarche.

Ensuite, la qualité des revues dans lesquelles les articles de notre échantillon ont été publiés est une autre limite à prendre en considération. En effet, comme l'Infosec comportementale est un domaine très récent, il n'est pas étonnant que les études ne soient pas publiées dans les revues les plus prestigieuses, pour lesquelles le processus de publication est plus long. Le problème qui peut survenir ici est que les articles de l'échantillon sont majoritairement publiés dans des revues qui sont moins rigoureuses, notamment en termes de méthodologie, ce qui peut remettre en question la fiabilité de certains articles. Il faut également mentionner une certaine surreprésentation des études quantitatives dans l'échantillon étudié, qui constituaient 70% des articles académiques. Il s'agit d'une limite non négligeable, puisque la présente étude ne bénéficie pas suffisamment des avantages qu'apportent les études qualitatives, notamment de permettre de nuancer les résultats quantitatifs. Par ailleurs, une approche qualitative aurait également pu permettre de clarifier et d'expliquer certaines contradictions relevées dans la littérature, ce qu'aucun article de l'échantillon ne fait. Toutefois, ces limites ne sont pas très surprenantes, car nous avons sciemment choisi d'effectuer une revue systématique de type conceptuel, qui permet davantage de souplesse sur le critère de la qualité, et que d'autres types de revues de littérature plus strictes sur la qualité des articles ne nous auraient vraisemblablement pas permis d'avoir un échantillon suffisant pour cette étude. En effet, déjà que les articles trouvés étaient peu nombreux en faisant abstraction de la qualité des revues, nous estimons que si ce critère avait été pris en compte, nous n'aurions eu qu'une dizaine d'articles composant l'échantillon et ils n'auraient pas été récents pour la plupart.

Une autre limite a été le nombre de bases de données consultées. Nous avons utilisé celles qui retournaient le plus de résultats pertinents, mais nous aurions toujours pu en consulter davantage. Par ailleurs, il est à noter qu'en raison de la pandémie de Covid-

19, HEC Montréal était fermée au moment où nous avions effectué notre recherche d'articles et, par conséquent, nous n'avions pas accès à certaines bases de données, qui ne sont accessibles que sur place à partir des ordinateurs de la bibliothèque. Ensuite, la difficulté d'accéder à davantage de sources de littérature professionnelle constitue également une limite. Nous avions délibérément choisi de consulter cette catégorie de littérature dans le but d'enrichir nos connaissances sur le comportement sécuritaire et avoir un échantillon plus complet, mais notre recherche a donné relativement peu de résultats. Cela pourrait s'expliquer en partie par le fait que nous n'avions pas accès à certaines bases de données telles que Forrester (voir explication plus haut) et que les recherches dans les bases de données que nous avons pu consulter ne donnaient pas d'articles professionnels. Par ailleurs, il est difficile de dire s'il s'agit seulement d'une question d'accès, car il y a aussi le fait que certaines publications d'importance telles que *Harvard Business Review*, *MIT Sloan Management Review* ou *MISQ Executive* ne semblent pas avoir d'articles publiés sur le sujet à l'étude ici.

6.4 Pistes pour les recherches futures

La présente recherche ouvre plusieurs possibilités pour des études futures afin de permettre de combler les limites identifiées et d'approfondir certains aspects du comportement sécuritaire qui ne sont abordés que sommairement pour l'instant.

Ainsi, une piste de recherche importante serait la validation empirique du concept de comportement sécuritaire et de sa définition ou encore une validation des dimensions et de leurs relations. En effet, aucun des articles que nous avons recensés ne validait le concept et encore moins la définition, et seulement un petit nombre d'articles validait certaines relations entre les dimensions. Ces éléments pourraient être testés par des approches quantitatives ou qualitatives, mais nous croyons qu'un moyen fort pertinent serait de mener des entrevues avec des praticiens et des chercheurs car ces dernières pourraient permettre d'obtenir des données plus riches sur le comportement

sécuritaire et contribuer à augmenter l'apport qualitatif au domaine. Dans un ordre d'idées similaire, il serait important que les études s'intéressant à valider empiriquement des aspects du comportement sécuritaire emploient des mesures objectives pour ce faire, en l'occurrence utiliser le comportement réel et par conséquent des actions observables pour évaluer ce dernier.

De manière générale il y aurait lieu d'effectuer davantage d'études empiriques de nature qualitative, qui pourraient permettre d'abord de nuancer les résultats quantitatifs des études existantes, mais aussi de mieux comprendre le comportement et les motivations du comportement chez les employés (Crossler *et al.*, 2013). À cet effet, Crossler *et al.* (2013) mentionnent également la pertinence de mener des études longitudinales, par exemple pour évaluer l'adoption à long terme d'un comportement sécuritaire ou pour déterminer l'efficacité d'une théorie donnée pour prédire le comportement.

Notre recherche a fait ressortir que la plupart des articles n'examinent qu'une seule dimension du comportement sécuritaire et que quelques-uns étudient deux sur les trois principales dimensions identifiées. La pertinence de chacune de ces dimensions dans la compréhension du comportement sécuritaire est très claire dans la littérature, il faudrait désormais mener des études qui combinent les trois dimensions. Cela permettrait notamment de clarifier les relations existant entre ces dimensions, mais aussi d'avoir des pistes à savoir comment ce comportement se développe. Par ailleurs, étudier les trois dimensions simultanément pourrait permettre d'identifier s'il y a des lacunes significatives dans la compréhension du concept et soulever potentiellement la nécessité d'investiguer d'autres dimensions possibles.

Enfin, nous avions soulevé dans ce mémoire des éléments peu étudiés à ce jour, mais qui pourraient constituer des avenues de recherche prometteuses. D'abord, il y a la question de la pression temporelle et son impact sur le comportement des employés. Sachant que la plupart des incidents de sécurité sont causés de façon non intentionnelle, la pression temporelle et le temps que prend l'exécution d'actions liées à la sécurité

pourraient constituer une explication importante quant à l'adoption de comportements non sécuritaires de la part des employés. Ensuite, nous avions relevé dans quelques articles de Gartner la question des impacts de la manière dont une organisation utilise ses TI sur la sécurité de l'info. Alors que l'emphase est mise sur les impacts directs du comportement des employés sur la protection de l'actif informationnel, avec raison, il n'en demeure pas moins que l'utilisation des technologies par une organisation et certains aspects comme les recours à des partenaires ou à de tierces parties peut constituer une menace potentielle. Ce sujet n'a d'ailleurs été relevé dans aucun article académique à l'étude ici. Il serait pourtant intéressant de connaître les effets de ces pratiques, de même que leur prévalence, afin de permettre aux organisations de mieux adapter leurs stratégies en matière de sécurité.

Ultimement, les chercheurs devront utiliser la définition proposée ici pour la valider empiriquement dans différents contextes. Et même lorsqu'on aura une définition validée empiriquement, il restera encore beaucoup de recherche à faire afin de démystifier complètement le comportement sécuritaire.

Bibliographie

Abraham, Sherly et InduShobha Chengalur-Smith (2019). « Evaluating the effectiveness of learner controlled information security training », *Computers & Security*, vol. 87, p. 1-12.

Albrechtsen, Eirik (2007). « A qualitative study of users' view on information security », *Computers & Security*, vol. 26, no 4, p. 276-289.

Alohali, Manal, Nathan Clarke, Steven Furnell et Saad Albakri (2017). « Information security behavior: Recognizing the influencers », *2017 Computing Conference*, p. 844-853.

Barki, Henri (2008). « Thar's gold in them thar constructs », *The DATA BASE for Advances in Information Systems*, vol. 39, no 2, p. 9-20.

Bazargan, Michelle, Paul Proctor, Leigh McMullen et Peter Skyttegaard (2020). *20 culture hacks cios can use to make their organizations more secure*, Gartner.

Boss, Scott R., Dennis F. Galletta, Paul Benjamin Lowry, Gregory D. Moody et Peter Polak (2015). « What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors », *MIS Quarterly*, vol. 39, no 4, p. 837-864.

Boss, Scott R., Laurie J. Kirsch, Ingo Angermeier, Raymond A. Shingler et R. Wayne Boss (2009). « If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security », *European Journal of Information Systems*, vol. 18, no 2, p. 151-164.

Burns, A. J. (2019). « Security organizing: A framework for organizational information security mindfulness », *The DATA BASE for Advances in Information Systems*, vol. 50, no 4, p. 14-27.

Buytendijk, Frank (2017). *Digital ethics, or how to not mess up with technology*, Gartner.

Buytendijk, Frank, Jim Hare et Lydia Clougherty-Jones (2020a). *Digital ethics by design: A framework for better digital business*, Gartner.

Buytendijk, Frank, Brian Lee et Chris Howard (2020b). *Digital ethics: What every executive leader should know*, Gartner.

Cearley, David et Brian Burke (2018). *Top 10 strategic technology trends for 2019*, Gartner.

Chartrand, Geneviève (2010). *Vers une meilleure compréhension de la nature et des effets du soutien de la direction sur le succès des projets ti : Le regard des praticiens ti*, Maîtrise, Montréal, HEC Montréal.

Chen, Hao, Patrick Y. K. Chau et Wenli Li (2019). « The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior », *Information Technology & People*, vol. 32, no 4, p. 973-992.

Chowdhury, Noman H., Marc T. P. Adam et Geoffrey Skinner (2018). « The impact of time pressure on human cybersecurity behavior: An integrative framework », *2018 26th International Conference on Systems Engineering*.

Chowdhury, Noman H., Marc T. P. Adam et Timm Teubner (2020). « Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures », *Computers & Security*, vol. 97, p. 1-13.

Crossler, Robert E, Allen C. Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin et Richard Baskerville (2013). « Future directions for behavioral information security research », *Computers & Security*, vol. 32, p. 90-101.

Dang-Pham, Duy, Siddhi Pittayachawan et Vince Bruno (2017). « Why employees share information security advice? Exploring the contributing factors and structural patterns

of security advice sharing in the workplace », *Computers in Human Behavior*, vol. 67, p. 196-206.
de Guinea, Ana Ortiz et Guy Paré (2017). « What literature review type should i conduct? », dans *The routledge companion to management information systems*, p. 73-82.
den Hamer, Pieter, Katie Gove, Bart Willemsen, Christie Struckman et Frank Buytendijk (2020). *Digital ethics: From compliance duty to competitive differentiator*, Gartner.
Dinev, Tamara et Qing Hu (2007). « The centrality of awareness in the formation of user behavioral intention toward protective information technologies * », *Journal of the Association for Information Systems*, vol. 8, no 7, p. 386-408.
Donalds, Charlette et Kweku-Muata Osei-Bryson (2020). « Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents », *International Journal of Information Management*, vol. 51, p. 1-16.
Dulipovici, Alina et Richard L. Baskerville (2015). « An eduction model of disciplinary emergence: The ripples of knowledge management », *Knowledge Management Research & Practice*, vol. 13, no 2, p. 115-133.
EY (2018). *Is cybersecurity about more than protection?*
EY (2020). *Your employees are the weakest link in your cybersecurity chain*. Récupéré de https://www.ey.com/en_ca/cybersecurity/your-employees-are-the-weakest-link-in-your-cybersecurity-chain
Furnell, Steven et Nathan Clarke (2012). « Power to the people? The evolving recognition of human aspects of security », *Computers & Security*, vol. 31, p. 983-988.
Furnell, Steven et Kerry-Lynn Thomson (2009). « From culture to disobedience: Recognising the varying user acceptance of it security », *Computer Fraud & Security*, vol. 2, p. 5-10.
Gawronski, Bertram (2012). « Back to the future of dissonance theory: Cognitive consistency as a core motive », *Social cognition*, vol. 30, no 6, p. 652-668.
Hadlington, Lee, Jens Binder et Natalia Stanulewicz (2021). « Exploring role of moral disengagement and counterproductive work behaviours in information security awareness », *Computers in Human Behavior*, vol. 114, p. 1-8.
Hare, Jim, Frank Buytendijk et Lydia Clougherty Jones (2018). *Hype cycle for data security - digital ethics*, Gartner.
Harmon-Jones, Eddie et Cindy Harmon-Jones (2007). « Cognitive dissonance theory after 50 years of development », *Zeitschrift für Sozialpsychologie*, vol. 38, no 1, p. 7-16.
Herath, Tejaswini, Yim Myung-Seong, D'Arcy John, Kichan Nam et H. R. Rao (2018). « Examining employee security violations: Moral disengagement and its environmental influences », *Information Technology & People*, vol. 31, no 6, p. 1135-1162.
Herath, Tejaswini et H. R. Rao (2009a). « Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness », *Decision Support Systems*, vol. 47, no 2, p. 154-165.
Herath, Tejaswini et H. Raghav Rao (2009b). « Protection motivation and deterrence: A framework for security policy compliance in organisations », *European Journal of Information Systems*, vol. 18, no 2, p. 106-125.
Hsu, Jack Shih-Chieh, Sheng-Pao Shih, Yu Wen Hung et Paul Benjamin Lowry (2015). « The role of extra-role behaviors and social controls in information security policy effectiveness », *Information Systems Research*, vol. 26, no 2, p. 282-300.
Huisman, Joanna (2018). *Effective security awareness starts with defined objectives*, Gartner.
Huisman, Joanna et Perry Carpenter (2019). *Avoid 10 common security awareness mistakes*, Gartner.

IBM (2020). *Cost of a data breach report 2020 highlights*, IBM Security. Récupéré le 19 octobre 2020 https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Ifinedo, Princely (2014). « Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition », *Information & Management*, vol. 52, p. 69-79.

Kajtazi, Miranda, Hasan Cavusoglu, Izak Benbasat et Darek Haftor (2018). « Escalation of commitment as an antecedent to noncompliance with information security policy », *Information and Computer Security*, vol. 26, no 2, p. 171-193.

Karjalainen, Mari, Mikko Siponen et Suprateek Sarker (2020). « Toward a stage theory of the development of employees' information security behavior », *Computers & Security*, vol. 93, p. 1-18.

Kim, Sang Soo et Yong Jin Kim (2017). « The effect of compliance knowledge and compliance support systems on information security compliance behavior », *Journal of Knowledge Management*, vol. 21, no 4, p. 986-1010.

Korolov, Maria (2015). *Does security awareness training even work?*, CSO Online. Récupéré le 10 septembre 2020 https://www.csoonline.com/article/2987822/does-security-awareness-training-even-work.html

Lankton, Nancy K., Charles Stivason et Anil Gurung (2019). « Information protection behaviors: Morality and organizational criticality », *Information and Computer Security*, vol. 27, no 3, p. 468-488.

Larousse (2020). *Attitude*. Récupéré le 29 novembre 2020 https://www.larousse.fr/dictionnaires/francais/attitude/6295

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar et Xiaohong Yuan (2019). « Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior », *International Journal of Information Management*, vol. 45, p. 13-24.

MacKenzie, Scott B., Philip M. Podsakoff et Nathan P. Podsakoff (2011). « Construct measurement and validation procedures in mis and behavioral research: Integrating new and existing techniques », *MIS Quarterly*, vol. 35, no 2, p. 293-334.

Mamonov, Stanislav et Raquel Benbunan-Fich (2018). « The impact of information security threat awareness on privacy-protective behaviors », *Computers in Human Behavior*, vol. 83, p. 32-44.

McCormac, Agata, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius et Malcolm Pattinson (2017). « Individual differences and information security awareness », *Computers in Human Behavior*, vol. 69, p. 151-156.

McMillan, Rob et Jay Heiser (2018). *Five golden rules for creating effective security policy*, Gartner.

Moeini, Mohammad et Suzanne Rivard (2019). « Sublating tensions in the it project risk management literature: A model of the relative performance of intuition and deliberate analysis for risk assessment », *Journal of the Association for Information Systems*, vol. 20, no 3, p. 243-284.

Moody, Gregory D., Mikko Siponen et Seppo Pahnila (2018). « Toward a unified model of information security policy compliance », *MIS Quarterly*, vol. 42, no 1, p. 285-311.

Ng, Boon-Yuen, Atreyi Kankanhalli et Yunjie Calvin Xu (2009). « Studying users' computer security behavior: A health belief perspective », *Decision Support Systems*, vol. 46, p. 815-825.

Nguyen, Cindy (2017). *Mieux comprendre l'influence de la culture et du climat organisationnels sur les pratiques en sécurité de l'information*, Maîtrise ès sciences en gestion, Montréal, HEC Montréal.

Okoli, Chitu et Kira Schabram (2010). « A guide to conducting a systematic literature review of information systems research », *Sprouts: Working Papers on Information Systems*, vol. 10, no 26, p. 1-49.

Omidosu, Joseph et Jacques Ophoff (2016). « A theory-based review of information security behavior in the organization and home context », *2016 Third International Conference on Advances in Computing, Communication and Engineering*, p. 225-231.

Parsons, Kathryn, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac et Tara Zwaans (2017). « The human aspects of information security questionnaire (hais-q): Two further validation studies », *Computers & Security*, vol. 66, p. 40-51.

Parsons, Kathryn, Agata McCormac, Marcus Butavicius et Lael Ferguson (2010). *Human factors and information security: Individual, culture and security environment*, no DSTO-TR-2484, Australia, Command, Control, Communications and Intelligence Division Defence Science and Technology Organisation.

Parsons, Kathryn, Elise Young, Marcus Antanas Butavicius, Agata McCormac, Malcolm Robert Pattinson et Cate Jerram (2015). « The influence of organizational information security culture on information security decision making », *Journal of Cognitive Engineering and Decision Making*, vol. 9, no 2, p. 117–129.

Politique de sécurité de l'information (2019). Montreal, HEC Montréal.

PwC (s.d.). *Workforce pulse survey: It's time to adopt a cyber-savvy culture*. Récupéré le 7 septembre 2020 https://www.pwc.com/us/en/library/covid-19/workforce-pulse-survey.html?WT.mc_id=CT1-PL50-DM2-TR1-LS4-ND40-PR3-CN_Covid19WorkplaceReboot-&eq=CT1-PL50-DM2-CN_Covid19WorkplaceReboot

Reed, Brian, Richard Addiscott et Claude Mandy (2020). *Market guide for security awareness computer-based training*, Gartner.

Rhee, Hyeun-Suk, Cheongtag Kim et Young U. Ryu (2009). « Self-efficacy in information security: Its influence on end users' information security practice behavior », *Computers & Security*, vol. 28, no 8, p. 816-826.

Ruighaver, A. B., S. B. Maynard et M. Warren (2010). « Ethical decision making: Improving the quality of acceptable use policies », *Computers & Security*, vol. 29, no 7, p. 731-736.

Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani et Tutut Herawan (2015). « Information security conscious care behaviour formation in organizations », *Computers & Security*, vol. 53, p. 65-78.

Safa, Nader Sohrabi, Rossouw Von Solms et Steven Furnell (2016). « Information security policy compliance model in organizations », *Computers & Security*, vol. 56, p. 70-82.

Sampath, Srinath (2019). *Fight unsecure employee behaviors by fixing your risk culture*, Gartner.

Shropshire, Jordan, Merrill Warkentin et Shwadhin Sharma (2015). « Personality, attitudes, and intentions: Predicting initial adoption of information security behavior », *Computers & Security*, vol. 49, p. 177-191.

Siponen, Mikko, M. Adam Mahmood et Seppo Pahnila (2014). « Employees' adherence to information security policies: An exploratory field study », *Information & Management*, vol. 51, no 2, p. 217-224.

Sommestad, Teodor (2018). « Work-related groups and information security policy compliance », *Information and Computer Security*, vol. 26, no 5, p. 533-550.

Sommestad, Teodor, Henrik Karlzén et Jonas Hallberg (2015). « The sufficiency of the theory of planned behavior for explaining information security policy compliance », *Information and Computer Security*, vol. 23, no 2, p. 200-217.

Szajna, Bernadette et Richard W. Scamell (1993). « The effects of information system user expectations on their performance and perceptions », *MIS Quarterly*, vol. 17, no 4, p. 493-516.

Templier, Mathieu et Guy Paré (2015). « A framework for guiding and evaluating literature reviews », *Communications of the Association for Information Systems*, vol. 37, no Article 6, p. 112-137.

Topa, Ioanna et Maria Karyda (2019). « From theory to practice: Guidelines for enhancing information security management », *Information and Computer Security*, vol. 27, no 3, p. 326-342.

Tsohou, Aggeliki et Philipp Holtkamp (2018). « Are users competent to comply with information security policies? An analysis of professional competence models », *Information Technology & People*, vol. 31, no 5, p. 1047-1068.

van Bavel, René, Nuria Rodríguez-Priego, José Vila et Pam Briggs (2019). « Using protection motivation theory in the design of nudges to improve online security behavior », *International Journal of Human-Computer Studies*, vol. 123, p. 29-39.

Van de Ven, Andrew H. et Marshall Scott Poole (1995). « Explaining development and change in organizations », *The Academy of Management Review* vol. 20, no 3, p. 510-540.

Wall, Jeffrey D., Prashant Palvia et Paul Benjamin Lowry (2013). « Control-related motivations and information security policy compliance: The role of autonomy and efficacy », *Journal of Information Privacy & Security*, vol. 9, no 4, p. 52-79.

Wall, Jeffrey D., Bernd Carsten Stahl et A. F. Salam (2015). « Critical discourse analysis as a reviewmethodology: An empirical example », *Communications of the Association for Information Systems*, vol. 37, no 11, p. 258-285.

Walls, Andrew (2013). *Short, focused and just-in-time approaches to security awareness*, Gartner.

Warkentin, Merrill, Allen C. Johnston, Jordan Shropshire et William D. Barnett (2016). « Continuance of protective security behavior: A longitudinal study », *Decision Support Systems*, vol. 92, p. 25-35.

Watts, John (2020). *How to respond to the 2020 threat landscape*, Gartner.

Webster, Jane et Richard T. Watson (2002). « Analyzing the past to prepare for the future: Writing a literature review », *MIS Quarterly*, vol. 26, no 2, p. xiii-xxiii.

Weems, Carl F., Irfan Ahmed, Golden G. Richard, Justin D. Russell et Erin L. Neill (2018). « Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behavior », *Plos One*, vol. 13, no 12, p. 1-18.

Westerman, George (2009). « It risk as a language for alignment », *MIS Quarterly Executive*, vol. 8, no 3, p. 109-121.

Williams, Clay K., Donald Wynn, Ramana Madupalli, Elena Karahanna et Barbara K. Duncan (2014). « Explaining users' security behaviors with the security belief model », *Journal of Organizational and End User Computing*, vol. 26, no 3, p. 23-46.

Wu, Yu, Carl S. Guynes et John Windsor (2012). « Security awareness programs », *Review of Business Information Systems*, vol. 16, no 4, p. 165-168.

Xiao, Yu et Maria Watson (2019). « Guidance on conducting a systematic literature review », *Journal of Planning Education and Research*, vol. 39, no 1, p. 93-112.

Yan, Zheng, Thomas Robertson, River Yan, Sung Yong Park, Samantha Bordoff, Quan Chen*, et al.* (2018). « Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? », *Computers in Human Behavior*, vol. 84, p. 375-382.

Yazdanmehr, Adel et Jingguo Wang (2016). « Employees' information security policy compliance: A norm activation perspective », *Decision Support Systems*, vol. 92, p. 36-46.

Annexe 1 – Guide de codage

Champ	Description	Valeurs/codes
1. Information bibliographiques	Informations de base sur l'article comme l'auteur, le titre, la date de publication et la revue où l'article a été publiée.	*(utilisation du logiciel EndNote)*
2. Concept utilisé dans l'article	Termes utilisés dans l'article pour désigner le concept ou ses dimensions	2.1. Terme utilisé pour le comportement sécuritaire (général, dimension non spécifiée) 2.2. Terme utilisé pour la dimension conformité 2.3. Terme utilisé pour la dimension éthique 2.4. Terme utilisé pour la dimension jugement
3. Définition du concept	Définition, mot pour mot, utilisée dans l'article pour définir le concept ou ses dimensions.	3.1. Définition du concept de comportement sécuritaire 3.2. Définition d'un concept connexe 3.3. Absence de définition, mais le concept de comportement sécuritaire est mentionné dans l'article
4. Actions du comportement	Description, dans l'article, d'actions qui constituent un comportement sécuritaire, de préférence concrètes et perceptibles	4.1. Actions liées à des pratiques de sécurité (p.ex. rapporter des éléments suspects, suivre des formations, utiliser des mots de passe forts) 4.2. Actions liées à l'utilisation d'une technologie (p.ex. antivirus, pare-feu)
5. Dimension associée	Dimension(s) du comportement sécuritaire abordée(s) dans l'article	5.1. Conformité 5.2. Éthique 5.3. Jugement
6. Justification de la dimension	Éléments mentionnés dans l'article permettant d'expliquer la dimension identifiée	6.1. La définition donnée pour le comportement sécuritaire 6.2. Le cadre théorique 6.3. Autre : spécifier en toutes lettres
7. Cadre théorique	Cadre théorique qui a servi de référence pour l'étude du concept	7.1. Protection Motivation Theory 7.2. Theory of Planned Behavior 7.3. Autre, spécifier
8. Méthode utilisée	Méthode utilisée pour la collecte de données mesurant le comportement sécuritaire	8.1. Sondage (survey) : collecte de données à partir d'un échantillon de la population à l'étude, par questionnaire et menant à une analyse statistique (corrélation, etc.); 8.2. Étude de cas (single or multiple case study) : collecte de données par observation, entrevues et différentes sources documentaires sur un cas précis; 8.3. Méta-analyse : démarche statistique combinant les résultats d'une série d'études indépendantes sur un problème donné. 8.4. Article conceptuel 8.5. Autre : spécifier en toutes lettres

9. Mesures utilisées	Éléments de mesure utilisés pour le concept de comportement sécuritaire dans le cadre de la collecte de données de l'article : items de questionnaires, questions d'une grille d'entrevue, etc.	9.1. Items de questionnaires 9.2. Questions d'entrevue 9.3. Autre : spécifier en toutes lettres
10. Caractéristiques des répondants	Ce champ permet d'indiquer les personnes qui ont répondu à l'enquête (si l'article n'est pas conceptuel ou une méta-analyse)	10.1. Gestionnaire TI, 10.2. Utilisateur /spécialiste TI 10.3. Utilisateur non TI 10.4. Autre : spécifier
11. Utilisation du concept	Comment le concept de comportement sécuritaire est utilisé dans l'article	11.1. Comme variable dépendante 11.2. Comme variable indépendante 11.3. Comme variable intermédiaire (modératrice ou médiatrice)
12. Liens entre dimensions	Si l'article voit le comportement sécuritaire comme un concept multidimensionnel, quels sont les liens proposés et/ou validés entre les dimensions?	(en mots)
13. Conditions	Si l'article avance un concept multidimensionnel, dont les dimensions se réalisent de manière consécutive, quelles sont les conditions qui influence le passage d'une dimension à une autre?	(en mots)
14. Domaine principal de l'article	Domaine scientifique concerné par l'article	14.1. Technologies de l'information 14.2. Management 14.3. Health informatics 14.4. Autre: spécifier
15. Commentaires	Commentaires jugés pertinents par le lecteur, pour une meilleure compréhension de l'article ou pour ajouter des informations pertinentes pour la recherche.	(en mots)

Annexe 2 – Exemple d'un extrait du codage

Article	Code EndNote	Concept utilisé dans l'article	Définition du concept	Actions observables du comportement	Dimension associée	Justification de la dimension	Cadre théorique	Méthode	Mesures	Caractéristiques répondants	Utilisation du concept	Lien mentionn d'autre
Karjalainen et al. (2020)	#259	2.2 Information security behavior	3.3 Pas explicitement défini, mais l'étude suggère le comportement comme quelque chose qui se développe par phases et change avec le temps	4.1 Verrouiller son ordinateur, mots de passe: actions suggérées par les réponses d'entervue, mais pas explicitement mentionnées dans l'étude	5.1	6.2	7.3 Stage theories	8.2	9.2	10.4 Employés de différents niveaux d'une organisation du secteur maritime et de l'énergie, plusieurs pays	11.1	n.d.
Ng et al. (2009)	#280	2.4 Computer security behavior	3.1 "Computer security behavior in organisations [...] is broader than compliance to organisational security policies" (p.816)	4.1 Mots de passe forts, faire régulièrement des copies de sauvegarde, précautions et vérification avec les pièces jointes des courriels, s'informer sur les pratiques des sécurité	5.3	6.1	7.3 Health Belief Model	8.1	9.1	10.4 Étudiants universitaires en TI (temps partiel) et employés dans des organisations TI	11.1	n.d.
Ruighaver et al. (2010)	#472	2.3 Ethical behavior	3.3 Pas explicitement défini, mais: "Our current approach to address this socio-technical gap in acceptable use policy development is based on the assumption that the behaviour of IT users is no longer primarily based on following rules, but that most users are willing to consider the consequences that their behaviour might have for the organisation" (p.733)	n.d	5.2 5.3	6.3 : Le but de l'étude: voir colonne définition Aussi,pont vers le jugement: The advantage is that employees will now become aware of the consequences many of their actions will have for the security of the organisation, which will assist them in unforeseen situations (p.735)	7.3 Différents principes et théories de l'éthique mis en comparaison avec des politiques organisationnelles traditionnelles	8.2	9.2 9.3: données secondaires	10.4 Différentes parties prenantes d'une compagnie de services TI de taille moyenne	11.1	L'étude suggère éthiques peuven davantage le jug

Annexe 3 – Répartition des articles par publication

Nom de la publication	Nombre d'articles
Computers & Security	14
Computers in Human Behavior	5
Decision Support Systems	4
European Journal of Information Systems	2
Information and Computer Security	9
Information Systems Frontiers	2
Information Technology & People	5
International Journal of Information Management	3
Journal of the Association for Information Systems	4

Autres publications (un seul article par publication)

Revues

Information & Management
Information Management & Computer Security
Information Systems Management
Information Systems Research
International Journal of Human-Computer Studies
International Journal of Information Security and Privacy
International Journal of Medical Informatics
Journal of Information Privacy & Security
Journal of Information Security and Applications
Journal of Information Systems and Technology Management
Journal of Knowledge Management
Journal of Management Policy and Practice
Journal of Organizational and End User Computing
Online Information Review
Plos One
Sustainability

Conférences

2016 Third international conference on advances in computing, communication and engineering
2017 Computing Conference
2017 IEEE International conference on intelligence and security informatics
2018 26th International conference on systems engineering

Annexe 4 – Définitions du comportement sécuritaire

Auteur	Nom du concept	Définition
Abraham et Chengalur-Smith (2019)	Behavior intention	"Behavioral intention is defined as the intention of the user to perform the recommended action" (p.4)
Boss et al. (2009)	Precaution taking	“precaution taking is defined as the degree to which individuals perceive they take measures to secure their computers and deal with information security in accordance with prescribed corporate security policies and procedures as well as through individual, proactive actions” (p.155)
Burns et al. (2019)	Protection motivated behaviors	“PMBs are the volitional behaviors organizational insiders can enact to protect organizational information and ISs from information-security threats” (p.1)
Chu et So (2020)	Unethical information security behavior	3.1 "voluntary employee behavior characterized by a failure to follow organizational rules, standards, codes, or principles that may affect the privacy, accuracy, property, and/or accessibility of information in the workplace. Employees who engage in unethical information security behavior may not have malicious intentions, but they may try to benefit themselves, such as saving time or accessing extra information to complete a task." (p.3)
Connolly et al. (2017)	Employee security behavior	"the behaviour of employees in using organisational IS (including hardware, software, and network systems etc.), and such behaviour may have security implications" (p.123)
Crossler et al. (2019)	Security behavior	"the behaviors of individuals which relate to protecting information and information systems assets" (p.344)
Dang-Pham et al. (2017)	Security knowledge sharing	the “provision of task information and know how to help others and to collaborate with others to solve problems, develop new ideas, or implement policies or procedures” (p.197)
Doherty et Tajuddin (2018)	Compliant security behavior	"set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies" (p.350)
Donalds et Osei-Bryson (2020)	Security compliance behavior	"security compliance relates to individuals and how s/he perceives and comprehend security threats and chooses to respond, i.e., whether to comply or not with security best practices" (p.2)

Hsu et al. (2015)	In-role behavior Extra-role behavior	"**in-role** behaviors, which are required or expected organizational behaviors that are the basis of regular and ongoing job performance evaluations and are linked to rewards and punishments" "Accordingly, mindful employees should be motivated to pay attention to others' behaviors in an interdependent context and thus engage in **extra-role** behaviors such as performing altruistic behaviors to aid others [...]and speaking up with the intent to improve organizational functioning" (p.283)
Hwang et Cha (2018)	Information security compliance	"Compliance intention is defined as an employee's intention to protect the organization's information resources**"** (p.286)
Khatib et Barki (2020)	Information security noncompliance	"Information security violations occur when employees contravene an organization's ISP, which provides them with instructions about what they should do to safeguard their organization's information and technology resource" (p.486)
Kim et Kim (2017)	Compliance intention	"compliance intention is defined as an individual's intention to protect information and technology resources from potential security-related damages" (p.988)
Lin et Wittmer (2017)	Proactive information security behavior	"It is "taking initiative in improving current circumstances, it involves challenging the status quo rather than passively adapting present conditions"" (p.1)
Ng et al. (2009)	Computer security behavior	"Computer security behavior in organisations […] is broader than compliance to organisational security policies" (p.816)
Omidosu et Ophoff (2016)	Information security behavior	"applying recommended practices that would facilitate the achievement of information confidentiality, integrity and availability of computer systems resources" (p.226)
Rhee et al. (2009)	Security practice behavior	" the use of security technology and security conscious care behavior" (p.817) self-efficacy in information security: "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability" (p.818)
Safa et al. (2015)	Conscious care behavior	"Conscious care behaviour means that users think about the consequences of their actions in terms of information security when they work with a system, particularly on the Internet." (p.66)

Safa et al. (2016)	Information security behavior information security organizational policies and procedures (ISOP) compliance	"information security behaviour, besides the technological aspects of information security, mitigates the risk of information security breaches in organizations" (p.71) ISOP compliance: non défini, mais les items de questionnaire suggèrent qu'il s'agit de suivre les politiques et pratiques de l'organisation
Vedadi et Warkentin (2020)	Secure behavior	Définition de la variable behavioral intention: "Users' intention to use a particular security solution" (p.450)
Warkentin et al. (2016)	Protective security behavioral continuance	"the use of any protective behavioral security action subsequent to initial adoption" (p.26)
Williams et al. (2014)	Security behavior intentions	"the extent to which an individual intends to adopt certain behaviors that serve to minimize or eliminate potential information security threats" (p.28)
Zauwiyah et al. (2019)	Security assurance behavior	"SAB represents employees' intentional and effortful actions that are aimed towards protecting information systems, for instance, using strong passwords for computer access, performing data backup regularly and checking the recipients list prior sending out emails" [...] SAB is a learned behaviour that can be improved if the human factor is properly addressed by organisations" (p.166)
Littérature professionnelle		
Buytendijk (2017), Gartner	Digital ethics	"Digital ethics is just two things: How not to mess up with digital technologies. How to use technology to do "the right thing" for all stakeholders, contributing to "the good life"." (définiton informelle, p.3) "The systems of values and moral principles for the conduct of electronic interactions." (définition formelle, p.3)
Buytendijk et al. (2020b), Gartner	Digital ethics	"Digital ethics comprises the systems of values and moral principles for the conduct of electronic interactions among people, organizations and things." (p.2)
den Hamer et al. (2020), Gartner	Digital Ethics	Idem que ci-dessus, mais aussi "ethics is about so much more thanregulatory compliance" (p.2)

Kim et al. (2020), Gartner	Ethics and compliance management	"There are five common ethics and compliance management capabilities including: 1. Code of conduct and corporate policy management 2. Employee compliance training and certification 3. Conflict of interest (COI) disclosure management 4. Gifts and entertainment approval workflow 5. Whistleblower hotline and investigative case management" (p.2)
Scholtz et al. (2015), Gartner	People centric security	People-centric security (PCS) is a strategic approach to information security that emphasizes individual accountability and trust, and that de-emphasizes restrictive, preventive security controls. PCS is based on a set of key principles, and on the rights and related responsibilities of individuals. The premise of PCS is that employees have certain rights — but these are linked to specific responsibilities.

Annexe 5 – Actions du comportement sécuritaire

Article	Code EndNote	Concept utilisé dans l'article	Actions observables du comportement	Dimension associée
Albrechtsen (2007)	#266	Information security role of users	Verrouiller son ordinateur, mots de passe forts, précautions avec les courriels et l'usage d'Internet, ne pas utiliser de logiciels non-autorisés, précautions si utilisation de biens appartenant à l'organisation à l'extérieur de celle-ci, rapporter les brèches de sécurité	Conformité (suggéré, pas explicite)
Boss et al. (2009)	#110	Precaution taking	Être sensibilisé à la sécurité faire de son mieux pour assurer la sécurité du système (suggéré par les items)	Conformité
Burns et al. (2019)	#143	Protection motivated behaviors	Se rappeler entre collègues les pratiques à adopter, reconnaître et rapporter un comportement suspect d'un employé, être sensibilisé aux politiques de sécurité, se conformer aux politiques	Conformité Jugement (suggéré par l'idée d'adaptation dans les items)
Cavallari (2012)	#466	Information system security	Suivre les politiques organisationnelles et respecter les législations et règlementations; gestion des accès sur les infrastructures et plateformes, sécurité du réseau, audit	Conformité

Chowdhury et al. (2018)	#323	Human cybersecurity behavior	(non sécuritaire): **Divulgation** (mots de passe, données sensibles) **Autorisation d'accès** (à son poste de travail, à ses appareils personnels p.ex) Évitement (des formations Infosec p.ex.) **Inaction** (ne pas agir à un avertissement de sécurité, ne pas utiliser d'anti-virus ou d'outils de chiffrement) **Faire trop confiance** **Laxisme/indifférence** (face aux pratiques et politiques, pour rapporter des incidents p.ex.)	Conformité Jugement
Chowdhury et al. (2020)	#158	Human cybersecurity behavior	(non sécuritaire) Évitement, contournement des autorisations d'accès, divulgation, inaction/laxisme, influence négative des collègues, faire trop confiance	Conformité Jugement
Chu et So (2020)	#331	Unethical information security behavior	(non sécuritaire) Comportement imprudent avec les réseaux ou les applications, utilisation dangereuse du web, comportement d'omission (ne pas verrouiller son poste de travail, laisser trainer des informations, p.ex.), mauvaise gestion des accès	Éthique
Connolly et al. (2017)	#41	Employee security behavior	Gestion des mots de passe, manière d'utiliser les données organisationnelles et les ressources liées au réseau	Conformité
Da Veiga et Eloff (2010)	#225	Information security behavior	Rapporter des incidents de sécurité, application d'un clear desk policy, élimination (disposal) sécuritaire de documents contenant des informations confidentielles	Conformité

Fernández-Alemán et al. (2015)	#279	Security behavior	Choix et protection des mots de passe, copies de sauvegarde régulières, précautions avec liens et pièces jointes dans les courriels	Conformité (suggéré, pas explicite)
Herath et Rao (2009a)	#255	Information security behavior Security policy compliance	Suivre les politiques organisationnelles en matière de sécurité	Conformité
Herath et Rao (2009b)	#111	Security policy compliance intention	Suivre les politiques organisationnelles en matière de sécurité, se conformer aux exigences des politiques (suggéré par les items)	Conformité
Hsu et al. (2015)	#559	In-role behavior Extra-role behavior	**In-role**: s'adapter aux changements nécessaires en matière de sécurité, acquérir de nouvelles compétences pour s'adapter à ces changements effectuer les actions nécessaires pour assurer la sécurité (suggéré par les items) **Extra-role**: aider ses collègues à bien appliquer les principes de sécurité, s'exprimer pour suggérer des améliorations au programme de sécurité	Conformité Jugement
Hwang et Cha (2018)	#426	Information security compliance	Les items suggèrent qu'il s'agit de suivre les politiques en matière de sécurité	Conformité
Kajtazi et al. (2018)	#78	Non compliance with information security policy	(non sécuritaire) Idée que c'est le fait de ne pas suivre les politiques de sécurité, principalement pour pouvoir compléter une tâche puisque de suivre les politiques constituerait un obstacle à le complétion de la tâche	Conformité

Karjalainen et al. (2020)	#259	Information security behavior	Verrouiller son ordinateur, mots de passe: actions suggérées par les réponses d'entrevue, mais pas explicitement mentionnées dans l'étude	Conformité
Khatib et Barki (2020)	#468	Information security non compliance	(non sécuritaire): Copier des données confidentielles sur une clé USB non sécurisée pour pouvoir travailler de la maison, laisser son ordinateur ouvert pour ne pas perdre de temps avec le démarrage, partager un mot de passe avec un collègue pour pouvoir terminer une tâche urgente plus rapidement	Conformité
Kim et Han (2019)	#72	Information security policy (ISP) Compliance	Suivre les politiques organisationnelles en matière de sécurité afin de protéger les SI de l'organisation (suggéré par les items)	Conformité
Kim et Kim (2017)	#457	Compliance intention	Se conformer aux lois et règlementations liées à son emploi, encourager ses collègues à s'y conformer, ne pas violer les lois et règlementations (suggéré par les items)	Conformité
Klein et Luciano (2016)	#43	Safe bahavior	Précaution générale avec les courriels: vérifier l'expéditeur, vérifier le nom des pièces jointes, ne pas ouvrir le courriel s'il semble suspect	Conformité
Li et al. (2019)	#161	Cyberscurity behavior Information security behavior	Suivre des formations en Infosec, confiance pour gérer des des fichiers infectés, des malware etc.; anti-virus, configurations de sécurité pour le navigateur web (suggéré par les items)	Conformité

Lin et Wittmer (2017)	#346	Proactive information security behavior	Initier quelque chose sans qu'on le demande explicitement à l'employé et sans que cela fasse partie de ses tâches, avoir des idées orientées vers le long terme. 2 composantes clés: implantation proactive d'idées et résolution proactive de problèmes	Jugement
Mamonov et Benbunan-Fich (2018)	#561	privacy-protective behaviors	Refus de divulguer des informations personnelles en ligne, choix d'un mot de passe fort	Jugement
Ng et al. (2009)	#280	Computer security behavior	Mots de passe forts, faire régulièrement des copies de sauvegarde, précautions et vérification avec les pièces jointes des courriels, s'informer sur les pratiques de sécurité	Jugement
Parsons et al. (2010), Command, Control, Communications and Intelligence Division Defence Science and Technology Organisation	#580	Security behavior	Pas explicitement établies, mais le rapport suggère que ce sont des actions permettant de prévenir le piratage psychologique (p.ex. mots de passe, verrouiller son ordinateur, ne pas transmettre des données senisbles par téléphone intelligent, etc.)	Conformité
Rhee et al. (2009)	#579	Security practice behavior	Pratiques de conformité lors de l'utilisation d'un ordinateur ou d'Internet, tels que choisir des mots de passe forts et faire des copies de sauvegarde régulièrement, utilisation de technologies pour la sécurité tels que des anti-virus, logiciels anti-espion, blocage de pop-ups	Jugement Conformité
Safa et al. (2015)	#189	Conscious care behavior	Consulter des experts en sécurité au besoin, réfléchir aux conséquences avant de poser une action, miser sur son expérience pour évaluer une situation	Jugement

Safa et al. (2016)	#233	Information security behavior Information security organizational policies and procedures (ISOP) compliance	Se conformer aux pratiques et politiques, collaborer avec des collègues et des experts pour favoriser la protection des actifs	Conformité
Sommestad (2018)	#30	Information security policy compliance	(non sécuritaire): Ouvrir un courriel d'hameçonnage, naviguer des sites web malicieux, brancher des clés USB infectées, transférer des données sur un ordinateur personnel	Conformité
Sommestad et al. (2015b)	#48	Information security policy compliance	Adhérer aux pratiques prescrites par la politique, ne pas violer la politique (suggéré par les items)	Conformité
Takemura (2011)	#60	Information security awareness and behavior	S'informer sur la sécurité de l'information, recevoir une formation, ne pas faire suivre des chaînes de courriels (chain mail), ne pas se connecter à des réseaux Internet non encryptés, utiliser un anti-virus	Conformité
van Bavel et al. (2019)	#470	Online security behavior	Selon l'expérience: choisir une connexion sécurisée, choisir un vendeur de confiance, choisir un mot de passe fort, se déconnecter	Jugement
Van Slyke et Belanger (2020)	#249	Insider security behaviors	(non sécuritaire) Violation des politiques de sécurité, écrire des mots de passe sur papier, réutiliser des mots de passe	Jugement (idée d'un comportement qui va au-delà de la conformité)
Wall et al. (2013)	#100	Information security policy (ISP) Compliance	Se conformer aux exigences de la politique de sécurité, protéger l'information et les actifs selon ce qui est prescrit dans la politique, accomplir les responsabilités prescrites dans la politique (suggéré par les items)	Conformité

Weems et al. (2018)	#370	Secure/insecure behavior	Faire preuve de prudence avec les courriels et les pop-ups, faire attention avec les téléchargements 4.2 Effectuer des mises à jour (suggéré par les items)	Jugement
Williams et al. (2014)	#363	Security behavior intentions	Installer des solutions protectrices (anti-virus, pare-feu, etc.), effectuer les mises à jour, utiliser les logiciels pour prévenir les accès non-autorisés, appliquer les politiques de la compagnie	Conformité
Yan et al. (2018)	#159	Cybersecurity judgement	Évaluer le risque d'une situation donnée et prendre les actions de sécurité appropriées (suggéré par la méthodologie)	Jugement
Yazdanmehr et Wang (2016)	#447	Information security policy compliance behavior	Le fait de suivre les politiques (suggéré par les items de questionnaire)	Conformité
Littérature professionnelle				
Buytendijk (2017), Gartner	#572	Digital ethics	**Accountability**: faire preuve de transparence au sujet de ses actions **Responsibility**: prendre responsabilité des conséquences (même inattendues) liées à l'exploitation des TI	Éthique
Buytendijk et al. (2020a), Gartner	#570	Digital ethics/care ethics	**Empathie**: se soucier des clients et des autres parties prenantes (en ce qui concerne l'utilisation des TI) **Responsabilité**: prendre responsabilité des conséquences potentiellement inattendues de l'utilisation des TI **Compétence**: la capacité de prendre de bonnes décisions/actions dans le cadre de la prise de responsabilité **Confiance**: la manière dont les membres de l'organisation prennent responsabilité doit inspirer confiance aux autres parties prenantes	Éthique

den Hamer et al. (2020), Gartner	#571	Digital Ethics	Être proactif dans la mise en place de principes éthiques, faire preuve d'une utilisation responsable des technologies (l'article interpelle les gestionnaires à faire preuve de prudence avec les technos comme l'IA et avec la manière dont l'entreprise utilise les données, ce qui peut potentiellement compromettre la sécurité de l'information)	Éthique
Huisman (2018a)	#566	Secure behavior Desired/undesired behavior	Ne pas cliquer sur un lien d'hameçonnage, ne pas utiliser de clé USB personnelle sur un poste de travail	Conformité
Noakes-Fry et Carpenter (2008), Gartner	#569	Security awareness	Connaître les risques pour l'entreprise liés aux systèmes et actifs TI, et savoir comment les protéger (connaissance des politiques et actions à poser); Avoir une intention d'appliquer les politiques de sécurité	Conformité
Reed et al. (2020), Gartner	#562	Security awareness	Développer une sensibilisation qui permet de prendre des décisions plus complexes que simplement "ne pas cliquer sur un lien" par exemple	Conformité Jugement (faible)

Annexe 6 – Relations entre les dimensions

Article	Code EndNote	Concept utilisé dans l'article	Dimension associée	Lien mentionné dans l'article avec d'autres dimensions
Burns et al. (2019)	#143	Protection motivated behaviors	Conformité Jugement (suggéré par l'idée d'adaptation dans les items)	Idée que les actions de conformité et celles d'adaptation font partie d'un spectre de rôles (appelé security behavioral repertoire) que l'employé doit avoir afin d'assurer la sécurité de l'information
Chen et al. (2019)	#23	Information security policy violation behavior	Conformité Éthique	Suggestion que l'éthique serait un antécédent de la conformité, car l'étude avance que c'est un manque de considération éthique qui mène à la violation des politiques de sécurité
Dang-Pham et al. (2017)	#260	Security knowledge sharing	Conformité Jugement (vaguement évoqué)	La partage de connaissances relèverait de motivations découlant de la conformité; mais aussi **idée** que les employés partagent leurs connaissances de leur propre gré, selon le contexte, s'ils évaluent que c'est pertinent à la situation…
Hadlington et al. (2021)	#268	Information security awareness behavior	Éthique Conformité	un désengagement moral mène à une sensibilisation plus faible. La sensibilisation mène à une conformité aux pratiques et politiques organisationnelles.
Herath et al. (2018)	#79	IS Security Policy Violation Likelihood	Conformité Éthique (faible)	Le désengagement moral favorise une violation des politiques; par contre une sensibilisation aux politiques réduit le risque de désengagement moral
Hong et Furnell (2021)	#162	Cybersecurity behavior	Conformité Jugement	Les items du questionnaire suggèrent que le comportement (et les développement d'habitudes comportementales) passe autant par la conformité que le jugement (le sujet du jugement n'est pas très élaboré dans l'étude, seulement suggéré par certains items)

Hsu et al. (2015)	#559	In-role behavior Extra-role behavior	Conformité Jugement	In-role et extra-role sont nécessaires ensemble pour assurer l'efficacité des programmes de sécurité. In-role s'apparente davantage à la conformité (mais aussi un peu jugement à cause de l'aspect adaptation). Extra-role s'apparente au jugement)
Rhee et al. (2009)	#579	Security practice behavior	Jugement Conformité	Le modèle de recherche indique que l'auto-efficacité (liée ici au jugement) est un antécédent du security practice behavior, qui est davantage associé à la conformité
Ruighaver et al. (2010)	#472	Ethical behavior	Éthique Jugement	L'étude suggère que les principes éthiques peuvent aider à développer davantage le jugement
Safa et al. (2015)	#189	Conscious care behavior	Jugement	Le conscious care behavior, qui est lié au jugement, se forme à partir d'éléments de conformité (SEF et politiques) et d'éléments du jugement (expériences antérieures)
Tsohou et Holtkamp (2018)	#36	Information security policy (ISP) Compliance	Conformité	L'étude suggère que la décision de se conformer (ou non) découle d'une évaluation d'une situation et de l'évaluation de la pertinence des actions en fonction de la situation. Possible lien entre jugement et conformité.
van Bavel et al. (2019)	#470	Online security behavior	Jugement	L'étude suggère que le jugement seul ne suffit pas toujours, qu'une composante de la conformité (ici une suggestion d'actions à entreprendre) permet de diminuer le risque de subir une cyberattaque
Van Slyke et Belanger (2020)	#249	Insider security behaviors	Jugement (idée d'un comportement qui va au-delà de la conformité)	L'article avance que la conformité ou la non-conformité ne sont pas les seules options qu'ont les employés, il existe d'autres moyens d'adopter un comportement sécuritaire.
Littérature professionnelle				
Buytendijk (2017), Gartner	#572	Digital ethics	Éthique	Idée que la conformité seule ne suffit pas: " Because ethics always precede laws and regulations, this is not a compliance issue, but requires taking a stand yourself." (p.6)

Buytendijk et al. (2020a), Gartner	#570	Digital ethics/care ethics	Éthique	Idée que la conformité ne suffit pas, il faut quelque chose qui va plus loin: "Information security and data privacy are topics that require you to go beyond treating them as regulatory compliance" (p.10)
Buytendijk et al. (2020b), Gartner	#575	Digital ethics	Éthique	La conformité est la base sur laquelle on peut développer des principes éthiques en ce qui concerne l'utilisation des technologies. La conformité aide à prévenir ce qui est "mal", mais l'éthique individuelle est ce qui permet de créer/innover ce qui est "bien"
den Hamer et al. (2020), Gartner	#571	Digital Ethics	Éthique	Accent sur le fait que la conformité seule est insuffisante, qu'il faut favoriser une sensibilisation à l'éthique de l'utilisation de la technologies chez les employés
Huisman (2018b)	#565	Employee secure behavior	Jugement (idée qui va au-delà de la conformité)	idée que les formations typiques en Infosec qui favorisent la conformité sont insuffisantes, avoir complété un formation ne permet pas en soi d'assurer que l'employé ne sera pas victime d'une attaque par rançongiciel par exemple. Idée qu'il faut guider les employés à participer et s'engager dans la sécurité à un degré plus élevé que la routine et la participation aux formation
Kim et al. (2020), Gartner	#576	Ethics and compliance management	Conformité Éthique	Idée que l'éthique et la conformité vont de pair. La conformité aux politiques organisationnelles n'est qu'un élément parmi d'autres de l'*ethics and compliance management*
Reed et al. (2020), Gartner	#562	Security awareness	Conformité Jugement (faible)	Idée que la conformité telle que souvent décrite ou apprise ne suffit pas. Par exemple, il faut que les employés apprennent à identifier ce qui peut constituer un courriel d'hameçonnage, pas seulement qu'il ne faut pas cliquer sur un lien.

Note : Certains article ne font part que d'une dimension clairement identifiable, mais la description qu'ils en donnent permet de comprendre qu'il y a une relation avec une autre dimension

Annexe 7 – Liste des articles composant l'échantillon final

Littérature académique
Cote 5
Albrechtsen, Eirik (2007). « A qualitative study of users' view on information security », *Computers & Security*, vol. 26, no 4, p. 276-289
Alohali, Manal, Nathan Clarke, Steven Furnell et Saad Albakri (2017). « Information security behavior: Recognizing the influencers », communication présentée au *2017 Computing Conference.*
Cavallari, Maurizio (2012). « A conceptual analysis about the organizational impact of compliance on information security policy », communication présentée au *Exploring Services Science.*
Crossler, Robert E., France Bélanger et Dustin Ormond (2019). « The quest for complete security: An empirical analysis of users' multi-layered protection from security threats », *Information Systems Frontiers*, vol. 21, no 2, p. 343-357.
Donalds, Charlette et Kweku-Muata Osei-Bryson (2020). « Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents », *International Journal of Information Management*, vol. 51, p. 1-16.
Fernández-Alemán, José Luis, Ana Sánchez-Henarejos, Ambrosio Toval, Ana Belén Sánchez-García, Isabel Hernández-Hernández et Luis Fernandez-Luque (2015). « Analysis of health professional security behaviors in a real clinical setting: An empirical study », *International Journal of Medical Informatics*, vol. 84, no 6, p. 454-467.
Herath, Tejaswini et H. R. Rao (2009). « Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness », *Decision Support Systems*, vol. 47, no 2, p. 154-165.
Hong, Yuxiang et Steven Furnell (2021). « Understanding cybersecurity behavioral habits: Insights from situational support », *Journal of Information Security and Applications*, vol. 57, p. 1-9.
Hsu, Jack Shih-Chieh, Sheng-Pao Shih, Yu Wen Hung et Paul Benjamin Lowry (2015). « The role of extra-role behaviors and social controls in information security policy effectiveness », *Information Systems Research*, vol. 26, no 2, p. 282-300.
Hwang, Inho, Daejin Kim, Taeha Kim et Sanghyun Kim (2017). « Why not comply with information security? An empirical approach for the causes of non-compliance », *Online Information Review*, vol. 41, no 1, p. 2-18.
Karjalainen, Mari, Mikko Siponen et Suprateek Sarker (2020). « Toward a stage theory of the development of employees' information security behavior », *Computers & Security*, vol. 93, p. 1-18.
Klein, Rodrigo Hickmann et Edimara Mezzomo Luciano (2016). « What influences information security behavior? A study with brazilian users », *Journal of Information Systems and Technology Management : JISTEM*, vol. 13, no 3, p. 479-496.
Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar et Xiaohong Yuan (2019). « Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior », *International Journal of Information Management*, vol. 45, p. 13-24.
Mamonov, Stanislav et Raquel Benbunan-Fich (2018). « The impact of information security threat awareness on privacy-protective behaviors », *Computers in Human Behavior*, vol. 83, p. 32-44.
Ng, Boon-Yuen, Atreyi Kankanhalli et Yunjie Xu (2009). « Studying users' computer security behavior: A health belief perspective », *Decision Support Systems*, vol. 46, no 4, p. 815-825.
Omidosu, Joseph et Jacques Ophoff (2016). « A theory-based review of information security behavior in the organization and home context », communication présentée au *2016 Third International Conference on Advances in Computing, Communication and Engineering.*
Rhee, Hyeun-Suk, Cheongtag Kim et Young U. Ryu (2009). « Self-efficacy in information security: Its influence on end users' information security practice behavior », *Computers & Security*, vol. 28, no 8, p. 816-826.

Ruighaver, A. B., S. B. Maynard et M. Warren (2010). « Ethical decision making: Improving the quality of acceptable use policies », *Computers & Security*, vol. 29, no 7, p. 731-736.
Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani et Tutut Herawan (2015). « Information security conscious care behaviour formation in organizations », *Computers & Security*, vol. 53, p. 65-78.
Safa, Nader Sohrabi, Rossouw Von Solms et Steven Furnell (2016). « Information security policy compliance model in organizations », *Computers & Security*, vol. 56, p. 70-82
Shropshire, Jordan, Merrill Warkentin et Shwadhin Sharma (2015). « Personality, attitudes, and intentions: Predicting initial adoption of information security behavior », *Computers & Security*, vol. 49, p. 177-191.
Takemura, Toshihiko (2011). « Statistical analysis on relation between workers' information security awareness and the behaviors in Japan », *Journal of Management Policy and Practice*, vol. 12, no 3, p. 27-36.
Warkentin, Merrill, Allen C. Johnston, Jordan Shropshire et William D. Barnett (2016). « Continuance of protective security behavior: A longitudinal study », *Decision Support Systems*, vol. 92, p. 25-35.
Yazdanmehr, Adel et Jingguo Wang (2016). « Employees' information security policy compliance: A norm activation perspective », *Decision Support Systems*, vol. 92, p. 36-46.
Zauwiyah, Ahmad, Ong Thian Song, Liew Tze Hui et Mariati Norhashim (2019). « Security monitoring and information security assurance behaviour among employees », *Information and Computer Security*, vol. 27, no 2, p. 165-188.
Cote 4+
Chowdhury, Noman H., Marc T. P. Adam et Timm Teubner (2020). « Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures », *Computers & Security*, vol. 97, p. 1-13.
Hadlington, Lee, Jens Binder et Natalia Stanulewicz (2021). « Exploring role of moral disengagement and counterproductive work behaviours in information security awareness », *Computers in Human Behavior*, vol. 114, p. 1-8.
Lankton, Nancy K., Charles Stivason et Anil Gurung (2019). « Information protection behaviors: Morality and organizational criticality », *Information and Computer Security*, vol. 27, no 3, p. 468-488.
van Bavel, René, Nuria Rodríguez-Priego, José Vila et Pam Briggs (2019). « Using protection motivation theory in the design of nudges to improve online security behavior », *International Journal of Human-Computer Studies*, vol. 123, p. 29-39.
Weems, Carl F., Irfan Ahmed, Golden G. Richard, Justin D. Russell et Erin L. Neill (2018). « Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behavior », *Plos One*, vol. 13, no 12.
Yan, Zheng, Thomas Robertson, River Yan, Sung Yong Park, Samantha Bordoff, Quan Chen*, et al.* (2018). « Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? », *Computers in Human Behavior*, vol. 84, p. 375-382.
Cote 4
Abraham, Sherly et InduShobha Chengalur-Smith (2019). « Evaluating the effectiveness of learner controlled information security training », *Computers & Security*, vol. 87, p. 1-12.
Barlow, Jordan B., Merrill Warkentin, Dustin Ormond et Alan R. Dennis (2018). « Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance », *Journal of the Association for Information Systems*, vol. 19, no 8, p. 689-715.
Bauer, Stefan, Edward W. N. Bernroider et Katharina Chudzikowski (2017). « Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks », *Computers & Security*, vol. 68, p. 145-159.
Boss, Scott R., Laurie J. Kirsch, Ingo Angermeier, Raymond A. Shingler et R. Wayne Boss (2009). « If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security », *European Journal of Information Systems*, vol. 18, no 2, p. 151-164.

Burns, A. J., Clay Posey et Tom L. Roberts (2019). « Insiders' adaptations to security-based demands in the workplace: An examination of security behavioral complexity », *Information Systems Frontiers*, p. 1-18.
Chen, Hao, Patrick Y. K. Chau et Wenli Li (2019). « The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior », *Information Technology & People*, vol. 32, no 4, p. 973-992.
Chowdhury, Noman H., Marc T. P. Adam et Geoffrey Skinner (2018). « The impact of time pressure on human cybersecurity behavior: An integrative framework », communication présentée au *2018 26th International Conference on Systems Engineering.*
Chu, Amanda M. Y. et Mike K. P. So (2020). « Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective », *Sustainability*, vol. 12, no 8.
Connolly, Lena Yuryna, Michael Lang, John Gathegi et Doug J. Tygar (2017). « Organisational culture, procedural countermeasures, and employee security behaviour », *Information and Computer Security*, vol. 25, no 2, p. 118-136.
Connolly, Lena Y., Michael Lang et David S. Wall (2019). « Information security behavior: A cross-cultural comparison of irish and us employees », *Information Systems Management*, vol. 36, no 4, p. 306-322
Da Veiga, A. et J. H. P. Eloff (2010). « A framework and assessment instrument for information security culture », *Computers & Security*, vol. 29, no 2, p. 196-207.
Dang-Pham, Duy, Siddhi Pittayachawan et Vince Bruno (2017). « Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace », *Computers in Human Behavior*, vol. 67, p. 196-206.
Dinev, Tamara et Qing Hu (2007). « The centrality of awareness in the formation of user behavioral intention toward protective information technologies * », *Journal of the Association for Information Systems*, vol. 8, no 7, p. 386-408.
Doherty, Neil F. et Sharul T. Tajuddin (2018). « Towards a user-centric theory of value-driven information security compliance », *Information Technology & People*, vol. 31, no 2, p. 348-367.
Feng, Gengzhong, Jiawen Zhu, Nengmin Wang et Huigang Liang (2019). « How paternalistic leadership influences it security policy compliance: The mediating role of the social bond », Journal of the Association for Information Systems, vol. 20, no 11, p. 1650-1691.
Furnell, Steven et Kerry-Lynn Thomson (2009). « From culture to disobedience: Recognising the varying user acceptance of it security », *Computer Fraud & Security*, vol. 2009, no 2, p. 5-10.
Herath, Tejaswini, Yim Myung-Seong, D'Arcy John, Kichan Nam et H. R. Rao (2018). « Examining employee security violations: Moral disengagement and its environmental influences », *Information Technology & People*, vol. 31, no 6, p. 1135-1162.
Herath, Tejaswini et H. Raghav Rao (2009). « Protection motivation and deterrence: A framework for security policy compliance in organisations », *European Journal of Information Systems*, vol. 18, no 2, p. 106-125.
Hwang, Inho et Oona Cha (2018). « Examining technostress creators and role stress as potential threats to employees' information security compliance », *Computers in Human Behavior*, vol. 81, p. 282-293.
Kajtazi, Miranda, Hasan Cavusoglu, Izak Benbasat et Darek Haftor (2018). « Escalation of commitment as an antecedent to noncompliance with information security policy », *Information and Computer Security*, vol. 26, no 2, p. 171-193.
Kearney, Wayne D. et Hennie A. Kruger (2016). « Theorising on risk homeostasis in the context of information security behaviour », *Information and Computer Security*, vol. 24, no 5, p. 496-513.
Khatib, Rima et Henri Barki (2020). « An activity theory approach to information security non-compliance », *Information and Computer Security*, vol. 28, no 4, p. 485-501.
Kim, Hyungjin Lukas et Jinyoung Han (2019). « Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective », *Information Technology & People*, vol. 32, no 4, p. 858-875.

Kim, Sang Soo et Yong Jin Kim (2017). « The effect of compliance knowledge and compliance support systems on information security compliance behavior », *Journal of Knowledge Management*, vol. 21, no 4, p. 986-1010.

Lin, Canchu et Jenell L. S. Wittmer (2017). « Proactive information security behavior and individual creativity: Effects of group culture and decentralized it governance », communication présentée au *2017 Ieee International Conference on Intelligence and Security Informatics*.

Öğütçü, Gizem, Özlem Müge Testik et Oumout Chouseinoglou (2016). « Analysis of personal information security behavior and awareness », *Computers & Security*, vol. 56, p. 83-93.

Parsons, Kathryn, Agata McCormac, Marcus Butavicius et Lael Ferguson (2010). *Human factors and information security: Individual, culture and security environment*, no DSTO-TR-2484, Australia, Command, Control, Communications and Intelligence Division Defence Science and Technology Organisation.

Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson et Cate Jerram (2014). « Determining employee awareness using the human aspects of information security questionnaire (hais-q) », *Computers & Security*, vol. 42, p. 165-176.

Siponen, Mikko, M. Adam Mahmood et Seppo Pahnila (2014). « Employees' adherence to information security policies: An exploratory field study », *Information & Management*, vol. 51, no 2, p. 217-224.

Sommestad, Teodor (2018). « Work-related groups and information security policy compliance », *Information and Computer Security*, vol. 26, no 5, p. 533-550.

Sommestad, Teodor, Jonas Hallberg, Kristoffer Lundholm et Johan Bengtsson (2014). « Variables influencing information security policy compliance: A systematic review of quantitative studies », *Information Management & Computer Security*, vol. 22, no 1, p. 42-75.

Sommestad, Teodor, Henrik Karlzen et Jonas Hallberg (2015). « A meta-analysis of studies on protection motivation theory and information security behaviour », *International Journal of Information Security and Privacy*, vol. 9, no 1, p. 26-46.

Sommestad, Teodor, Henrik Karlzén et Jonas Hallberg (2015). « The sufficiency of the theory of planned behavior for explaining information security policy compliance », *Information and Computer Security*, vol. 23, no 2, p. 200-217.

Topa, Ioanna et Maria Karyda (2019). « From theory to practice: Guidelines for enhancing information security management », *Information and Computer Security*, vol. 27, no 3, p. 326-342.

Tsohou, Aggeliki et Philipp Holtkamp (2018). « Are users competent to comply with information security policies? An analysis of professional competence models », *Information Technology & People*, vol. 31, no 5, p. 1047-1068.

Van Slyke, Craig et France Belanger (2020). « Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective », *Computers & Security*, vol. 99, p. 1-16.

Vedadi, Ali et Merrill Warkentin (2020). « Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions », *Journal of the Association for Information Systems*, vol. 21, no 2, p. 428-459.

Wall, Jeffrey D., Prashant Palvia et Paul Benjamin Lowry (2013). « Control-related motivations and information security policy compliance: The role of autonomy and efficacy », *Journal of Information Privacy & Security*, vol. 9, no 4, p. 52-79.

Williams, Clay K., Donald Wynn, Ramana Madupalli, Elena Karahanna et Barbara K. Duncan (2014). « Explaining users' security behaviors with the security belief model », *Journal of Organizational and End User Computing*, vol. 26, no 3, p. 23-46.

Littérature professionnelle

Buytendijk, Frank (2017). *Digital ethics, or how to not mess up with technology*, Gartner.

Buytendijk, Frank, Jim Hare et Lydia Clougherty-Jones (2020). *Digital ethics by design: A framework for better digital business*, Gartner.

Buytendijk, Frank, Brian Lee et Chris Howard (2020). *Digital ethics: What every executive leader should know*, Gartner.

den Hamer, Pieter, Katie Gove, Bart Willemsen, Christie Struckman et Frank Buytendijk (2020). *Digital ethics: From compliance duty to competitive differentiator*, Gartner.
Huisman, Joanna (2018). *Rewards and consequences motivate employee secure behaviors*, Gartner.
Huisman, Joanna (2018). *Effective security awareness starts with defined objectives*, Gartner.
Kim, Elizabeth, Jie Zhang et Jim Murphy (2020). *Market guide for ethics and compliance management solutions*, Gartner.
Noakes-Fry, Kristen et Perry Carpenter (2008). *Training is critical for building a security-aware workforce*.
Reed, Brian, Richard Addiscott et Claude Mandy (2020). *Market guide for security awareness computer-based training*, Gartner.
Sampath, Srinath (2019). *Fight unsecure employee behaviors by fixing your risk culture*, Gartner.
Scholtz, Tom, Matt Cain et Andrew Walls (2015). *Prepare for the security implications of the digital workplace*, Gartner.
Walls, Andrew (2013). *Short, focused and just-in-time approaches to security awareness*, Gartner.
Walls, Andrew (2014). *User behavior can improve security, but only with development and practice*, Gartner.