HEC Montréal

Impacts de l'adoption forcée du télétravail sur la sécurité informationnelle en organisation

Par
Igor Novikov

Sciences de la gestion
Intelligence d'Affaires

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

Avril 2023

HEC MONTRÉAL

Comité d'éthique de la recherche

CERTIFICAT D'APPROBATION ÉTHIQUE

La présente atteste que le projet de recherche décrit ci-dessous a fait l'objet d'une évaluation en matière d'éthique de la recherche avec des êtres humains et qu'il satisfait aux exigences de notre politique en cette matière.

Projet # : 2023-5074

Titre du projet de recherche : Comment et pourquoi la transition vers le télétravail impacte-t-elle le niveau de la sécurité informationnelle?

Chercheur principal :
Igor Novikov,

Directeur/codirecteurs :
Bogdan Negoita
Professeur - HEC Montréal

Date d'approbation du projet : 05 octobre 2022

Date d'entrée en vigueur du certificat : 05 octobre 2022

Date d'échéance du certificat : 01 octobre 2023

Maurice Lemelin
Président
CER de HEC Montréal

Signé le 2022-10-12 à 14:40

TABLE DES MATIÈRES

TABLE DES TABLEAUX

TABLE DES FIGURES

1. Introduction

1.1. Présentation contextuelle

Depuis mars 2020, une crainte incessante de quarantaines répétées caractérise la pandémie du virus SARS-CoV-2 et amène d'importantes réformes dans plusieurs strates de la société. Pourtant, en comparaison à ses prédécesseurs, le nouveau virus est respectivement 4,36 et 15,46 fois moins dangereux que le SARS-CoV et le MERS-CoV (Velavan et Meyer, 2020). Alors, pourquoi le considère-t-on comme étant plus menaçant que les autres ? En réalité, c'est le contexte de transmission et le haut taux de reproduction (TR) du SARS-CoV-2 qui représentent un risque pour la société. Le TR du virus, soit le nombre moyen de cas générés par un cas d'infection, se situe entre 1,5 et 3,5, pour le variant de Wuhan (Caspi *et al.*, 2020), et deux fois plus, pour le variant *Delta*. L'importante variation de cet intervalle est due aux éléments contextuels de l'environnement de propagation, à savoir les habitudes culturelles, la densité de population et les stratégies adoptées par les gouvernements, telles que la quarantaine, les fermetures de frontières ainsi que le télétravail (Caspi *et al.*, 2020).

Le **télétravail** est « *un arrangement de travail dans lequel un employé effectue au moins une partie de ses responsabilités professionnelles à domicile ou dans un autre lieu que son bureau habituel* » (Beasley et Lomo-David, 2000). Les études préalables indiquent l'aspect volontaire de cet arrangement et sont fondées sur une classe plus notable de travailleurs, soit ceux dont le revenu annuel moyen s'élève au-delà de 65 000 $ US (Desilver, 2020). La pandémie a forcé cette adoption si brusquement, que les organisations n'ont pas disposé du temps nécessaire pour introduire des mesures assurant le bien-être des employés (Wang *et al.*, 2021). Bien qu'il soit vrai que cette méthode présente de nombreux avantages, comme la diminution du temps de déplacement et la possibilité de remplir des tâches domestiques (Anderson et Kelliher, 2020), nous ne devons pas sous-estimer les aspects négatifs qui y sont associés. Les études suggèrent que cette méthode consoliderait les rôles de genre traditionnels (Chung et Van der Lippe, 2020), augmenterait l'isolement social, affecterait le partage de connaissance et donnerait un sentiment de « *deuxième quart* » qui couvre les tâches ménagères et la gestion des enfants (Hochschild et Machung, 1989). Sans communication et collaboration, la détérioration de l'environnement de travail doit être

mitigée par l'adoption de différents outils technologiques, comme *Teams*, *Outlook* et *Slack* (Anderson *et al.*, 2020). Une course au numérique est alors entamée, comme le démontrent les nombreuses statistiques, avec une croissance de l'utilisation de l'Internet, passant de 40 % à 100 % en mars et avril 2020 (Pandey et Pal, 2020). Étant isolé à domicile, l'unique moyen de communication et de travail disponible aux individus était l'Internet. Cette réalité à inciter les organisations à adopter le télétravail et à accroître leurs infrastructure et réseau intégrés (Vargo *et al.*, 2021). Pour satisfaire cette demande, des nouveautés technologiques ont été déployées, ce qui a engendré une restructuration des systèmes informatiques et une révision des procédés usuels en sécurité informationnelle (Pandey *et al.*, 2020).

La sécurité informationnelle est « *un sous-ensemble de la cybersécurité, qui est conçue pour maintenir la confidentialité, l'intégrité et la disponibilité des données* » (Seemma, Nandhini et Sowmiya, 2018). C'est un processus qui assure le respect des dimensions de sécurité et qui contribue à la politique de gouvernance des données. C'est une interaction entre les comportements, les composantes et la culture de sécurité informationnelle qui caractérisent une organisation (Da Veiga et Eloff, 2010). La numérisation organisationnelle a concédé des enjeux significatifs à cet égard compte tenu des vulnérabilités admises par les nouveautés technologiques, adoptées en 2020. Cette numérisation alloue certainement des bénéfices, comme une rapidité d'exécution et une efficience améliorée, mais pour être sécuritaire, elle nécessite un savoir-faire et un budget considérable — des éléments souvent négligés en organisation. En effet, les ressources dédiées à la sécurité informationnelle sont souvent insuffisantes alors que les systèmes informatiques sont désuets, les budgets sont limités et près de 40 % des cadres stratégiques ne sont pas formés sur les enjeux de sécurité des données (Sweeney, 2016). Pour stimuler la numérisation, les dirigeants attribuent, en moyenne, 95 % du budget TI à l'introduction de nouvelles technologies, en comparaison à moins de 3 %, à l'entretien et à la sécurité (Kruse *et al.*, 2017). Il en résulte que, depuis mars 2020, le nombre d'hameçonnages en ligne (*phishing attacks*) a augmenté de 6 fois et le nombre de cybermenaces, de 300 fois, ce qui démontre une négligence organisationnelle au niveau de la sécurité des données (Kruse *et al.*, 2017).

1.2. Question de recherche et justification de l'étude

Étant une méthode d'organisation du travail peu étudiée en contexte d'adoption forcée, le télétravail nécessite aujourd'hui une attention particulière. Son incidence sur la sécurité des données constitue l'axe de recherche central de ce mémoire. Ainsi, considérant les réalités organisationnelles énumérées précédemment, tels le sous-financement de l'infrastructure informatique et la valeur élevée des informations entreposées, les résultats présentés dans les chapitres suivants contribuent à la littérature académique existante par une formulation d'une conséquence et de deux mécanismes inconsidérés préalablement. L'environnement extraordinaire, qui démocratise le télétravail par son adoption forcée, procure un bassin de télétravailleurs et produit une opportunité exceptionnelle pour répondre à la question de recherche suivante : **comment ET pourquoi l'adoption forcée du télétravail impacte-t-elle la sécurité informationnelle en organisation ?** Une revue de littérature, appuyée par une étude qualitative, nous permet d'évaluer les pratiques introduites en période d'adoption forcée du télétravail et leur incidence respective sur la sécurité des données.

1.3. Objectifs et contributions potentielles de l'étude

Cette étude cible une compréhension de « *comment ?* » et « *pourquoi ?* » l'adoption forcée du télétravail détient une incidence sur la sécurité informationnelle (Whetten, 1989). Pour répondre au « *pourquoi ?* », nous avons pour but de définir les facteurs explicatifs de cette incidence grâce à l'induction analytique. Pour répondre au « *comment ?* », nous avons pour but d'explorer les concepts théoriques, tel le *misfit* au télétravail, les tensions résultantes, les mécanismes de gestion et les conséquences grâce à une analyse thématique. Cette étude nous permettra de compléter le modèle conceptuel initial, issu de la revue de littérature, grâce aux réponses des participants.

La contribution de ce mémoire réside dans l'élaboration d'un modèle conceptuel qui établit l'impact de l'adoption forcée du télétravail sur la sécurité informationnelle en organisation. Le modèle est formulé grâce à l'étude d'une population hétérogène de télétravailleurs dans un environnement peu documenté préalablement. Cette hétérogénéité instaure un contexte d'exploration opportun permettant de satisfaire les objectifs énumérés précédemment et de développer des axes de recherche pour les études futures. Le mémoire complète également

la littérature existante en ajoutant deux mécanismes de gestion, l'adaptation individuelle au niveau individuel et la culture de sécurité informationnelle au niveau du groupe et une seule conséquence, au niveau organisationnel, à savoir la divergence des intérêts. Nous illustrons aussi les relations interconceptuelles qui n'étaient pas formulées préalablement, telles que la rétroactivité des conséquences et leur interdépendance.

1.4. Structure du mémoire

Ce mémoire est composé de six chapitres : l'introduction, la méthodologie, la présentation des résultats, la discussion des résultats et la conclusion. La revue de littérature, construite entièrement sur les fondements des études préalables, constitue une élaboration des thèmes de *télétravail*, de *sécurité informationnelle* et des *risques de sécurité informationnelle*. Ces thèmes sont développés séparément, mais couplés ensuite lors de l'élaboration du modèle conceptuel initial, qui sert également à la construction du guide d'entrevue, présenté à l'annexe 10. Le chapitre suivant, soit la méthodologie, définit les méthodes de collecte et d'analyse des données. Nous y justifions la sélection d'une conception d'étude en démontrant les principes de l'induction analytique et de l'analyse thématique de données qualitatives. Nous y décrivons les activités de sollicitation pour illustrer le respect des normes éthiques et valider les résultats de notre étude. Nous y formulons également les étapes de déroulement des entrevues semi-structurées et définissons les notions d'encodage utilisées pour le traitement de données qualitatives collectées (*open coding*, *axial coding* et *selective coding*). Les résultats des analyses sont communiqués au quatrième chapitre de ce mémoire, soit la présentation des résultats. Les éléments recensés dans ce chapitre sont décrits, sans contextualisations, alors que l'objectif est plutôt de compléter notre modèle conceptuel initial avec les réponses des participants. Cette partie est sectionnée par concept issu de la revue de littérature, où chaque section illustre une perspective détaillée par niveau d'étude. Les citations des participants sont directement insérées dans ce chapitre. Au terme de ce dernier, un modèle conceptuel amélioré est développé par l'intégration des éléments d'amélioration au modèle conceptuel initial. Ces éléments sont ensuite associés aux notions théoriques, présentées précédemment, dans la discussion des résultats. Le dernier chapitre de ce mémoire, soit la conclusion, illustre les contributions de l'étude, formule les limites de notre méthodologie et suggère des axes de recherche pour les études futures.

2. Revue de littérature

Une revue de littérature intégrant les concepts de *télétravail*, de *sécurité informationnelle* et des *risques de sécurité informationnelle* en organisation est nécessaire à l'établissement d'un modèle conceptuel initial. Ce chapitre formule donc une définition de ces concepts et établit les relations interconceptuelles qui les définissent. Il érige aussi une compréhension explicite des thèmes soulevés, ce qui permet ultimement de concevoir un protocole d'étude efficace et de situer nos résultats dans un domaine académique existant.

2.1. Le télétravail

Depuis plusieurs décennies, les études relatives au télétravail sont caractérisées par des résultats divergents, ce qui engendre un sujet dilemmatique (Noble, 2007). Initialement, le télétravail n'était pas acclamé des organisations en raison de l'inégalité des coûts et des bénéfices découlant de la recherche à son égard (Noble, 2007). Néanmoins, en contexte de crise pétrolière des années 70, il capte progressivement de l'intérêt à titre de solution pour réduire les coûts de déplacements professionnels. Les organisations réservent alors ce privilège à une classe plus notable de travailleurs, composée principalement d'employés au salaire annuel moyen au-delà de 65 000 $ US (Desilver, 2020). La forme démocratique du télétravail apparaît uniquement en 2020, en réponse aux confinements obligatoires, alors que près de 557 millions d'individus, soit 20 % de la population active mondiale, exercent leur profession depuis leur domicile (Berg, Humblet et Soares, 2021). La démocratisation de l'adoption du télétravail, par son imposition, accorde une nouvelle opportunité d'étude, minimisant les biais de sélection et les limites associées à une classe non représentative de télétravailleurs

2.1.1. Qu'est-ce que le télétravail ?

Le **Tableau 1** présente quelques définitions conférées aux termes utilisés, pour définir le télétravail, à travers les études préalables. En anglais, le terme *telecommuting* est employé pour la première fois en 1972, par Jack Nilles, ingénieur de la NASA, alors qu'il travaillait sur un système de communication complexe (Ellison, 1999). Dès le commencement de son projet, Nilles contemple l'éventuelle application de son système en vertu d'une modalité de travail à distance et en perçoit les bénéfices potentiels. Depuis, une multitude de

définitions ont été émises avec une claire divergence sur des aspects centraux, comme l'emplacement physique, l'utilité des TIC et la définition d'un télétravailleur.

Tableau 1 Définitions conceptuelles du télétravail

Auteur(s)	Numéro de page	Terme(s) utilisé(s)	Définition	Aspect(s) mentionné(s)
(Nilles, 1988)	p.301	*Telecommunting*	« *Une forme de substitution (partielle ou totale) des déplacements professionnels traditionnels par l'utilisation des TI.* »	Utilisation des technologies de l'information et de communication
(Hill, 1995)	p.3-4	*Mobile telework*	« *Travail effectué en dehors du bureau conventionnel grâce à l'utilisation des outils de télécommunication.* »	Utilisation des outils de télécommunication/ Emplacement physique externe au bureau
(Beasley *et al.*, 2000)	p.113	*Telework*	« *Un mode de travail alternatif qui prend place soit à domicile, soit à un emplacement satellite grâce à l'utilisation de l'informatique et des outils de télécommunication.* »	Utilisation des outils de télécommunication/ Emplacement physique externe au bureau
(Di Martino et Wirth, 1990)	p.530	*Telework*	« *Modalité de travail flexible où les employés travaillent d'un endroit éloigné de leurs bureaux, et entretiennent un contact avec leurs collègues par l'utilisation des TIC.* »	Utilisation des outils de télécommunication/ Emplacement physique externe au bureau
(Vivadelli, 2005)	p.22	*Telework*	« *Une disposition qui utilise la technologie pour permettre aux télétravailleurs d'être aussi productifs en dehors du bureau que lorsqu'ils travaillent en milieu de travail conventionnel.* »	Utilisation des outils de télécommunication/ Emplacement physique externe au bureau
(Wontorczyk et Rożnowski, 2022)	p.2	*Telework*	« *Méthode d'organisation et d'exécution du travail par laquelle l'employé travaille en dehors du bureau pendant une partie importante de son temps, fournissant à l'employeur des résultats de travail en utilisant les technologies de l'information et les technologies de transfert de données, en particulier Internet.*»	Utilisation des outils de télécommunication/ Emplacement physique externe au bureau

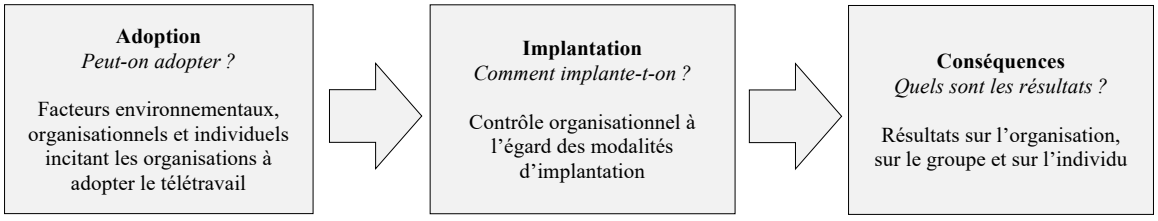
Pour mieux adapter la définition du télétravail à notre question de recherche centrale, qui est axée sur l'adoption forcée, nous percevons une nécessité de combler certains manques par une reformulation des propositions du **Tableau 1**. Dans un contexte d'adoption forcée, nous devons mentionner que les télétravailleurs sont contraints à travailler à domicile en raison des circonstances extraordinaires, telles qu'une situation de crise, plutôt que par choix personnel. Le **télétravail** est donc un arrangement d'organisation du travail, mesurée

en heures, complétées strictement à domicile, grâce à des technologies d'information et de communication. Dans une logique similaire, le **télétravailleur** est un individu, employé à l'interne, qui opère strictement à son domicile et qui, grâce aux technologies d'information et de communication, est en état de compléter ses obligations professionnelles.

2.1.2. Antécédents du télétravail

Cette section développe une analyse des cadres et des antécédents académiques relatifs au concept de télétravail, formulés dans les études préalables. Comme soulevé précédemment, ces études sont généralement caractérisées par des résultats divergents, produisant un sujet dilemmatique (Noble, 2007). Une compréhension explicite de ces antécédents permet donc de comprendre ces divergences et de verbaliser les tendances académiques du domaine. On dénote trois tendances, à savoir l'adoption, l'implantation et l'évaluation des conséquences du télétravail [Figure 1 ; Annexe 1] (Errichiello et Pianese, 2016). Elles détiennent toutes une incidence sur la sécurité informationnelle tel qu'illustré dans les chapitres subséquents.

Figure 1 Modèle conceptuel du télétravail de Errichiello et Pianese (2016)



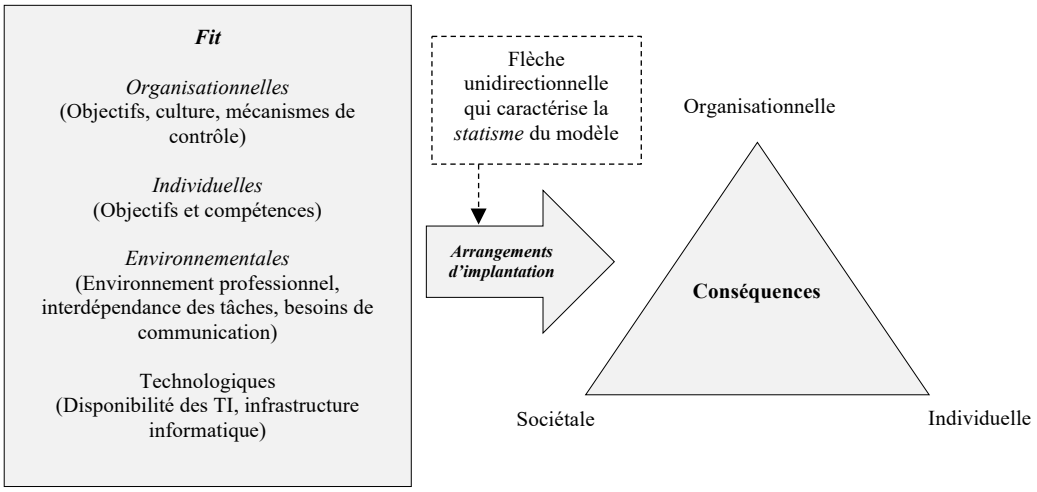
Les études relatives à l'**adoption** du télétravail sont modelées sur les fondements des études de l'adoption technologique dans les organisations (Beaudry et Pinsonneault, 2005; Davis, 1989; Venkatesh *et al.*, 2003). Ces fondements énoncent que l'adoption technologique dans les environnements organisationnels découlent des facteurs perceptifs des utilisateurs quant à l'utilité et à la facilité d'utilisation d'une technologie donnée (Davis, 1989). Pour certains, deux facteurs perceptifs sont suffisants pour expliquer la théorie d'adoption alors que pour d'autres, il est nécessaire de compléter ces facteurs de stratégies d'adaptation individuelle (Beaudry *et al.*, 2005) ou même de facteurs perceptifs supplémentaires, comme l'influence sociale et les conditions contextuelles (Venkatesh *et al.*, 2003). Toutefois, tous ces facteurs soulèvent l'importance de concevoir des technologies qui sont compatibles (*fit*) aux besoins et aux compétences des individus pour favoriser leur adoption en organisation. En adoption

forcée du télétravail, le concept de *fit* est particulièrement pertinent en raison du volet forcé qui caractérise l'environnement des télétravailleurs. Dans un tel contexte, le *fit* correspond à l'adéquation perçue entre les exigences professionnelles en télétravail et les compétences des télétravailleurs. Il est mesuré sur trois niveaux d'études, soit l'individu, par les facteurs de motivation intrinsèque, le groupe, par les facteurs de synergie d'équipe et l'organisation, par l'attitude des dirigeants. Au niveau individuel, le *fit* au télétravail découle des attitudes, du contexte, des perceptions et des préférences des individus relativement leur mode de vie [Annexe 2] (Mokhtarian et Salomon, 1993). Un individu productif dans un environnement calme et isolé est peut-être mieux compatible (*fit*) au télétravail, qu'un individu facilement distrait et agité (Wang *et al.*, 2021). Au niveau du groupe, le *fit* est plutôt stimulé par des facteurs, comme l'opportunité de croissance, la flexibilité et surtout, la synergie [Annexe 3] (Peters, Tijdens et Wetzels, 2004). Sans synergie, les télétravailleurs peuvent quelques fois ressentir l'isolement, ce qui engendre une incidence négative sur leur *fit* au télétravail. Au niveau organisationnel, par ailleurs, le *fit* est évalué par un questionnement à deux niveaux : (1) « *le télétravail, est-il efficace ?* » et (2) « *quelles sont les conséquences prévisibles de son implantation en organisation ?* » (Gajendran et Harrison, 2007). Les organisations sont pressées de comprendre comment cette adoption influence les facteurs de performance, tels que la productivité, la satisfaction des employés, la santé psychologique et le taux de roulement [Annexe 4] (Gajendran *et al.*, 2007). Sans compréhension, une adoption hâtive du télétravail produit une resistance au changment et instaure un *misfit* organisationnel. Le *misfit* correspond à une situation où un individu, un groupe ou une organisation adopte une technologie qui n'est pas *fit* à ses compétences, ses besoins ou ses préférences (Mokhtarian *et al.*, 1993). Ce phénomène est particulièrement probable en contexte d'adoption forcée du télétravail, où un individu, un groupe ou une organisation sont forcés à travailler à distance, nonobstant les facteurs de prédisposition ou d'indisposition qui les caractérisent.

Les études relatives à l'**implantation** du télétravail soulèvent donc la nécessité d'introduire des modalités adaptées aux réalités des trois niveaux d'étude, afin de réduire le *misfit*. Elle résulte d'une conjonction entre l'adoption organisationnelle et l'infusion technologique, soit un procédé d'intégration d'une technologie dans un environnement de travail existant, ce qui implique la révision de la structure organisationnelle, la modification des processus et la formation des individus pour s'adapter à une nouveauté technologique (Cooper et

Zmud, 1990). La réussite de ce processus dépend essentiellement des facteurs de prédisposition, qui ont été énumérés précédemment, et de l'effort d'infusion déployé par une organisation (Cooper *et al.*, 1990). Pour qu'une implantation ait des retombées positives, nous devons considérer les exigences organisationnelles, ainsi que les compétences et les attitudes des télétravailleurs. Un premier modèle, produisant une conception statique de l'implantation du télétravail, illustre ce processus par une incidence du *fit* technologique, organisationnel, environnemental et individuel à l'égard des conséquences individuelles, organisationnelles et sociétales [Figure 2] (Collins, 1998). Une implantation statique insinue que les modalités d'implantation initiale resteront inchangées pendant tout le processus. Au niveau sociétal, par exemple, le *fit* au télétravail des individus mène à une vaste adoption dans une société et subséquemment à une baisse des déplacements professionnels et des émissions de gaz à effet de serre. Au niveau individuel, le *fit* technologique produit des modalités d'organisation qui réduisent les effets de l'interférence du télétravail dans la vie des télétravailleurs, mais qui, conformément au concept de statisme, ne peuvent pas être changées respectivement aux conséquences d'implantation préalables. C'est ce statisme qui est souvent critiqué, alors qu'une société, une organisation ou un individu, dont les conséquences d'implantation sont insatisfaisantes, repositionnera les arrangements adoptés précédemment (Collins, 1998).

Figure 2 Modèle d'implantation du télétravail de Collins (1998)



Un second modèle, adoptant une conception dynamique d'implantation du télétravail, vient alors remédier à ce statisme, en élaborant une conceptualisation qui intègre la rétroactivité

des conséquences [Annexe 5] (Bélanger, Watson-Manheim et Swan, 2013). Ce modèle est composé de trois niveaux d'étude, soit l'individu, le groupe et l'organisation, contrairement aux trois niveaux, illustrés en **Figure 2** (individu, organisation et société). Une rétroactivité, en contexte d'implantation organisationnelle du télétravail, considère ce processus comme étant en interaction avec son environnement immédiat. Cette interaction constante alloue une rétroaction des conséquences, ce qui favorise une adaptation rapide aux changements de l'environnement des niveaux d'étude concernés (Bélanger *et al.*, 2013). Pour l'individu, cette interaction permet à un télétravailleur d'altérer ses habitudes de travail (*arrangement d'implantation*) pour mieux s'adapter aux défis de son environnement. Pour le groupe, elle permet aux membres d'une équipe d'altérer la façon de collaborer à distance (*arrangement d'implantation*) pour améliorer la synergie de groupe. Pour l'organisation, une rétroactivité des conséquences permet d'ajuster les normes de sécurité informationnelle (*arrangement d'implantation*) pour répondre aux enjeux de cybersécurité, associés à une décentralisation de la main-d'œuvre. Ce dynamisme octroie aux niveaux d'études une possibilité d'adaptation, ce qui est particulièrement pertinent en adoption forcée du télétravail.

2.1.3. Conséquences de l'adoption forcée du télétravail

L'étape d'évaluation des **conséquences** correspond à l'étude des résultats de l'implantation organisationnelle sur les trois niveaux d'étude concernés. Avant l'introduction généralisée de l'Internet, les individus étaient sceptiques à l'égard l'efficacité du télétravail pour des raisons relatives aux défis qui y sont associés. Cette section explore ces défis.

2.1.3.1. Conséquences de l'adoption forcée du télétravail sur l'organisation

L'implantation organisationnelle du télétravail mène à une baisse de la qualité des relations professionnelles, alors qu'un employé sur cinq n'aurait jamais rencontré son gestionnaire immédiat (Lojeski et Reilly, 2008). Cet affaiblissement produit une baisse de collaboration dans les équipes de travail, une démotivation associée à un climat défavorable et une baisse du contrôle exercé par l'organisation (Bélanger *et al.*, 2013). Les organisations témoignent alors d'un manque de support social[1], ce qui augmente l'isolement des individus et impacte

[1] Le *manque de support social* réfère au soutien émotionnel admis dans une organisation.

négativement leur sentiment d'appartenance (Bavik, Shaw et Wang, 2020). Combinés, ces effets stimulent l'individualisme et produisent un impact sur la performance, par une baisse de productivité et un affaiblissement de la sécurité informationnelle. Le contrôle est réduit et les télétravailleurs, qui témoignent d'un *misfit* au télétravail, sont davantage prônes à des comportements qui ne favorisent pas les intérêts organisationnels. Par exemple, en situation d'augmentation de la charge de travail, certains individus, étant plus disciplinés, réagiront de façon positive, alors que d'autres adopteront des comportements procrastinateurs, qui engendreront une réduction de la motivation professionnelle (Grant-Vallone et Donaldson, 2001). En adoption forcée du télétravail, les charges élevées sont banalisées, ce qui mène généralement à un phénomène d'anxiété, nommé « *technostress* », dont les caractéristiques comprennent une augmentation du rythme de travail, des interruptions constantes, du « *multitasking* » et une diminution de la productivité à long terme (Molino *et al.*, 2020). Le *technostress* est généralement associé à l'hyperconnectivité en télétravail, qui résulte d'une numérisation des outils de travail. Bien qu'elle engendre des conséquences négatives, cette numérisation contribue à l'amélioration de l'efficience organisationnelle par l'introduction de meilleures pratiques en matière de formation des télétravailleurs. Les formations virtuelles réaffectent la responsabilité d'apprentissage de l'employeur vers l'employé, fortifiant ainsi l'efficacité des programmes de formation. Elles offrent également des ressources et des outils interactifs, qui incitent l'autoapprentissage et automatisent le partage du savoir-faire sur des éléments d'importance organisationnelle, comme la sécurité des données. Les outils de travail numériques contribuent également à une hausse de l'efficience organisationnelle par une diminution des dépenses, à mesure de 2000 $ US à 10 000 $ US annuellement par télétravailleur (Pemble, 2020). Ils permettent aux organisations de réaliser des économies significatives au niveau des coûts des déplacements professionnels, des coûts de maintien de l'infrastructure immobilière et des coûts relatifs au matériel de bureau.

Considérant ces nombreuses conséquences, que pouvons-nous donc dire de la performance globale des organisations en télétravail ? Les résultats d'une étude chinoise, menée auprès d'un département de service à la clientèle, démontrent une impressionnante augmentation de 13 % du volume d'appels traités, lorsque les employés sont contraints au télétravail de façon obligatoire (*adoption forcée*), et de 22 %, lorsque le télétravail est offert sur une base

volontaire (*adoption volontaire*) (Pemble, 2020). Cette variation émane de deux éléments : une sélection optimale des travailleurs en fonction du *fit* au télétravail, permettant d'exclure les travailleurs moins productifs, et d'une liberté qui caractérise la gestion de ces individus. En télétravail, la gestion est souvent orientée vers l'adoption d'une approche fondée sur le rendement professionnel, et par conséquent sur une flexibilité d'emploi, au détriment d'une approche fondée sur le contrôle. À cet égard, nous recensons deux approches managériales, à savoir l'**approche transactionnelle** et l'**approche transformationnelle**. L'approche transactionnelle réfère à une gestion axée sur les bénéfices mutuels tirés par un gestionnaire et par ses subordonnés dans un contexte d'échanges impliquant une compensation pour la réalisation d'objectifs professionnelle. L'approche transformationnelle, en revanche, réfère à une gestion fondée sur le développement des employés, qui cherche à atteindre leur bien-être au travail, d'où la formulation ***transformationnelle*** (Nanjundeswaraswamy et Swamy, 2014). Bien qu'il semble clair que les organisations en télétravail devraient miser sur une approche transformationnelle, par une communication motivante (Madlock, 2013) et par une communication transparente (Lautsch, Kossek et Eaton, 2009), les tendances indiquent que les gestionnaires préfèrent pour l'approche transactionnelle (Abidoye, 2021).

2.1.3.2. Conséquences de l'adoption forcée du télétravail sur le groupe

Considérant la collaboration comme facteur déterminant de la productivité dans un groupe, plusieurs études évaluent l'incidence de la distance sur la collaboration au travail. D'après une étude réalisée à cet effet, la probabilité de collaboration entre individus est inversement corrélée à la distance qui les sépare (Lojeski *et al.*, 2008). Ce lien de corrélation inverse est valide jusqu'à une distance maximale de trente mètres (Lojeski *et al.*, 2008). Au-delà de ce seuil, la distance incrémentale n'a aucune incidence sur la probabilité de collaboration alors que celle-ci est véritablement égale à zéro. Certes, les avancements technologiques et l'âge considérable de l'étude constituent deux arguments valables pour réfuter la pertinence de ces propos. Cependant, aucun de ces avancements n'est réellement en état de reproduire une contextualisation équivalente à une communication en face à face (Watson-Manheim et Bélanger, 2007). L'inexécution des tâches au travail, le manque d'attention, la diminution du partage informationnel et le déclin de la qualité des interactions sociales alimentent tous la complexité de la collaboration à distance. Cela dit, le redressement de

cette collaboration débute essentiellement par un contrôle de deux composantes de la distance, soit la **distance physique** et la **distance psychologique** (Lojeski *et al.*, 2008). La distance physique réfère à la distance géographique qui sépare les membres d'un même groupe, alors que la distance psychologique réfère plutôt à la perception des individus par rapport à cette distance. « *Plus grande est la distance psychologique entre les membres d'une équipe, plus importants seront les problèmes expérimentés par celle-ci* » (Lojeski *et al.*, 2008). Puisqu'en adoption forcée du télétravail, une réduction de la distance physique n'est pas une solution possible, les organisations doivent diminuer la distance psychologique en développant un sentiment de communauté virtuelle (Yakovleva, Reilly et Werko, 2010). C'est la contextualisation de l'information véhiculée, au cours des rencontres formelles et informelles, qui permettra aux membres d'un groupe de développer ce sentiment. En partageant informellement avec leurs collègues, les individus admettent une ouverture affective et tissent les liens nécessaires à l'efficacité d'un travail en groupe. « *Un problème courant avec les équipes en télétravail réside du fait que les conversations mettent plus l'accent sur la logistique et les exigences professionnelles au détriment du développement des relations individuelles* » (Watson-Manheim *et al.*, 2007).

2.1.3.3. Conséquences de l'adoption forcée du télétravail sur l'individu

L'implantation organisationnelle du télétravail mène à deux défis principaux, au niveau de l'individu, soit l'*interférence du télétravail* et la *diminution de la qualité des relations individuelles*. Les responsabilités domestiques des télétravailleurs sont des distractions aux obligations professionnelles, qui briment leur productivité au travail. L'interférence du télétravail renforce alors le sentiment d'exténuation des télétravailleurs et mène parfois à l'épuisement professionnel (Wang *et al.*, 2021). L'impact engendré par cette interférence contient une notion d'iniquité en fonction des facteurs sociodémographiques, comme le sexe, la parenté et l'occupation professionnelle. Par exemple, le temps consacré aux tâches ménagères par une femme mariée correspond généralement au double du temps consacré par son conjoint (Bianchi *et al.*, 2012), ce qui forme une source d'interférence et d'iniquité. Lors du premier confinement, en printemps 2020, quand les écoles et les garderies étaient closes, des millions de femmes ont réagencé leur programmation quotidienne, allant même jusqu'à travailler la nuit, afin d'accommoder les attentes soulevées par leur organisation

(Manzo et Minello, 2020). De cette interférence suit inévitablement une *diminution de la qualité des relations individuelles*, qui est augmentée par une communication ineffective. Cette inefficience engendre un coût temporel réel dans l'accomplissement des tâches des télétravailleurs (Wang *et al.*, 2021), alors que les distractions deviennent accessibles et que les interactions sociales sont réduites considérablement. Dans un tel contexte, les individus ressentent l'isolement et une démotivation, qui doivent être comblés par d'autres moyens que la communication, pour assurer leur bien-être. Traditionnellement, les interactions sociales permettaient de réduire le sentiment d'anxiété, mais furent éventuellement remplacées par des mécanismes d'introversion, comme l'utilisation des réseaux sociaux et le refoulement [Annexe 6] (Wang *et al.*, 2021). D'ailleurs, près du tiers des télétravailleurs sont insatisfaits de la qualité des relations qu'ils entretiennent avec leurs collègues (Wang *et al.*, 2021). La proximité physique dans les interactions sociales est nécessaire à la création de liens, à une relation de confiance et à une culture organisationnelle favorable. Les individus ont besoin de contacts informels, durant lesquels ils peuvent discuter de sujets, qui ne relèvent pas du travail, et de se sentir plus intégrés dans l'environnement organisationnel. Les interactions virtuelles n'offrent pas cette proximité, obligeant les individus à être proactifs pour entreprendre des échanges de la sorte. Cette proactivité motive les individus, bâtit leur confiance, stimule l'affectivité et réduit le sentiment d'isolement au moyen d'un support social élevé (Wang *et al.*, 2021).

2.2. La sécurité informationnelle

La sécurité informationnelle est une discipline des sciences informatiques datant du début des années 60 alors que les ordinateurs étaient principalement orchestrés sur des réseaux fermés. En 1969, l'émergence d'ARPANET, premier réseau ouvert offrant la connectivité des systèmes informatiques, provoque une croissance du nombre d'utilisateurs ayant accès à des données confidentielles. Cette augmentation suscite une préoccupation des ingénieurs alors que l'avancement technologique des années 70 n'assure pas une sécurité convenable. Ainsi, dépourvus de solutions techniques, ces derniers améliorent l'entreposage des données, ce qui permet une meilleure hygiène informatique, admis par le hachage et le cryptage de données confidentielles. Ces améliorations atténuent les craintes d'infiltrations et révèlent un intérêt organisationnel pour une implantation des réseaux ouverts à l'échelle globale. À cette époque, malgré les avancées technologiques considérables, cette interconnectivité des systèmes expose les données confidentielles des organisations qui adhèrent au réseau. Nous pouvions régulièrement constater des attaques sur des infrastructures organisationnelles et gouvernementales à travers les différentes régions du monde. Aujourd'hui, avec l'adoption forcée du télétravail, « *l'expansion rapide de la littéracie informatique assure un nombre croissant d'individus pouvant potentiellement mener des attaques informatiques sur les systèmes des organisations* » (Warner, 2012), ce qui manifeste l'importance de considérer la sécurité informationnelle.

2.2.1. Qu'est-ce que la sécurité informationnelle ?

Le **Tableau 2** présente les définitions conférées aux termes utilisés pour définir la sécurité informationnelle dans les études préalables. Généralement, la sécurité informationnelle est définie indistinctement de la cybersécurité (Von Solms et Van Niekerk, 2013) alors que les limites d'étude des deux concepts sont manifestement différentes et nécessitent une claire délimitation. La **cybersécurité** réfère à la « *protection des réseaux de communication et de l'information qu'ils contiennent contre les infiltrations ou les perturbations malveillantes* » (Lewis, 2006). La **sécurité informationnelle** est plutôt à un sous-concept de cybersécurité dont les limites sont strictement définies par la protection des informations contre ces soi-disant infiltrations et perturbations malveillantes.

Tableau 2 Définitions conceptuelles de cybersécurité et de sécurité informationnelle

Auteur(s)	Numéro de page	Terme(s) utilisé(s)	Définition	Aspect(s) mentionné(s)
(Kemmerer, 2003)	p.706	*Cybersecurity*	« *En grande partie, des méthodes défensives utilisées pour détecter et déjouer les infiltrations potentielles* »	Stratégies, processus et méthodes/ Événements
(Lewis, 2006)	p.1	*Cybersecurity*	« *Protection des réseaux de communication et de l'information qu'ils contiennent contre les infiltrations ou les perturbations malveillantes* »	Solutions technologiques/ Événements
(Ladan, Yari et Khodabandeh, 2008)	p.734	*Information security*	« *Activités visant à protéger l'information contre un large éventail de menaces afin d'assurer la pérennité des activités commerciales, de minimiser les dommages et maximiser le retour sur investissement et les opportunités d'affaires* »	Stratégies, processus et méthodes/ Objets référentiels
(Von Solms *et al.*, 2013)	p.98	*Information security*	« *Protection de l'information et de ses éléments critiques composés de systèmes et de l'infrastructure informatique qui utilise, entrepose et transmet cette information* »	Solutions technologiques/ Stratégies, processus et méthodes
(Craigen, Diakun-Thibault et Purse, 2014)	p.13	*Cybersecurity*	« *Ensemble de ressources, processus et structures utilisées pour protéger le cyberespace et les systèmes compatibles contre les occurrences mal alignées du droit à la propriété* »	Solutions technologiques/ Stratégies, processus et méthodes/ Événements/ Objets référentiels
(Seemma *et al.*, 2018)	p.125	*Cybersecurity, Information security*	« *Notion de protection des systèmes informatiques connectés, soit l'infrastructure, les logiciels et les données, contre les cyberattaques. […] La sécurité, conçue pour maintenir la confidentialité, l'intégrité et la disponibilité des données, est un sous-ensemble de la cybersécurité [la sécurité informationnelle].* »	Solutions technologiques/ Événements/ Objets référentiels

Au cours du XX^{e} siècle, un modèle conceptuel, surnommé *la triade CIA* (*Confidentiality*, *Integrity and Availability*), est élaboré conformément à un consensus scientifique basé sur trois principes fondamentaux : la *confidentialité*, l'*intégrité* et la *disponibilité* des données. Cependant, l'évolutivité informatique rapide amène des enjeux inconsidérés préalablement

et oblige une révision perpétuelle de ces trois dimensions. C'est ainsi que, dans les années subséquentes, la communauté académique intègre des dimensions additionnelles, comme l'*authenticité,* la *non-répudiation,* l'*exactitude,* l'*utilisation éthique* et l*'authentification des utilisateurs,* pour renforcer la sécurité informationnelle (Dhillon et Kolkowska, 2011). Conformément à notre question de recherche centrale, nous avons intégré quelques-unes de ces dimensions pour définir la **sécurité informationnelle**, comme un processus intégré dans une gouvernance des données, ayant pour but d'assurer la confidentialité, l'intégrité, la disponibilité, l'authenticité et l'exactitude des informations, tout en respectant l'intégrité individuelle, la responsabilisation et l'utilisation éthique des données grâce aux TIC.

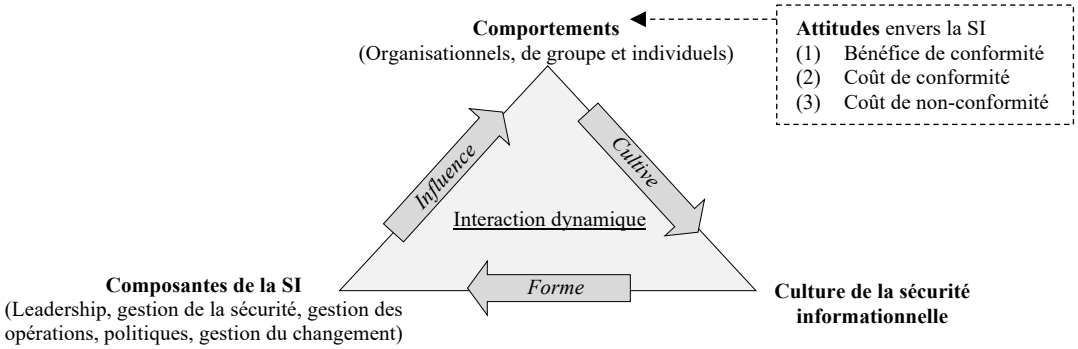
2.2.2. Antécédents de la sécurité informationnelle

Cette section développe une analyse des cadres et des antécédents académiques relatifs au concept de sécurité informationnelle. Les études préalables sont divisées en deux courants académiques dominants, dont un basé sur la modélisation conceptuelle et un second, sur la gouvernance des données et la culture de sécurité informationnelle.

Le premier courant, représentatif de la **modélisation conceptuelle**, correspond entre autres à l'identification des dimensions nécessaires à un environnement informatique sécuritaire. Comme mentionné précédemment, le modèle utilisé traditionnellement est nommé *la triade CIA*. À son origine, ce modèle fit allusion aux éléments fondamentaux des contrôles de sécurité de base en systèmes informatiques. Il paraît initialement en 1975, alors que deux scientifiques allemands définissent la protection des données comme étant l'objectif central en sécurité informationnelle, au détriment de la protection des systèmes informatiques (Saltzer et Schroeder, 1975). Depuis ce temps, ces trois dimensions ont non seulement forgé une compréhension exhaustive du concept, mais ont aussi incité l'adoption de meilleures pratiques quant à son implantation en organisation (Samonas et Coss, 2014). Dans les années suivantes, cependant, *la triade CIA* sème le doute auprès des spécialistes alors que les sciences informatiques évoluent d'une perspective sociotechnique, ce qui implique une nécessité de considérer le facteur humain. Après tout, puisque la majorité des vulnérabilités techniques exploitées dans les brèches informationnelles relève de ce facteur, l'encadrement inefficace du facteur humain est un manquement majeur du modèle initial. Les dimensions *CIA* sont donc insuffisantes et doivent être complétées par des dimensions

additionnelles, telles l'*exactitude*, l'*authenticité*, l'*utilité* et la *possession informationnelle* (Von Solms *et al.*, 2013). En pratique, toutes les dimensions énumérées détiennent une importance considérable, mais leur poids relatif peut varier d'une organisation à une autre, conformément aux particularités organisationnelles, telles que le secteur d'activités au sein duquel opère une organisation. Les organisations du secteur public, par exemple, peuvent accorder plus d'importance à la responsabilisation, l'intégrité individuelle et l'éthique, pour demeurer transparentes et conserver la confiance du public. Les organisations financières, par ailleurs, peuvent priser la non-répudiation, pour assurer la justesse de leurs transactions financières. Le choix de cette importance relative rapporte de la **gouvernance des données**, à savoir « *l'exercice de l'autorité et du contrôle sur la gestion des données. L'objectif de la gouvernance des données est d'augmenter la valeur des données et de minimiser les coûts et les risques liés aux données* » (Abraham, Schneider et Vom Brocke, 2019). Une politique de gouvernance des données alloue justement une considération du facteur humain, alors qu'elle maintient le respect des dimensions sélectionnées pour la protection des données (Anderson, 2003) et instaure une culture de sécurité, qui façonne les comportements et les attitudes des individus à cet égard. À travers les années, une multitude de modèles ont été développés pour définir une **culture de sécurité informationnelle**. Ces modèles sont conçus sur la base de six facteurs déterminants, soit les *comportements individuels*, la *gestion du changement*, la *sensibilisation*, les *exigences*, le *système d'une organisation* et le *savoir-faire informatique*. Les six facteurs interagissent entre eux, à savoir : les comportements individuels constituent les intrants des stratégies adoptées ; la gestion du changement favorise l'adaptabilité desdits comportements ; la sensibilisation conscientise les individus ; les exigences définissent les limites ; et le savoir-faire informatique détermine le niveau de familiarité individuelle avec le système informatique d'une organisation. Ces six déterminants sont éventuellement contextualisés par l'intégration des trois niveaux d'étude (individu, groupe et organisation), pour considérer une granularité des comportements qui sont adoptés en organisation (Da Veiga *et al.*, 2010) [Figure 3 ; Annexe 7].

Figure 3 Niveaux d'étude en contexte de stratégies de gouvernance des données



Cette contextualisation érige une interaction dynamique entre les comportements des trois niveaux d'études, les composantes de sécurité informationnelle et la culture de sécurité des données qui résulte. Les composantes de sécurité informationnelle réfèrent aux intrants qui influencent directement les comportements des individus dans une organisation. On dénote alors des éléments comme le *leadership organisationnel* et la *gouvernance* ; la *gestion de la sécurité*, *des opérations* et *des programmes résultants* ; les *politiques de sécurité* ; et la *gestion du changement* (Da Veiga *et al.*, 2010). Une organisation, dont la gouvernance des données est suffisamment explicite, démontre un engagement en sécurité informationnelle et incite les individus à adopter des comportements sécuritaires. La politique de sécurité, qui résulte ultimement de cette gouvernance, érige des pratiques de gestion de sécurité et d'opérations qui protègent les données confidentielles d'une organisation. Cependant, ces composantes sont insuffisantes dans un environnement dénué de leadership et de gestion du changement parce que ces deux composantes sont indispensables à l'instauration d'une culture de sécurité des données et agissent directement sur les comportements des différents niveaux d'étude. Les comportements en sécurité informationnelle dépendent en partie des attitudes individuelles qu'adoptent les télétravailleurs envers les composantes de sécurité informationnelle, telles que la gouvernance des données (Bulgurcu, Cavusoglu et Benbasat, 2010). Les télétravailleurs doivent percevoir un bénéfice de conformité aux politiques de sécurité, de sorte que ces bénéfices excèdent les coûts de non-conformité (Bulgurcu *et al.*, 2010). Une délimitation par niveau d'étude illustre la divergence des attitudes au sein des organisations si bien que la culture de sécurité informationnelle constitue une interaction dynamique entre les comportements d'individu, de groupe et d'organisation, qui découlent de ces attitudes, et les composantes de sécurité (Da Veiga *et al.*, 2010).

2.2.3. Conséquences de l'adoption forcée sur la SI

Pour évaluer l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle, la présente sous-section est inspirée du modèle dynamique, en **Figure 3**, et est délimitée par les trois niveaux d'étude. Cela nous permet d'évaluer les différentes conséquences à l'égard de la sécurité informationnelle pour l'individu, le groupe et l'organisation.

2.2.3.1. Conséquences de l'adoption forcée sur la SI au niveau de l'organisation

Une première conséquence de l'adoption forcée du télétravail, au niveau de l'organisation, constitue une **révision des procédures** de sécurité. Par exemple, l'*authentification à multifacteurs* (*MFA*) constitue une procédure d'identification des utilisateurs, dont la popularité est directement liée à l'adoption forcée du télétravail (Abidoye, 2021). Considérant que l'entreposage physique de mots de passe établit une vulnérabilité importante des systèmes informatiques, une procédure *MFA* permettent de décentraliser ce processus et de mitiger le risque de sécurité résultant. De cette perspective, l'adoption forcée du télétravail détient une incidence positive sur la sécurité informationnelle étant donné l'amélioration des procédures de sécurité usuelles, comme l'authentification par nom d'utilisateur et par mot de passe. « *L'authentification MFA est une question de saine habitude. Renforcer cette procédure permettra d'habituer les employés à l'authentification additionnelle et à être plus conscient de l'effort déployé par l'organisation à cet égard* » (Abidoye, 2021). De même que, l'automatisation de ces procédures est un élément de la numérisation ayant une incidence positive sur la sécurité informationnelle, alors que la diminution de l'implication humaine réduit les erreurs potentielles. En organisation, une automatisation des procédures de sécurité supporte les tâches quotidiennes des télétravailleurs en libérant du temps pour des activités qui nécessitent l'interaction humaine et la pensée critique, comme la formation de nouveaux employés (Clipper, 2020). Cependant, étant donné que certaines applications de sécurité, tel le *MFA*, sont déployées sans communication complémentaire exhaustive, les télétravailleurs peuvent les percevoir comme un obstacle inutile dans leur flux de travail quotidien, plutôt qu'une mesure de sécurité efficace (Das, Kim et Camp, 2021). Cela peut inciter les individus à se comporter inadéquatement, sous l'effet d'attitudes défavorables à l'égard du *MFA*, dans le but de

contourner l'application, ce qui peut nuire considérablement à la sécurité informationnelle (Bulgurcu *et al.*, 2010).

En adoption forcée du télétravail, la **virtualisation des formations** accroît l'efficience de ces programmes et conscientise davantage les individus vis-à-vis la sécurité des données. Des formations virtuelles transfèrent la responsabilité d'apprentissage de l'employeur vers l'employé, améliorant ultimement la qualité des activités d'apprentissage et une adoption de meilleures pratiques en sécurité. Ces pratiques correspondent à un ensemble de normes et de directives, souvent présenté sous forme d'une liste de contrôle, utilisée pour protéger la sécurité informationnelle (Ma, Johnston et Pearson, 2008). De cette optique, l'adoption forcée du télétravail détient une incidence positive sur la sécurité informationnelle étant donné que la sensibilisation des individus aux enjeux de sécurité des données est une des principales préoccupations en télétravail (Abidoye, 2021). Pour former les individus aux enjeux de sécurité, les organisations doivent investir dans l'amélioration des formations pour solliciter l'engagement des individus dans l'application des politiques de sécurité (He et Zhang, 2019). Considérant l'être humain comme un facteur de vulnérabilité dominant, l'adoption seule des dernières technologies en sécurité informationnelle n'est pas suffisante (Singer et Friedman, 2014). Une sécurité informationnelle adéquate résulte en grande partie du niveau d'éducation des individus (He *et al.*, 2019), traduite par une culture de sécurité informationnelle au niveau de l'organisation. La sensibilisation guide les travailleurs dans l'identification des risques, dans l'emploi des meilleures pratique et permet une protection des actifs informationnels par l'adoption de comportements favorables pour la sécurité des données (Da Veiga *et al.*, 2010). « *Les organisations doivent exposer leurs employés à du matériel de sensibilisation sur une base annuelle […] pour qu'ils soient conscients des attentes de l'organisation* » (Abidoye, 2021).

Une troisième conséquence de l'adoption forcée du télétravail, au niveau organisationnel, est l'adoption d'une **gestion transactionnelle**, aux dépens d'une gestion traditionnellement transformationnelle. De cette perspective, l'adoption forcée détient une incidence négative sur la sécurité informationnelle, car une gestion transformationnelle est jugée plus effective pour la promotion d'une culture de sécurité adéquate. À la question « *quelle est l'approche managériale préférée des télétravailleurs ?* », 57 % des spécialistes ont démontré une

prédilection pour la transformationnelle justifiant ce choix par la nécessité de rassembler tous les télétravailleurs derrière un seul objectif de sécurité informationnelle. « *L'avantage des pratiques de gestion transformationnelles est qu'elles favorisent la communication, en permettant à l'équipe d'utilisateurs d'observer des failles de la sécurité informationnelle et de les communiquer directement au gestionnaire* » (Abidoye, 2021). L'importance d'une collaboration et d'une confiance entre les trois niveaux d'étude a été soulignée à plusieurs reprises dans les sections précédentes (voir **Section 2.1.3**). Ces deux éléments alimentent un discours organisationnel libre, jugé nécessaire à l'instauration d'une culture de sécurité informationnelle. Or, en gestion transactionnelle, ce discours est limité par les relations qui régissent les interactions des individus au sein d'une organisation.

2.2.3.2. Conséquences de l'adoption forcée sur la SI au niveau du groupe

En adoption forcée du télétravail, toutefois, l'**augmentation de la distance psychologique** entre les membres d'un groupe complique la collaboration, la communication et le support social. De cette perspective, l'adoption forcée du télétravail a une incidence négative sur la sécurité informationnelle, considérant que ces éléments sont nécessaires au développement d'une culture de sécurité informationnelle (Abidoye, 2021). Banalement, « *la culture est la communication et la communication est la culture* » (Gudykunst, 1997). L'utilisation de mots répétés spécifiques, dans une discussion courante, façonne ultimement les attitudes et les croyances qui caractérisent les comportements des individus (Gudykunst, 1997). Ces comportements, rappelons-le, constituent la base d'une culture de sécurité informationnelle (Da Veiga *et al.*, 2010). La communication conscientise les individus, par une amélioration de leur compréhension des formalités informatiques et une incitation à les impliquer dans les enjeux de sécurité informationnelle afin de former des attitudes positives (Bulgurcu *et al.*, 2010). Sans une communication efficace, les télétravailleurs perçoivent une diminution de leur impact sur les procédures de sécurité adoptées, ce qui les démotive et réduit leur niveau d'engagement (Abidoye, 2021). Après tout, c'est cet engagement des individus qui permet une adhésion à la culture de sécurité informationnelle et promeut cet aspect au sein de l'organisation. « *Peu importe votre un plan ou votre stratégie en matière d'une culture organisationnelle, si l'adhésion des individus n'est pas là, le tout va échouer ou être certainement moins efficace* » (Abidoye, 2021).

2.2.3.3. Conséquences de l'adoption forcée sur la SI au niveau de l'individu

Au niveau individuel, l'adoption forcée du télétravail détient une incidence sur la sécurité informationnelle par la **numérisation des outils de travail**, qui incite le développement de compétences informatiques des individus et accroît les facteurs relatifs au *technostress* (Molino *et al.*, 2020). De cette perspective, l'incidence de l'adoption forcée du télétravail est mitigée considérant que des outils de travail numériques peuvent, à la fois, augmenter le nombre d'erreurs humaines et le diminuer. La numérisation complexifie les systèmes informatiques des organisations, ce qui provoque les malfaiteurs à exploiter d'autres vulnérabilités, comme des processus impliquant une intervention humaine. L'**ingénierie sociale** (*social engineering*) est « *une technique de manipulation basée sur la confiance et utilisée dans un environnement virtuel pour inciter un individu (la victime) à partager de l'information confidentielle sur une base volontaire* » (Fruhlinger, 2019). Cette technique est souvent utilisée dans les attaques d'hameçonnage, qui constituent l'outil de préférence des malfaiteurs pour cibler les organisations et soutirer de l'information confidentielle aux télétravailleurs. Ces attaques, communément appelées *phishing attacks*, sont des méthodes d'intrusion des systèmes informatiques orchestrés par l'entremise de courriels ou de sites Internet frauduleux ayant pour but d'inciter un individu (*la victime*) à les ouvrir et à fournir un accès à un système informatique (Fruhlinger, 2019). Pour minimiser les risques associés aux attaques d'hameçonnage, les organisations doivent conscientiser les individus par une formation récurrente, qui implique le développement de compétences informatiques et la familiarisation aux procédures de sécurité (Vayansky et Kumar, 2018). Ce n'est pas pour rien que près de 75 % des spécialistes soutiennent que l'éducation continue est une solution efficace pour combattre les fuites de données (Abidoye, 2021). Pour certains, l'éducation des individus est d'autant plus importante que l'implantation de nouveautés technologiques en sécurité, car « *nous pouvons mettre en place toute la technologie existante, mais nous devons préalablement nous assurer que nos employés sont vigilants. Il est préférable [dans un contexte de budget limité] de développer les compétences et la vigilance au détriment de la technologie* » (Abidoye, 2021).

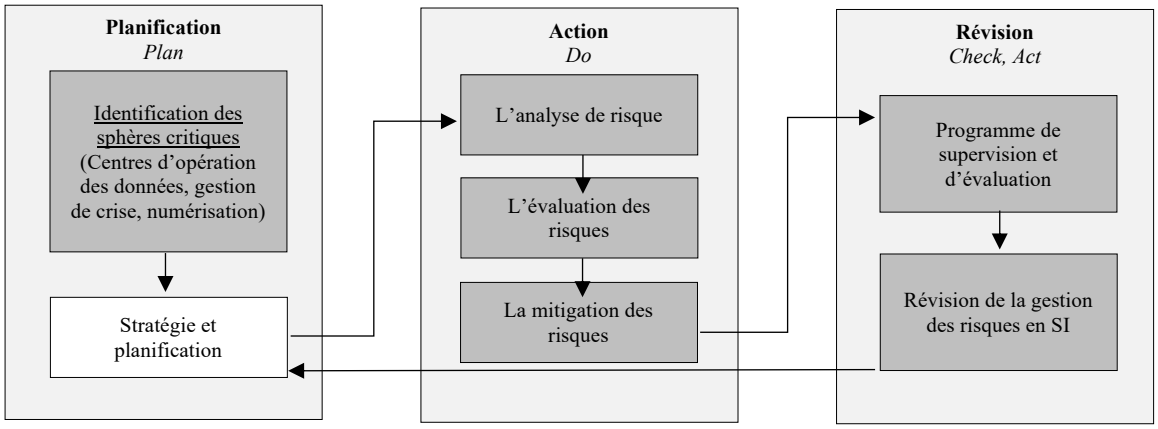
2.3. Les risques de sécurité informationnelle

En organisation, une multitude de risques de sécurité informationnelle sont existants et sont en évolution perpétuelle, tels les attaques d'hameçonnage, la négligence individuelle ou les accès non autorisés en télétravail. Si un télétravailleur utilise un ordinateur personnel pour accéder aux données organisationnelles, il pose un risque informationnel alors que son ordinateur n'est pas muni de logiciels de sécurité adéquats et expose les informations de l'organisation aux malfaiteurs potentiels. Pour mitiger l'exposition à ces risques, un modèle d'évaluation, nommé *PDCA*, est disponible aux organisations (Alberts et Dorofee, 2003) et est souvent intégré dans les meilleures pratiques en gestion de sécurité informationnelle (Tsohou *et al.*, 2010).

Le **modèle *PDCA*** [Figure 4] puise ses principes dans une méthode de gestion de la qualité, la roue de Deming, soit un schéma cyclique composé de quatre étapes, dites *PDCA* (*Plan*, *Do*, *Check*, *Act*), ayant pour objectif de transformer continuellement la planification en action et l'action en apprentissage. Au-delà de son application en gestion de la qualité, cet outil est couramment utilisé au sein de la littérature en gestion de risques organisationnels. En sécurité informationnelle, il est appliqué dans l'objectif de protéger les dimensions des données, comme la confidentialité, l'intégrité et l'accessibilité. Il repose sur sept principes, dont l'*identification* des sphères critiques ; la *planification* ; l'*analyse*, l'*évaluation* et la *mitigation* des risques ; le *programme de surveillance* et d'*évaluation* ; et une *révision des activités de gestion* qui sert d'intrants au processus de la planification stratégique. Ces sept processus sont répartis en quatre étapes, nommées *PDCA*, dont la première est l'étape de planification (*Plan*). Composée des processus d'identification des sphères critiques et d'un processus de planification stratégique, cette étape est fondamentale au développement d'un plan adéquat de mitigation des risques de sécurité informationnelle. La première sous-étape consiste à identifier les sphères critiques, qui peuvent constituer des vulnérabilités pour une organisation, comme la gouvernance, la conformité et l'audit des actifs informationnels. Cette identification sert de fondement pour l'élaboration d'un plan stratégique pour mitiger les risques de sécurité informationnelle, qui détiennent une incidence directe sur les sphères critiques énumérées, et pour formuler une direction à la gestion des risques (Zhang *et al.*, 2010). La deuxième étape constitue l'étape d'action (*Do*) qui correspond à l'application du

plan stratégique et inclut trois étapes, soit l'analyse, l'évaluation et la mitigation des risques organisationnels. L'étape d'analyse produit un examen de la fragilité et de la prudence des décisions stratégiques adoptées. La deuxième étape, soit l'évaluation, réfère plutôt à une détermination des probabilités d'occurrence, à une analyse de l'impact, à une classification des risques et à une liste de recommandations. Une pondération de classification (faible, moyen et élevé) est alors attribuée permettant à l'organisation de prioriser des risques au détriment des autres, considérant des ressources organisationnelles limitées. Sur la base de cette pondération, l'organisation est en état d'adapter ses pratiques de sécurité et d'élaborer des mesures spécifiques aux risques préétablis pour définir une stratégie de mitigation, soit *évitement*, *transfert*, *rétention*, *réduction* ou *acceptation* (Zhang *et al.*, 2010). Une fois la stratégie sélectionnée, un suivi devra être effectué par un procédé de vérification (*Check*) et d'ajustement (*Adjust*) des mesures établies. Ces procédés sont exécutés continuellement de sorte à déterminer s'il est nécessaire d'apporter des correctifs aux mesures adoptées initialement (Zhang *et al.*, 2010).

Figure 4 Modèle de l'évaluation des risques en sécurité informationnelle



2.3.1. Classification des risques en sécurité informationnelle

Nonobstant l'adoption forcée du télétravail, deux catégories de risques en sécurité informationnelle sont recensées, à savoir les risques internes et les risques externes. Les **risques internes** sont exclusivement relatifs aux employés d'une organisation et à certains comportements problématiques, comme l'ignorance, la curiosité ou l'insouciance (Samy, Ahmad et Ismail, 2009). Les **risques externes**, par ailleurs, réfèrent à une menace en lien avec les partenaires externes, les virus, les logiciels d'espionnage et les techniques de

chiffrement des données (Samy *et al.*, 2009). En organisation, les risques internes sont catégorisés en cinq sous-catégories, soit le risque technique, le facteur humain, l'obsolescence technologique, les pannes de matériel informatique et les pannes de logiciel (Zhang *et al.*, 2010). Ces risques sont généralement reliés aux individus, aux équipements, aux réseaux informatiques, aux systèmes d'exploitation et aux logiciels utilisés. En adoption forcée, cependant, les risques pertinents qui découlent des conséquences listées à la **Section 2.2.3** relèvent essentiellement du facteur humain, alors que nous explorons spécifiquement l'impact du comportement des individus en télétravail forcé sur la sécurité informationnelle des organisations. Le **Tableau 3** produit une classification des risques de sécurité informationnelle, qui proviennent des conséquences négatives de l'adoption forcée du télétravail, et illustre les mécanismes à la disposition des organisations pour mitiger et alléger ces conséquences. Les lignes associées aux conséquences positives ne sont pas classées (s.o.) puisqu'elles ne comportent pas un risque pour la sécurité informationnelle.

Tableau 3 Classification des risques de SI résultants de l'adoption forcée du télétravail

Conséquence de l'adoption forcée	Incidence sur la sécurité	Justification	Mécanisme	Classification
Révision des procédures de sécurité.	Adoption de procédures efficaces en SI.	Les nouvelles technologies, tel le *MFA*, sont estimées à croître, en lien avec la révision des procédures de sécurité.	Adoption de meilleures pratiques et d'une gouvernance des données adéquate.	Positive (s.o.)
Virtualisation des formations.	Responsabilisation des employés vis-à-vis leur apprentissage.	Étant mieux formés aux enjeux de SI, les employés commettent moins d'erreurs humaines.	Développement d'une culture de SI.	Positive (s.o.)
Adoption d'une approche de gestion transactionnelle.	Diminution de la motivation des employés et insatisfaction vis-à-vis le travail.	Une perte de motivation des employés entraîne une diminution de conscientisation et augmente le risque humain.	Adoption de meilleures pratiques.	Négative **Moyen**
Augmentation de la distance psychologique entre les membres d'un groupe.	Diminution de la qualité de l'environnement de travail, caractérisé par une baisse de collaboration.	Un mauvais environnement de travail impacte le sentiment de bien-être des individus et les incite à adopter des comportements illicites en SI.	Adoption de meilleures pratiques.	Négative **Élevé**
Numérisation des outils de travail.	Amélioration des compétences informatiques des employés et des habiletés techniques permettant d'être conscients des risques.	Les télétravailleurs subissent du *technostress*, qui impacte l'anxiété et accroît le risque d'erreur humaine. D'autre part, cette utilisation accrue des technologies améliore les habiletés techniques.	Adoption de meilleures pratiques et d'une gouvernance des données adéquate.	Mitigée **Élevé**

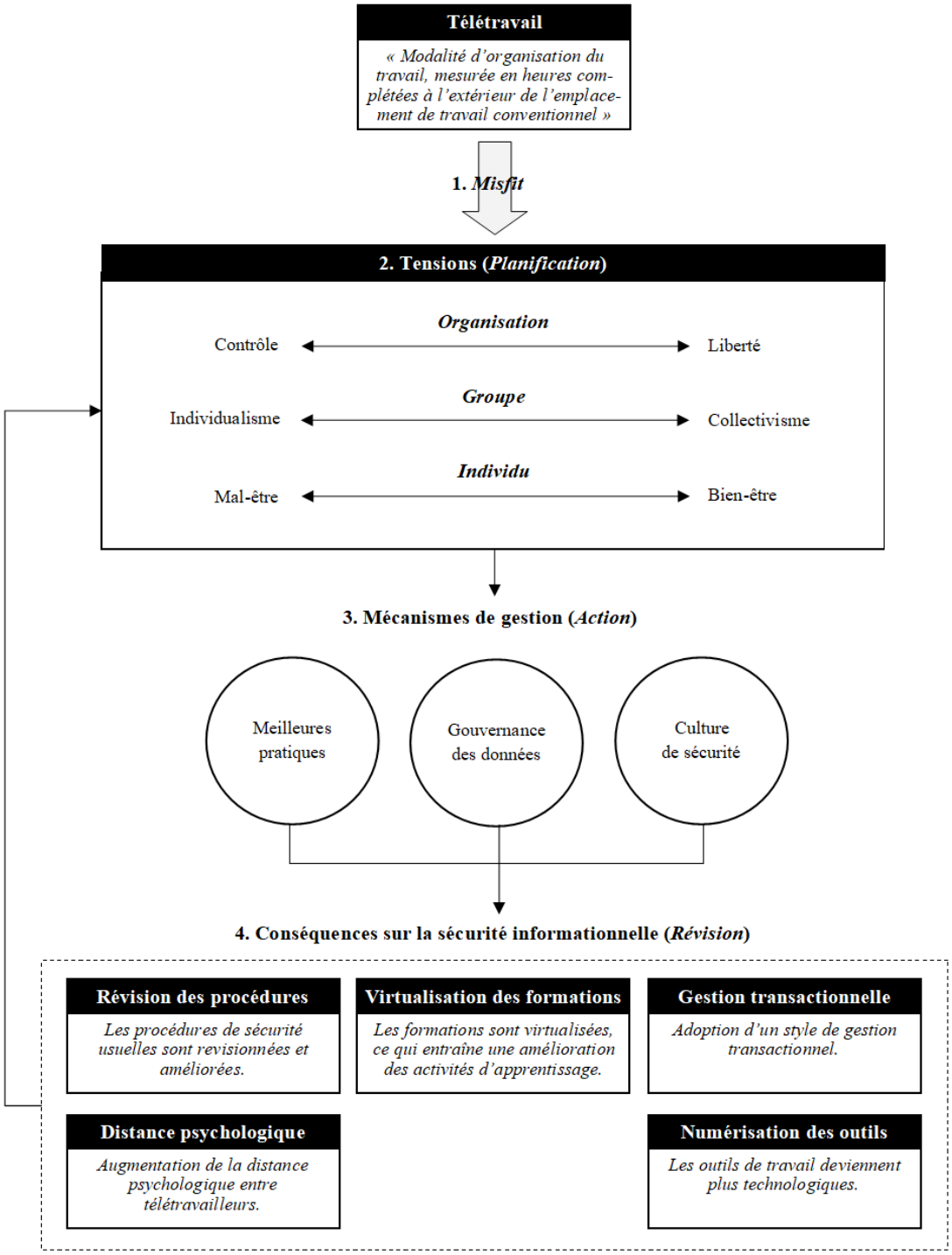
Comme présenté à la **Section 2.2.3**, la révision des procédures de sécurité mène à l'adoption de procédés efficaces, tel le *MFA*, pour protéger les données organisationnelles (Abidoye, 2021). Étant donné que l'entreposage physique d'informations de connexion aux serveurs organisationnels produit une vulnérabilité des systèmes informatiques, l'introduction d'une procédure *MFA* permet de décentraliser ce processus et de réduire le risque de sécurité qui en découle (*incidence positive*). La révision des procédures usuelles surgit de l'adoption de meilleures pratiques et d'une gouvernance des données qui considère les enjeux de sécurité actuels. Elle produit aucun risque pour la sécurité des données et n'est donc pas classée selon la pondération de classification du modèle *PDCA* (Zhang *et al.*, 2010), mais est tout de même considérée dans ce chapitre parce que nous étudions toutes les conséquences de l'adoption forcée qui sont illustrées dans la littérature académique existante. Similairement, la virtualisation des formations est une conséquence de l'adoption forcée du télétravail qui ne produit aucun risque pour la sécurité informationnelle puisqu'elle détient une incidence positive, par une responsabilisation des individus vis-à-vis leur apprentissage. Cette responsabilisation incite l'engagement individuel (Abidoye, 2021) et réduit les risques de sécurité informationnelle associés au facteur humain, qui sont nombreux en adoption forcée du télétravail. La gestion transactionnelle, par exemple, démotive les employés et limite le discours organisationnel entre individus (*incidence négative*), ce qui affaiblit la qualité de l'environnement de travail et incite l'adoption de comportements illicites, comme le non-respect des procédures de sécurité. L'augmentation de la distance psychologique affecte le bien-être individuel, ce qui réduit le sentiment d'appartenance et d'engagement individuel envers une organisation et ses objectifs. La numérisation des outils de travail, bien qu'elle familiarise les individus aux technologies organisationnelles, induit un *technostress* et une fatigue qui, à long terme, découle en un épuisement du télétravailleur (Molino *et al.*, 2020). Contrairement aux risques associés à la gestion transactionnelle, la numérisation des outils de travail et l'augmentation de la distance psychologique sont pondérées à « élevé » puisque la probabilité de leur occurrence est quasi certaine en contexte de télétravail.

2.4. Modèle conceptuel initial

Notre modèle conceptuel, issu de la revue de littérature, analyse les facteurs explicatifs de l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle (« *pourquoi ?* ») et les éléments contextuels (« *comment ?* ») (Whetten, 1989). Dans son développement, nous intégrons le modèle *PDCA*, illustré à travers les notions de *misfit*, des tensions, des mécanismes et des conséquences (Zhang *et al.*, 2010). Pour mesurer adéquatement l'impact de l'adoption forcée, nous évaluons d'abord le *misfit* entre le télétravail et les trois niveaux d'étude simultanément. Si au moins un des trois niveaux d'étude détient un *misfit*, cela génère des tensions au niveau individuel, de groupe et organisationnel. Au niveau de l'organisation, un *misfit* génère une tension entre le contrôle et la liberté, ce qui engendre l'adoption de politiques, de procédures et d'approches managériales sévères. Au niveau du groupe, un *misfit* produit une tension entre l'individualisme et le collectivisme sous l'effet d'une augmentation de la distance psychologique entre individus. Au niveau individuel, un *misfit* génère une tension entre le mal-être et le bien-être sous l'effet de l'épuisement professionnel et de l'isolement social. Puisque ces tensions produisent une incidence sur la sécurité informationnelle, telle qu'illustrée dans le **Tableau 3**, un plan d'action doit être conçu conformément à la première étape du modèle *PDCA*, à savoir la *planification*. Pour mitiger ces tensions, une multitude de mécanismes sont disponibles, soit la gouvernance des données, les meilleures pratiques et la culture de sécurité informationnelle. La seconde étape (*action*) consiste donc à utiliser ces mécanismes pour tempérer les effets du *misfit* sur les tensions énumérées précédemment. Par exemple, la gouvernance des données garantit l'utilisation efficiente des données tout en maintenant un niveau de contrôle pour répondre aux exigences organisationnelles (Abraham *et al.*, 2019). Elle permet d'introduire des règles et des normes qui visent l'encadrement de l'utilisation des données organisationnelles et la définition des rôles et responsabilités. Les meilleures pratiques, par ailleurs, forgent plutôt les normes informelles, qui caractérisent les interactions des travailleurs avec les systèmes informatiques de l'organisation (Tsohou *et al.*, 2010). Ces deux éléments forment la culture de sécurité informationnelle, d'où l'illustration d'une ligne commune qui les lie aux conséquences respectives. Les conséquences constituent les effets de l'adoption forcée du télétravail et forment l'étape de *révision*, alors que l'incidence sur la sécurité des données

est évaluée conformément aux risques qu'elle produit. À cette étape, un suivi est complété par un processus de vérification et d'ajustement des mécanismes de gestion adoptés. Cette rétroactivité des conséquences est représentée par une ligne unidirectionnelle, allant de l'encadré, en point 4, à l'encadré, en point 2. Conformément aux éléments du **Tableau 3**, notre modèle conceptuel initial inclut cinq conséquences, dont une révision des procédures de sécurité, une virtualisation des formations, une adoption d'une gestion transactionnelle et une numérisation des outils de travail.

Figure 5 Modèle conceptuel initial



3. Méthodologie

Une formulation théorique complète doit minimalement inclure trois éléments de réponses aux questions « *quoi ?* », « *comment ?* » et « *pourquoi ?* » un phénomène donné est observé (Whetten, 1989). Répondre au « *quoi ?* », c'est définir les variables explicatives du modèle qui décrit l'occurrence du phénomène considéré. Répondre au « *comment ?* », c'est choisir les variables pertinentes et définir les relations entre elles. Répondre au « *pourquoi ?* », c'est définir les dynamiques qui justifient ce choix et les relations recensées. Étant donné que la revue de littérature répond ultimement à la question « *quoi ?* », nous centrons notre méthode de recherche sur la poursuite de réponses aux questions restantes, à savoir « **comment ET pourquoi l'adoption forcée du télétravail impacte-t-elle la sécurité informationnelle en organisation ?** ». Deux méthodes d'analyse exploratoire de données qualitatives ont été employées pour répondre à chacune de ces sous-questions. Leur sélection est justifiée par l'environnement inédit qui est propice à l'émergence de nouvelles théories (Edmondson et McManus, 2007) et qui caractérise le contexte de notre étude.

3.1. Contexte de l'étude

En contexte d'adoption forcée du télétravail, la gestion du changement vise l'encadrement des tensions résultantes du *misfit* entre le niveau d'étude considéré et le télétravail. Après tout, ce contexte exige un effort d'ajustement important considérant l'évolution perpétuelle des systèmes informatiques et l'expansion d'enjeux contextuels (de Souza et Pidd, 2011). Dans des secteurs d'importance critique, comme la santé ou l'enseignement, la gestion du changement est complexe, car elle doit satisfaire quatre règles fondamentales, à savoir le maintien de la performance, des services offerts, d'une satisfaction et, bien évidemment, d'une sécurité des clients (de Souza *et al.*, 2011). La négligence d'au moins une des quatre règles énumérées produit un échec, justifiant ainsi la réticence organisationnelle vis-à-vis l'adoption de nouveaux procédés, comme le télétravail (Kaplan et Harris-Salamone, 2009). En contexte d'adoption forcée, cependant, cette réticence n'est pas admissible puisque les organisations sont contraintes à la mitigation des risques relatifs à l'incidence de l'adoption forcée du télétravail au moyen des mécanismes de gestion disponibles. C'est justement cet environnement inédit qui nous permet de formuler notre contribution principale et de bâtir un fondement pour les études futures, relatives à l'adoption forcée du télétravail.

3.2. Conceptions méthodologiques

Deux conceptions méthodologiques d'analyse exploratoire de données qualitatives ont été employées dans notre étude, soit l'induction analytique, pour répondre au « *pourquoi ?* », et l'analyse thématique, pour répondre au « *comment ?* ».

L'**analyse thématique** est une notion méthodologique de l'analyse exploratoire « *ayant pour cible d'identifier, d'analyser et d'interpréter des thèmes récurrents, issus de données qualitatives* » (Braun et Clarke, 2012), comme des transcriptions d'entrevues ou d'une revue de littérature. Cette méthode constitue un moyen d'identification des similarités sur la façon dont un phénomène est expérimenté par des individus, impliqués dans l'occurrence du phénomène, comme en contexte du télétravail et des télétravailleurs. Ces similarités ne sont pas toujours pertinentes, alors que nous nous intéressons essentiellement à celles qui nous permettent de répondre à notre question de recherche. Notamment, si une majorité d'individus interrogés affirment, qu'en réponse à l'adoption forcée du télétravail, ils prennent des pauses prolongées, cela constitue certainement un patron de similarité, mais pas *un* qui est pertinent en contexte d'incidence sur la sécurité informationnelle. Cependant, si l'action de prolonger les pauses impacte la sécurité informationnelle puisque les télétravailleurs ne verrouillent pas leur ordinateur de travail, alors nous devons décidément la considérer. L'analyse thématique est produite dans une démarche en six étapes (Braun *et al.*, 2012). D'abord, nous nous *familiarisons* avec les données collectées à travers une lecture attentive des transcriptions d'entrevues et une écoute immersive des enregistrements. Lors de cette étape, nous notons les éléments importants et le temps auquel ils ont été observés. Conformément aux observations relevées, nous générons des *codes* de données qualitatives en vertu des méthodes d'encodage ouvert, axial et sélectif. Ces méthodes sont détaillées explicitement dans les sections subséquentes de ce chapitre. Ensuite, nous entamons notre quête de *thèmes récurrents* à travers les réponses des participants, d'où l'attribution du nom à cette conception méthodologique, soit l'analyse thématique. Nous *révisons* la pertinence des thèmes relevés, leur attribuons des *libellés* et produisons une carte thématique, appelée *structure de données* et *chaîne de preuves* [Annexe 9]. Cette carte est un outil visuel (Braun *et al.*, 2012), qui identifie les thèmes, les sous-thèmes et les connexions entre ces derniers et les citations d'entrevues semi-

structurées. Le choix de cette conception méthodologique est justifié par l'utilité d'identifier des patrons de similarité qui permettent de formuler de nouvelles théories qui découlent de la question : *comment* l'adoption forcée du télétravail détient une incidence sur la sécurité informationnelle en organisation ?

En 1934, Florian Znaniecki, sociologue polonais, développe l'**induction analytique** qui, contrairement à l'induction énumérative, n'attribue pas de valeur à l'accumulation de cas affirmatifs, mais recherche plutôt les cas contradictoires afin d'itérer les facteurs explicatifs en fonction de leur incidence sur un phénomène observé (Patton, 1990). Ces facteurs sont formulés initialement sur les éléments théoriques, issus des études relatives au télétravail, à la sécurité informationnelle et aux risques respectifs qui furent sélectionnées avec minutie pour leur pertinence et leur contribution à la recherche. En effet, le choix des études repose sur plusieurs critères de justification. D'abord, la pertinence a été évaluée conformément à leur capacité à fournir des concepts théoriques clés et à soulever des enjeux qui découlent de l'adoption du télétravail, que celle-ci soit forcée (Wang *et al.*, 2021) ou non (Mokhtarian *et al.*, 1993). Ensuite, l'autorité des auteurs a elle aussi été considérée, alors que plusieurs auteurs recensés dans notre revue de littérature sont de véritables experts dans les domaines à l'étude et furent cités à une multitude de reprise dans des projets de recherche subséquents (Bulgurcu *et al.*, 2010; Cooper *et al.*, 1990; Von Solms *et al.*, 2013). Finalement, la portion contributive des études à l'élaboration d'un modèle conceptuel de sécurité informationnelle en contexte de télétravail a été évaluée (Abidoye, 2021). Ces études ont permis d'identifier les éléments nécessaires (*misfit*, tensions, mécanismes de gestion, conséquences) à l'étude de la sécurité informationnelle en contexte de travail à distance, et ont fourni des preuves empiriques pour soutenir la construction de l'induction analytique. En réalité, l'induction analytique fut initialement appliquée en contexte d'études comportementales afin de formuler les facteurs de dépendance (Lindesmith, 1947), de crimes fiscaux (Cressey, 1950) et même de dépression (Angell, 1936). Toutefois, avec l'évolution du volet sociotechnique en sciences informatiques, les chercheurs ont élargi son usage à l'étude de phénomènes TI, telle la résistance au changement en adoption technologique (Lapointe et Rivard, 2005). L'induction analytique est *une approche méthodologique qui étudie les relations théoriques entre des conditions conjointement suffisantes et l'émergence d'un phénomène observé* (Katz, 2001). Appelé *explicandum*, le phénomène à l'étude est porté à altérer sur

une base itérative de sorte à maintenir une relation théorique avec des facteurs explicatifs, appelés *explicans*. Dans notre étude, l'explicandum constitue l'incidence d'une adoption forcée du télétravail sur la sécurité informationnelle et les explicans, les facteurs explicatifs de cette incidence. Le choix de cette conception méthodologique est justifié par la complexité ainsi que la nouveauté du phénomène qui caractérise les raisons « *pourquoi l'adoption forcée du télétravail détient-elle une incidence sur la sécurité informationnelle en organisation* ». Cette méthode est pertinente en contexte de phénomènes peu étudiés, comme l'adoption forcée du télétravail. Elle nécessite un encodage de données collectées pour faciliter l'analyse des informations, pour repousser les limites académiques et pour enrichir notre compréhension du phénomène (Patton, 1990). À cet effet, nous utilisons les codes produits conformément à l'analyse thématique.

3.3. Processus de collecte des données

Notre étude implique un volume considérable de données qualitatives, issues d'entrevues semi-structurées auprès de télétravailleurs qui ont expérimenté l'incidence d'une adoption forcée du télétravail en organisation. Ces données nous permettent d'explorer les concepts théoriques, abordés dans le deuxième chapitre de ce mémoire, et d'obtenir une perspective pratique, à travers une discussion ouverte avec des individus concernés.

3.3.1. Sélection des participants

Préalablement au processus de sollicitation, nous avons défini clairement quelle population nous souhaitions interroger, afin d'assurer une verbalisation des limites académiques et une sélection rigoureuse de l'échantillon, conformément aux objectifs inférentiels de l'étude (Eisenhardt, 1989). En contexte d'étude exploratoire de données qualitatives, l'inférence statistique est inadmissible puisque les résultats de l'étude sont ultimement définis par les participants qui la composent (Yin, 2003). Dans notre cas, les participants ne dérivent pas d'un échantillonnage aléatoire et nécessitent donc une justification des motifs de sélection (Taherdoost, 2016). Cet échantillonnage est issu d'une population de télétravailleurs actifs au moment de l'étude, filtré en fonction du sexe, de l'occupation et du secteur d'activités. Nous justifions ces critères par la nature des interactions des participants avec les systèmes informatiques de leur organisation, qui diffère respectivement à l'occupation et au secteur

d'activités. Le sexe est uniquement utilisé pour garantir une représentativité conforme des participants. Dans notre étude, nous excluons également les télétravailleurs contractuels, à temps partiel et ceux qui disposent d'une relation avec le chercheur. Pour l'échantillonnage, nous avons employé une méthode mixte, composée d'échantillonnage par quotas (*quota sampling*) et d'échantillonnage par convenance (*convenience sampling*), compte tenu de la commodité et de la représentativité qu'allouent ces méthodes, lorsqu'utilisées ensemble. L'**échantillonnage par quota** est une méthode d'échantillonnage non probabiliste, dont le fondement est établi sur la distribution proportionnelle des individus de sorte à représenter des caractéristiques spécifiques d'une population. L'**échantillonnage par convenance** est une méthode d'échantillonnage non probabiliste, dont le fondement constitue une sélection naïve des individus dans le but d'accommoder le chercheur. Notre échantillon est formé de participants diversifiés, comme illustré par le **Tableau 4** et le **Tableau 5**.

Tableau 4 Constitution de l'échantillon à l'étude

Secteur d'activités	Acronyme	Description des fonctions	Décompte
Consultation en technologie d'information	P1	Responsable d'un département de solutions technologiques pour les organisations en santé	1 (8 %)
Santé	P2	Gestionnaire intermédiaire d'une équipe de systèmes d'information	1 (8 %)
Consultation en technologie d'information	P3	Consultant en solutions technologiques des ressources humaines	3 (25 %)
	P4	Consultant en solutions technologiques relatives aux opérations	
	P5	Consultant en implantation de solutions Oracle	
Finance et comptabilité	P6	Auditeur(trice)	2 (17 %)
	P7	Analyste de titres financiers	
Santé	P8	Technicien(ne) en administration	2 (17 %)
	P9	Agent(e) de la gestion du personnel	
Bancaire	P10	Analyste d'affaires	1 (8 %)
Télécommunication	P11	Scientifique de données	1 (8 %)
Jeux vidéo	P12	Scientifique de données	1 (8 %)
Nombre total de participants			12 (100 %) (Sexe : 7H, 7F)

Tableau 5 Critères de sélection des participants

Critères		Justification
Inclusion	A vécu le pré et la post-adoption forcée du télétravail pendant la pandémie.	Le répondant doit avoir été présent au sein d'une organisation de son choix avant et après l'adoption forcée du télétravail, car nous souhaitons capter les différences.
Inclusion	Est un télétravailleur actif au moment de l'entrevue.	Une partie de l'étude vise à comprendre l'incidence des modalités de post-adoption du télétravail sur les individus.
Inclusion	Doit avoir vécu la transition au poste, qui sera évalué à l'étude.	Il est important que le participant sélectionné ait été employé à son poste au moment de la transition. Ultimement, nous voulons considérer l'expérience de transition de la perspective du poste considéré (salarié, gestionnaire intermédiaire, gestionnaire supériuer). Un gestionnaire doit avoir été un gestionnaire au moment de la transition.
Inclusion	Doit être à un poste qui nécessite une utilisation des systèmes informatiques ou des données.	Puisque notre étude est centrée sur la sécurité des systèmes informatiques, nous avons besoin de participants qui interagissent avec ces systèmes pour évaluer l'incidence du télétravail sur leur travail. Ce filtre ne s'applique pas aux gestionnaires et aux membres de la direction, en raison de la nature stratégique de leur poste.
Exclusion	Est un employé contractuel.	Les employés contractuels ne subissent pas les mêmes politiques à l'égard de sécurité informationnelle que les employés permanents
Exclusion	Détient une relation professionnelle active avec le chercheur.	Une relation professionnelle active du participant avec le chercheur brimerait la qualité des réponses collectées, alors qu'il est probable que le participant adapte ses réponses.
Exclusion	Est à temps partiel.	Un employé à temps partiel ne subit pas suffisamment les impacts de l'adoption forcée du télétravail pour évaluer son incidence sur la SI.

3.3.2. Sollicitation et déroulement des entrevues semi-structurées

La sollicitation et le déroulement des entrevues semi-structurées ont été complétés en vertu des normes éthiques, de sorte à minimiser les enjeux à cet égard. Ces normes reposent sur trois principes fondamentaux, à savoir le respect de la personne, de la justice et du bien-être. Dans notre étude, 350 individus ont été sollicités à travers une publication sur le réseau social professionnel, *LinkedIn*. Pour manifester un intérêt, les individus sollicités devaient écrire au chercheur, en privé, suite à quoi ils recevaient les détails explicitant les objectifs, les bénéfices, les risques et les implications d'une participation à l'étude. Si ces éléments satisfaisaient l'individu, il planifiait une date pour passer l'entrevue semi-structurée. À cet effet, un guide d'entrevue a été élaboré pour diriger une discussion entourant les concepts théoriques recensés dans la revue de littérature [Annexe 10]. Dix-sept questions ont été formulées en trois temporalités distinctes, à savoir la préadoption forcée, l'adoption forcée et la post-adoption forcée. La préadoption forcée correspond à une période allant jusqu'en mars 2020, soit le mois où le télétravail a été adopté obligatoirement dans les organisations. La période d'adoption forcée correspond plutôt à la période qui s'étale de mars 2020 à mars 2022, soit le mois où les organisations ont commencé à offrir le télétravail sur un fondement plus volontaire. La période de post-adoption forcée réfère à toute la période au-delà de mars 2022, qui caractérise le début d'une période où les individus considèrent le télétravail, telle une norme sociétale. Une distinction par temporalité est nécessaire pour établir l'effet isolé de l'adoption forcée du télétravail, à travers son évolution dans le temps. Les questions ont également été groupées par thèmes de notre modèle conceptuel initial, soit le *misfit*, les tensions, les mécanismes de gestion et les conséquences sur la sécurité informationnelle. Les participants ne pouvaient pas consulter ce guide préalablement à l'entrevue puisque nous souhaitions obtenir des réponses sur le vif, reflétant les sentiments immédiats des télétravailleurs. Effectuées sur la plateforme *Teams*, via vidéoconférence, les entrevues étaient d'une durée approximative d'une heure et leur contenu était enregistré et transcrit en verbatim, au processus d'analyse des données.

3.4. Processus d'analyse de données

Les transcriptions d'enregistrements ont été partiellement anonymisées considérant que les participants ont été définis par un acronyme (P1 à P12), par leur occupation et par le secteur d'activités de leur organisation. L'objectif de cette analyse de données est de complémenter notre modèle conceptuel avec de l'information, issue des entrevues semi-structurées. Celle-ci est complétée grâce à l'induction analytique et l'analyse thématique, comme mentionnée préalablement. D'abord, nous érigeons un système d'encodage pour faciliter le classement et l'exploration des données qualitatives en débutant par une transcription en verbatim des entrevues semi-structurées et en formulant un thème général par combinaison de question-réponse (« *open coding* », ou codage ouvert). À chaque combinaison, nous nous formulons les questions suivantes : « *qu'est-ce que ces données signifient ?* », « *à quelle catégorie de réponse correspondent-elles ?* », « *quel événement est observé ?* » et « *quelle préoccupation est définie par le participant ?* ». Nous étudions les transcriptions, une ligne à la fois, pour minimiser les risques d'omission, générer les codes initiaux et assurer une compréhension intégrale des données collectées. Cette compréhension est pertinente au développement du « *axial coding* », ou codage axial, où nous cherchons des similarités entre les codes initiaux et les groupons dans des regroupements homogènes, par section et sous-section. Un thème peut appartenir à plusieurs regroupements simultanément. Les relations établies entre ces regroupements fondent les concepts que nous adressons au chapitre de la présentation des résultats (« *selective coding* » ou codage sélectif). Ces concepts ont été détaillés à l'annexe 9, à travers une série de chaînes de preuve, soutenues par des observations empiriques de nos entrevues semi-structurées. Le **Tableau 6** présente quelques exemples du processus de construction du système d'encodage. Pour une version complète, voir l'**Annexe 8**.

Tableau 6 Exemples du processus de codage des transcriptions verbatim

	Codage ouvert	Codage axial		Codage sélectif
Citation	**Thème**	**Section**	**Sous-section**	**Code**
« *C'est sûr que la pandémie a beaucoup forcé le bras de l'organisation* » (P2)	Télétravail (TLTR)	Adoption (ADOP)	Misfit (FIT)	TLTR-ADOP-FIT
« *Il y a eu beaucoup de formations et même beaucoup de proactivité de la part des départements TI* » (P1)	Sécurité informationnelle (SI)	Implantation (IMPL)	Sensibilisation (SENS)	SI-IMPL-SENS
« *En finance, nous avons des partenaires à l'échelle mondiale, alors les TIC ont toujours été de mise pour rencontrer des partenaires* » (P7)	Mécanismes de gestion (GEST)	Implantation (IMPL)	Utilisation technologique (TIC)	GEST-IMPL-TIC
« *Nous avons mis en place un comité responsable de l'organisation d'événements de socialisation en contexte de télétravail* » (P2)	Mécanismes de gestion (GEST)	Implantation (IMPL)	Difficultés (DIFF)	GEST-IMPL-DIFF
« *Le gestionnaire doit développer son aspect empathique pour comprendre comment ses employés se sentent* » (P10)	Mécanismes de gestion (GEST)	Implantation (IMPL)	Approche managériale (MNGT)	GEST-IMPL-MNGT
« *Chez nous, le travail est basé sur la confiance et sur les livrables* » (P3)	Tensions (TENS)	Politiques (POL)	Contrôle et liberté (CONT-LIB)	TENS-POL-CONT-LIB
« *100 % plus d'individualisme en télétravail* » (P12)	Tensions (TENS)	Environnement (ENV)	Individualisme et collectivisme (IND-COL)	TENS-ENV-IND-COL
« *À la fin d'une journée en télétravail, je me sens moins satisfait. Le fait de rester à la maison me fait sentir plus moche* » (P6).	Tensions (TENS)	Ressenti (RESS)	Mal-être et bien-être (MAL-BIEN)	TENS-RESS-MAL-BIEN
« *Je pense qu'à court terme la performance a certainement explosé vers le positif, car les gens étaient très en faveur de la transition du télétravail* » (P10)	Conséquence (CONS)	Performance (PERF)	Indicateurs (IND)	CONS-PERF-IND

Pour répondre au « *comment?* » nous élaborons une conception théorique de l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle en identifiant les patrons de similarités entre la littérature et les éléments de réponses des participants. Chacune des réponses est associée à des codes, que nous utilisons pour évaluer la fréquence de répétition d'un thème spécifique. Dès lors, plus un thème est récurrent, plus importante est l'attention que nous y attribuons. Par exemple, si plusieurs participants mentionnent les effets du *misfit* au télétravail, sous forme d'inadéquation du matériel informatique à domicile, une réponse comme suit peut être formulée : l'adoption forcée du télétravail détient une incidence sur la sécurité informationnelle **par** l'effet du *misfit* sur les tensions individuelles, qui réduisent

le sentiment de bien-être et influencent la vigilance des individus aux enjeux organisationnels, comme la sécurité des données. Pour répondre au « *pourquoi?* », d'autre part, nous fixons une règle associative des facteurs expliquant l'occurrence du phénomène et confirmons la pertinence de cette règle à travers les réponses des participants. Dans notre étude, les facteurs explicatifs sont formulés conformément aux conséquences de l'adoption forcée du télétravail sur la sécurité informationnelle, issues de la revue de littérature et des entrevues semi-structurées. Par exemple, si un participant confirme que le télétravail produit un effet sur la virtualisation des formations, une réponse comme suit peut être formulée : l'adoption forcée du télétravail détient une incidence sur la sécurité informationnelle, **car** les individus sont davantage responsables vis-à-vis leur apprentissage et sensibles aux enjeux de sécurité des données. Conformément aux principes d'induction analytique, nous identifions d'abord les cas où le phénomène a été observé, grâce à la question dix-sept du guide d'entrevue.[2] Dans notre étude, tous les participants attestent que l'adoption forcée du télétravail impacte la sécurité informationnelle, d'où la raison pourquoi toutes les réponses sont considérées. Une fois complétée, l'analyse est présentée au chapitre de discussion des résultats, où nous incitons une discussion selon une logique de « *pattern-matching* » (Sinkovics, 2019).

[2] Question dix-sept : *En sommes, que pensez-vous de l'impact du télétravail sur la sécurité informationnelle au sein de votre organisation?*

4. Résultats de l'étude

Ce chapitre présente les données collectées dans le cadre d'entrevues semi-structurées avec des télétravailleurs actifs, au moment de l'étude. Ces données ne sont pas contextualisées alors que l'objectif du présent chapitre réside plutôt dans la verbalisation et la présentation des résultats. Rappelons que douze participants ont été sélectionnés sur la base de leur sexe, leur occupation et le secteur d'activités de leur organisation. Nous souhaitions obtenir une perspective hétérogène, avec une représentation équilibrée des différents niveaux d'étude.

4.1. Le concept de *misfit*

Notre modèle conceptuel, présenté au chapitre de la revue de littérature, conçoit le *misfit* à titre de facteur d'indisposition globale au télétravail. Cependant, en comparaison au modèle initial, la séparation du *misfit* par individu, groupe et organisation est nécessaire et soutenue par les réponses des participants à l'étude.

Au niveau **organisationnel**, tout comme pour l'individu, le *misfit* dépend essentiellement des composantes menant à la résistance de l'adoption du télétravail. Dans notre étude, une majorité des participants affirme que leur organisation autorisait le télétravail à une certaine fréquence, en préadoption forcée. Pour P1, l'organisation était tellement favorable à l'idée « *qu'ils ont entièrement fermé des bureaux présentiels [deux ans avant la pandémie]* ». Le télétravail était alors un privilège réservé à une classe affluente de travailleurs, en situation d'imprévus. « *On était principalement en présentiel, mais si nous avions un empêchement, comme trop de trafic, rendez-vous chez le médecin, c'était très possible [de télétravailler]* » (P1). Une implantation organisationnelle du télétravail préalablement à l'adoption forcée détient une incidence positive sur la sécurité informationnelle de l'organisation, en contexte de crise, comme la pandémie. Les organisations qui avaient déjà implanté le télétravail ont probablement sensibilisé leurs employés sur les meilleures pratiques et les comportements sécuritaires, ce qui déteint inévitablement sur les tensions résultantes de l'adoption forcée. Cependant, la fréquence de télétravail permise n'était souvent pas établie, alors que « *il n'y avait pas de politiques claires à cet égard* » (P3). L'absence de clarté en matière de télétravail peut entraîner une utilisation inappropriée des données organisationnelles, puis en un déficit de contrôle sur la sécurité informationnelle. Les secteurs bureaucratiques, par

ailleurs, empreints historiquement d'une utilisation inefficace des TIC, étaient davantage réticents à l'adoption du télétravail, traduit par un *misfit* et un contrôle supérieur des politiques adoptées. « *Nous sentons un resserrement au niveau de procédures de sécurité, comme une gestion plus restrictive des accès aux données confidentielles* » (P2). Les participants provenant des secteurs, comme la santé et le bancaire, étaient plus susceptibles de travailler dans ces organisations. Un contrôle sévère peut également impacter la sécurité informationnelle, alors qu'il complexifie les tâches des télétravailleurs, en les obligeant à suivre des protocoles supplémentaires. Cela peut entraîner une baisse de productivité et de motivation, ainsi qu'une frustration croissante chez les employés. Ultimement, ils peuvent être tentés de contourner ces protocoles, s'ils sont perçus comme étant excessifs et inutiles. « *Je crois qu'en télétravail, loin des yeux de ses collègues et des gestionnaires, il est naturel pour des individus d'être moins freinés à adopter un comportement illicite, comme jeter un coup d'œil à de l'information sensible* » (P4).

Au niveau du **groupe**, les gestionnaires soutiennent l'absence d'un *misfit* au télétravail, en justifiant ces propos par une productivité augmentée et une préférence des télétravailleurs. « *C'est sûr que la pandémie a beaucoup forcé le bras de l'organisation, mais mon équipe était prête depuis longtemps* » (P2). À titre de facteur déterminant de cette productivité et préférence, P2 mentionne la synergie d'équipe et note son effet positif sur les conséquences de l'adoption forcée du télétravail. « *La différence entre une équipe qui connaît du succès et une équipe qui éprouve des défis est dans le plaisir que chacun ressent individuellement à travailler au sein de cette même équipe* » (P2). Sans cette synergie, les facteurs, qui jouent un rôle sur les conséquences, sont amplifiés par le mécontentement des télétravailleurs d'où l'importance d'établir des pratiques de gestion qui favorisent l'établissement d'une culture d'équipe. La synergie détient une incidence positive sur la sécurité informationnelle, alors que les individus sont davantage prompts à respecter des procédures de sécurité lorsqu'ils éprouvent un sentiment d'appartenance à leur équipe et à leur organisation. Cependant, il y a également des équipes qui témoignent d'un *misfit* au télétravail puisque leurs gestionnaires ne croient pas aux bénéfices d'une telle méthode d'organisation. « *Ça dépend des équipes parce que j'ai entendu d'autres équipes que les gestionnaires préfèrent un retour complet, à une fréquence de 5 jours par semaine* » (P7). Lorsqu'un gestionnaire, ou au moins un membre de l'équipe de télétravailleurs ne sont pas suffisamment *fit* à travailler

à distance, cela résulte potentiellement en une adoption de comportements individualistes au sein d'un groupe. Ces comportements contre-productifs entraînent des répercussions indirectes sur la sécurité informationnelle, comme une faible communication, et des répercussions directes, comme une augmentation du nombre d'erreurs commises, des pertes de données et du non-respect des procédures de sécurité. Pour éviter cela, P2 soutient qu'une approche de gestion transactionnelle, avec une considération transformationnelle, est ce qui fonctionne le mieux pour son équipe. « *Nous nous sommes adaptés à déléguer plus. Aucune microgestion. Un laisser-aller, mais au sein positif, sachant que mon équipe était en mesure de livrer, sans être surchargée* » (P2). Cette adaptation n'a pas été répertoriée pour tous les participants, alors que P11 soulève que « *le style de gestion n'a pas changé, mais il aurait certainement dû* » (P11).

Au niveau **individuel**, le *misfit* est mesuré par les facteurs d'indisposition, comme le sociodémographique, les intérêts et les attitudes. « *Ça dépend de chaque personne. Peut-être en fonction des traits de personnalité, comme l'introversion et l'extraversion? Moi, je crois que je suis au milieu. Je suis relativement bien en télétravail, mais j'ai également besoin de changer d'air quelques fois* » (P10). Cet argumentaire rejoint notre conceptualisation initiale qui associe les facteurs d'adoption aux forces individuelles et aux caractéristiques de l'environnement de travail. Par exemple, l'accès à du matériel informatique de qualité est la préoccupation principale, soulevée par les participants en vertu du l'adoption forcée du télétravail. « *Moi, personnellement, le télétravail ne m'a pas dérangé, mais j'ai d'autres collègues qui n'aimaient pas ça du tout. Ce n'est pas tout le monde qui a accès à du matériel adéquat à la maison, il y en a qui habitent chez leurs parents ou qui ont un bureau dans leur chambre ou sur le coin de la table de cuisine* » (P1). Un manque d'accès à du matériel de qualité détient un impact négatif sur la sécurité informationnelle, alors que les appareils personnels des télétravailleurs ne sont habituellement pas équipés de logiciels de sécurité adéquats et peuvent constituer un point de vulnérabilité informatique. Quand une organisation ne procure pas un matériel de qualité, elle incite l'adoption de comportements indésirables, comme l'utilisation de téléphones personnels pour accéder à de l'information confidentielle. L'accès à un matériel de qualité est un intrant nécessaire à un environnement de travail, qui minimise les effets du *misfit* sur le bien-être. Dans un tel environnement, les télétravailleurs peuvent mieux

fixer une barrière évidente entre la vie personnelle et la vie professionnelle : « *Quand j'avais mon bureau dans ma chambre, c'était difficile de faire la barrière entre le travail et la maison. Maintenant que j'ai un bureau, c'est facile de fermer la porte et de décrocher psychologiquement* » (P11) ; et de réduire l'anxiété de performance, associée à une mauvaise utilisation du matériel informatique : « *Ce qui me préoccupait beaucoup, c'est la qualité de mon Wi-Fi et mes moniteurs. Souvent, en appels Teams, alors qu'il est important de faire bonne impression dans mon domaine, ma caméra figeait et ça ajoutait un stress à ma relation avec les clients* » (P3). P4 soulève le rôle que doivent jouer les organisations pour fournir aux télétravailleurs les conditions nécessaires à l'exercice de leurs fonctions professionnelles. « *J'ai demandé à mon ancien boss un accès à du matériel informatique additionnel, comme des écouteurs à son isolé parce que j'ai beaucoup de bruits à la maison et ça m'empêche de me concentrer. Ma demande a été refusée* » (P4). Après tout, l'accès à un environnement et à un matériel adéquat détient une incidence directe sur la productivité en télétravail, facteur qui est certainement amplifié par les situations personnelles spécifiques, comme la présence d'enfants dans un ménage. « *Quand les garderies étaient fermées et que mes enfants étaient à la maison, je ne pouvais pas travailler plus d'une demi-heure sans être interrompue. Tous les jours, je reprenais mes heures après qu'ils se couchent, à 20 heures* » (P9).

Notons que tous les participants étaient en faveur à l'implantation du télétravail, avant son adoption forcée, ce qui démontre un *fit* psychologique des individus à l'étude. Ils en notent aujourd'hui une amélioration nette de la commodité qui est principalement associée à une réduction du temps de déplacement. « *J'ai toujours été en faveur [du télétravail]. Surtout qu'en pandémie, j'étudiais en parallèle et que le télétravail m'a permis de réduire considérablement mon temps de déplacement* » (P8). Cette amélioration de commodité au travail permet d'accroître la qualité de vie familiale des individus : « *Avant le télétravail, je faisais près de 20 heures de déplacements par semaine, ça enlève la vie de famille* » (P1). Une meilleure balance entre la vie professionnelle et la vie personnelle réduit le *misfit* individuel, caractérisé par plusieurs autres facteurs, dont un exode urbain, alors que certains télétravailleurs ont profité de la pandémie pour s'installer à l'extérieur des villes. « *[Les politiques de retour au bureau] n'ont pas de problème pour les personnes qui habitent à Montréal, mais elles sont moins bien accueillies par les gens qui ont déménagé pendant la*

pandémie » (P10). De ces changements résulte inévitablement une divergence des intérêts qui positionne les gestionnaires intermédiaires en position délicate. D'un côté, ils doivent promouvoir l'atteinte d'objectifs organisationnels, par un contrôle et une supervision de l'avancement des projets ; de l'autre, assurer une pérennité mobilisatrice de leurs employés, en allouant de l'autonomie et de la liberté. « *[Au début de l'implantation du télétravail], notre principale préoccupation était de savoir comment effectuer un suivi des livrables de ton équipe. Comment fais-tu pour savoir que ton employé a complété sa journée de travail, en termes d'heures ? Nous misions alors sur des suivis quotidiens, des comptes-rendus. Avec le temps, on s'est aperçu que c'était inutile et que c'était mieux de miser sur la confiance* » (P2). De cette divergence résulte une tension entre le contrôle et la liberté, qui compare indirectement l'organisation à l'individu.

4.2. Les tensions

Au niveau **organisationnel**, un *misfit* au télétravail, mené par une ambiguïté des politiques adoptées, entraîne une incompréhension entre les gestionnaires et les télétravailleurs. Pour les gestionnaires, des politiques ambiguës engendrent une réticence à accorder une liberté aux télétravailleurs, car la sécurité informationnelle devient leur responsabilité immédiate. Pour les télétravailleurs, cette ambiguïté produit inversement une perception de liberté, qui est traduite par un délaissement organisationnel et qui permet l'adoption de comportements de sécurité non contrôlés. Cet élément de *misfit* produit une incohérence organisationnelle, traduite par une tension entre le **contrôle** et la **liberté**. « *Avec le temps nous nous sommes aperçus qu'elles [les mesures de contrôle] étaient inutiles et qu'il était beaucoup mieux de bâtir une organisation du travail basée sur la confiance et la flexibilité.* » (P2). L'inconnu associé au télétravail a incité les organisations à faire de l'essai-erreur, comparant de façon itérative les conséquences des politiques adoptées sur les tensions résultantes. « *Au début [de la pandémie], nous ne savions pas ce qu'étaient les mesures appropriées, nous faisions de l'essai-erreur. Chaque semaine, il y avait de la nouveauté* » (P1). Le processus d'essai-erreur admet, en soi, un risque pour la sécurité informationnelle puisqu'il implique la mise à l'épreuve de nouvelles procédures et l'introduction de nouvelles technologies peu testées préalablement. Bien que cette approche ait des bénéfices à long terme, elle ouvre des points de vulnérabilités des systèmes informatiques, généralement imprévus à court terme. Par

exemple, le partage d'informations confidentielles sur *Teams*, *Slack* ou *Outlook*, était une vulnérabilité admise par l'introduction généralisée de ces trois plateformes. Pareillement, l'adoption des VPN, qui permettent aux télétravailleurs de se connecter sécuritairement au réseau de l'organisation, a souvent mené à de mauvaises configurations, comme des mots de passe inadéquats, et conséquemment à une vulnérabilité accrue des connexions établies. Néanmoins, l'essai-erreur a admis une décentralisation des procédures de sécurité adoptées en télétravail, qui a été fortement appréciée des gestionnaires. « *Le fait de ne pas avoir une politique centralisée, c'est très accommodant puisque nous pouvons adapter les conditions de travail à notre équipe en particulier* » (P2). Des politiques organisationnelles sévères et centralisées mettent en péril la pérennité des ressources humaines, par un mécontentement des télétravailleurs, alors qu'elles ne sont pas suffisamment adaptées à la réalité des équipes de travail. Une politique décentralisée, en revanche, a une incidence mitigée sur la sécurité informationnelle puisqu'elle responsabilise les équipes (*incidence positive*), mais engendre également un élément de complexité dans l'introduction de nouvelles procédures, lorsqu'il est nécessaire de les adopter rapidement, comme en contexte de crise (*incidence positive*). Dans notre étude, la majorité affirme que les organisations étaient centrées sur la flexibilité, en période d'adoption forcée du télétravail, et donc sur une politique décentralisée, allouant une accommodation aux individus : « *Si j'ai un rendez-vous, il n'y a pas de problème que je m'absente, tant que l'équipe est avisée. Je peux reprendre mes heures plus tard et ma gestionnaire est très compréhensive* » (P9) ; cette flexibilité a souvent résulté en des abus de confiance par les télétravailleurs, qui incitent les organisations à augmenter leur contrôle par une politique de retour au présentiel, à une certaine fréquence hebdomadaire, en période de post-adoption forcée. Cependant, cette période est définie par une volonté des individus à maintenir leur liberté initialement promue, ce qui inflige une réalité organisationnelle, où le télétravail est perçu, comme une norme sociétale. « *Il y a une grande résistance à revenir au bureau. Pourquoi devrais-je me déplacer au bureau si au final, je fais les mêmes tâches qu'à la maison?* » (P11). Une telle divergence d'intérêt détient une incidence sur la sécurité informationnelle, alors qu'elle entraîne une diminution de collaboration entre les employés et l'organisation. Si une organisation maintient une politique forcée de retour au présentiel, malgré un *fit* des employés au télétravail, cela détiendra un impact négatif sur le bien-être

des individus, qui seront mécontents des mesures adoptées par l'organisation et adopteront des comportements indésirables à l'égard du traitement informationnel.

Au niveau du **groupe**, « *le côté qui manque en télétravail, malheureusement, c'est le côté social. Tu ne peux pas répliquer les interactions occasionnelles qui se produisent en personne* » (P2). Pour être *fit* au télétravail, une équipe doit être synergique, engageant tous les membres dans l'accomplissement d'une vision commune. Or, en travaillant à distance, établir cette synergie est complexe puisque les individus ressentent moins les sentiments d'appartenance et d'imputabilité envers leurs collègues, comparativement à un mode de travail en présentiel. De ce *misfit* résulte alors une tension entre le **collectivisme** et l'**individualisme**, qui régissent les interactions intragroupes, entre les membres d'une même équipe et les interactions inter-groupes, entre les membres de différentes équipes. De cette perspective, nos résultats sont fortement partagés, alors que près de la moitié des participants soutient la présence de collectivisme, au sein de leur équipe de télétravail. Pour ces participants, la proximité attribuée à l'amélioration des moyens de communication, par une numérisation des outils de travail, permet un renforcement de la collaboration et de la communication entre les équipes d'une même organisation. « *Dans les appels par vidéoconférences, on inclut facilement un plus grand nombre d'individus, alors qu'en présentiel, nous sommes généralement timides de socialiser au-delà de notre cercle de contacts immédiats* » (P10). L'introduction de ces outils technologiques, relatifs à l'adoption forcée du télétravail, augmente l'efficience des rencontres intraéquipe en réduisant l'utilisation des ressources organisationnelles. « *La collaboration est mieux. En présentiel, il fallait se déplacer d'une salle à un autre. Le matériel n'était pas toujours adéquat, on ne pouvait pas démontrer certains avancements de projets. À la limite, les notes des rencontres se faisaient sur un papier avec un crayon. Alors que maintenant il est facile de simplement enregistrer la rencontre au nécessaire, de partager ton écran et de laisser ton interlocuteur prendre le contrôle à distance. Il y a moins de limites* » (P8). Une communication efficace, admise par la numérisation des outils de travail, permet aux professionnels TI d'obtenir les renseignements nécessaires sur les activités des différentes équipes de travail, ce qui facilite la gestion des risques de sécurité informationnelle. Ces professionnels peuvent rapidement détecter les incidents, ce qui minimise généralement les dommages causés par une tentative d'infiltration et permet une transversalité du savoir-

faire, qui facilite la sensibilisation des individus aux meilleures pratiques, ainsi que la promotion d'une culture de sécurité. Pour certains, cependant, la réalité est différente alors que le télétravail est plutôt considéré comme un amplificateur d'individualisme dans leur équipe respective. Pour ces individus, la distance psychologique détient un facteur déterminant sur la synergie d'équipe et ne peut pas être améliorée par la numérisation des outils de travail. P6, par exemple, qui travaille continuellement avec des équipes changeantes, soutient que « *[le niveau de collectivisme] dépend des équipes. Dans les cas, où nous travaillons avec des équipes qui se trouvent à l'autre bout du monde, nous sentons plus d'individualisme. Alors qu'au sein des équipes, avec lesquelles nous nous trouvons dans la même ville, plus de collectivisme* » (P6). Cet argumentaire supporte notre modèle initial, qui soutient l'importance de la distance perçue entre les membres d'un groupe dans l'accomplissement à succès d'un projet commun. Les individus coopérant à une distance psychologique moindre auront davantage d'incitatifs à collaborer, car les sentiments d'imputabilité et de redevance sont plus importants. Surtout en adoption forcée du télétravail alors que l'impact de l'isolement social est aggravé par le contexte de crise. Le télétravail est perçu par plusieurs comme un facilitateur du travail en silo, traduit par une diminution de la communication et de la participation active. « *Pour ce qui est de la collaboration, nous travaillons chacun de notre côté et nous compilons nos résultats pour le projet en entier, quand tout est complété* » (P4). La distance physique peut avoir un impact dominant sur l'individualisme et la sécurité informationnelle, étant donné que les technologies actuelles sont insuffisantes pour reproduire le contexte véhiculé par le non verbal d'une communication que cela limite la transversalité du savoir-faire, présenté précédemment. Lorsque les équipes sont dispersées géographiquement, il est plus difficile de coordonner les efforts de sécurité, en raison de la nécessité de traduction du matériel de sensibilisation en plusieurs langues et d'adaptation des normes de sécurité aux différentes législations gouvernementales, tout en assurant une cohérence organisationnelle. En ajout à ces éléments, l'individualisme, qui résulte de la distanciation, freine le développement de l'esprit d'équipe et nuit aux télétravailleurs du point de vue de l'isolement social et du bien-être : « *En télétravail, surtout lorsque nous travaillons séparément, je me sens seul. Certes, nous avons des appels une fois par mois, mais ce n'est pas suffisant pour apprendre à connaître tes collègues et briser cette formalité* » (P5).

Au niveau **individuel**, des conditions de télétravail restrictives suscitent une inquiétude en matière d'épanouissement des télétravailleurs. Ces conditions sont influencées par le *misfit* organisationnel et produisent une tension opposant le **mal-être** au **bien-être** des individus. « *Je suis persuadé que nous préférons le télétravail à court terme, mais qu'à long terme, on se sent plus fatigués, l'épuisement professionnel s'installe et on se sent moins bien* » (P10). En période de préadoption forcée, le télétravail était un privilège, un élément novateur et excitant. En période de post-adoption forcée, cependant, cette perception est altérée par une incidence négative du télétravail sur l'isolement social et la démotivation professionnelle. Pour certains, la possibilité de fréquenter le bureau constitue une opportunité de « *changer d'air* » et s'avère être essentielle pour le bien-être individuel. « *Le fait de rester à la maison, ça me fait sentir moche. Tu ressens une sorte de manque d'accomplissement, comme si ton travail était invalidé par le fait que tu es resté toute la journée en pyjama* » (P6). Pour les individus, dont l'état émotionnel est altéré par l'adoption forcée du télétravail, on note une moindre concentration au travail et une augmentation inévitable du volume d'erreurs quand ils utilisent les systèmes informatiques de l'organisation. Les sentiments d'insatisfaction et d'isolement augmentent alors, considérant la diminution des contacts sociaux, et accroissent la vulnérabilité des télétravailleurs vis-à-vis les tentatives d'hameçonnage, car ils sont enclins à interagir avec des malfaiteurs en ligne. Les sources d'interférence avec la vie personnelle, comme les enfants, les animaux, les tâches ménagères et les bruits environnants, renforcent cette susceptibilité. Voilà pourquoi, comme présentée précédemment, une délimitation entre le travail et le domicile est nécessaire en contexte d'hyperconnectivité technologique. « *Une amie, qui travaille régulièrement avec des partenaires externes, m'a raconté que son organisation impose qu'elle soit disponible pour répondre aux questions, peu importe l'heure à laquelle elle est contactée* » (P12). Caractérisé par une adoption hâtive du travail à distance, ce manque d'étiquette est traduit par des comportements similaires à ceux sur les réseaux sociaux, soit des contacts à des heures irrégulières, une anticipation de réponses rapides et une accentuation du sentiment d'anxiété. « *Maintenant, tes collègues peuvent t'écrire en soirée, même en fin de semaine et tu pourrais être tenté d'aller consulter ces messages. C'est dur de faire cette séparation* » (P2). L'hyperconnectivité en télétravail est un élément aggravant la sécurité informationnelle, car elle implique que les individus soient

connectés à des heures et des endroits non sécurisés et utilisent leurs appareils personnels. Cette hyperconnectivité implique aussi une complexification du travail des professionnels TI alors qu'ils doivent contrôler les accès aux serveurs dans des périodes inhabituelles.

4.3. Les mécanismes de gestion

Dans notre étude, quatre mécanismes de gestion ont été répertoriés, à savoir la politique de gouvernance des données, les meilleures pratiques, la culture de sécurité informationnelle au niveau du groupe et l'adaptation individuelle. Nous sommes venus à conclure que, bien d'entre elles, sont implantées exclusivement de façon réactive, alors qu'en sécurité informationnelle, l'importance d'introduire une proactivité est une notion critique. « *On reçoit les courriels de rappels des bonnes pratiques seulement après un événement, comme la réception d'un courriel d'hameçonnage* » (P9). Tout de même, les quatre mécanismes ont été retenus en raison de leur impact sur la sécurité informationnelle de l'organisation.

Au niveau **organisationnel**, les participants nous indiquent la présence d'un mécanisme de gestion, soit la gouvernance des données[3]. Une gouvernance des données adéquate permet de mitiger la tension organisationnelle, car elle rend les mesures de sécurité adoptées moins intrusives, ce qui réduit le sentiment de contrôle éprouvé par les télétravailleurs. Quand la sécurité informationnelle est traitée dans un respect de l'autonomie individuelle, les normes introduites sont moins coercitives et mieux reçues, réduisant ainsi la divergence des intérêts dans l'organisation. « *Au début, quand nous n'avions pas de directives claires à l'égard de mesures de sécurité à appliquer dans nos codes, je ne me sentais pas à l'aise de prendre ces décisions tout seul* » (P11). En établissant des politiques et des normes pour minimiser les risques, les organisations peuvent donner aux individus une confiance et une sécurité dans l'exécution de leurs tâches, ce qui est souvent nécessaire en contexte d'isolement social, comme celui associé à l'adoption forcée du télétravail. Une négligence de la gouvernance des données, d'autre part, accroît l'incidence de l'adoption forcée par une augmentation du risque relatif au facteur humain : « *Les politiques varient d'une équipe à une autre et je crois que c'est pour ça qu'on voit des comportements illicites qui sont*

[3] La gouvernance des données réfère à « *l'exercice de l'autorité et du contrôle sur la gestion des données* » Abraham, Rene, Johannes Schneider et Jan Vom Brocke (2019). « Data governance: A conceptual framework, structured review, and research agenda », *International journal of information management*, vol. 49, p. 424-438..

parfois tolérés » (P1) ; et par une décentralisation des normes de sécurité : « *Quand nous développions des outils, nous n'avions pas de directives claires en matière de sécurité informationnelle. Nous ne savions pas ce qui était permis et ce qui ne l'était pas. Toute la gestion des accès était une décision libre aux développeurs* » (P8). En santé, par exemple, où l'accessibilité est une dimension essentielle de la sécurité des données, une gouvernance adéquate assure la pérennité des opérations de l'organisation et sauve littéralement des vies. « *Dans notre industrie, nous devons protéger nos serveurs pour la sécurité de nos patients. Lorsqu'on parle de médicaments à administrer ou de fonctionnement des appareils médicaux, nos systèmes informatiques doivent demeurer toujours fonctionnels* » (P2).

Les participants notent également que la gouvernance des données est devenue davantage transparente en période d'adoption forcée du télétravail. Effectivement, il paraîtrait que les organisations dévoilent plus couramment aux employés les tentatives d'infiltrations qui ont été menées à l'égard de leur organisation. Que ce soit à travers un courriel ou une note de service, le fait de divulguer ouvertement ces événements témoigne d'une transparence, qui est nécessaire à l'amélioration de la sécurité informationnelle. « *[Depuis que j'ai été mis au courant de la cyberattaque dont mon organisation a été victime], je suis beaucoup plus aux aguets des tentatives. Vu l'augmentation du volume d'échanges en ligne, nous sommes continuellement exposés à des risques, alors on y pense au quotidien* » (P12). Cependant, peu de participants associent ce changement directement à l'adoption forcée du télétravail et croient plutôt qu'il résulte du volume croissant de tentatives d'infiltrations des systèmes informatiques. « *Je pense que c'est plutôt la croissance du nombre d'attaques qui a poussé la transparence de l'organisation à cet égard et pas vraiment le télétravail* » (P1). Cette perspective produit une piste intéressante, complétée d'un élément justificatif, soulevé par P11 : « *je ne crois pas que ça soit directement lié au télétravail, mais plutôt à une réalité générationnelle. Cette génération [< 32 ans] est tellement exposée aux risques, qu'ils étaient déjà très alertes à ce niveau* » (P11). Cette réalité générationnelle, traduite par une familiarité vis-à-vis l'utilisation informatique, agit à titre de mécanisme de gestion en soi, sur lequel les organisations ne disposent pas de contrôle. Certes, ils déploient un effort de sélection des candidats, au moment de l'embauche, mais admettent qu'il ne s'agit pas d'un facteur de qualification indispensable, alors que « *notre problème central est le manque de socialisation entre télétravailleurs et la hausse du taux de roulement* » (P2), ce qui explique

pourquoi les compétences de communication, de collaboration et de socialisation sont plus en demande que les compétences informatiques.

Au niveau du **groupe**, les participants nous indiquent la présence de deux mécanismes de gestion, à savoir les meilleures pratiques et la culture de sécurité. Les meilleures pratiques forment l'ensemble des normes et des directives qui sont introduites pour assurer la sécurité informationnelle au sein d'une organisation. Pareillement à la gouvernance de données, cet ensemble est un complément à la stratégie généralisée de sécurité informationnelle, adoptée au niveau stratégique. À travers les réponses de nos participants, nous recensons quelques meilleures pratiques, dont la non-divulgation des mots de passe et le respect des termes de confidentialité, promues grâce à différents outils, comme les formations : « *côté formation, nous sommes très chargés […] nous avons des vidéos récurrentes et des vidéos non récurrentes, tout dépendamment de l'utilité de la question de sensibilisation. Après chacune de ces vidéos, nous avons des tests, qui sont assez difficiles à compléter* » (P10) ; les certifications : « *nous avons des certifications annuelles et des formations récurrentes sur l'importance de la protection des données des clients* » (P3) ; des lectures informatives : « *il s'agit des lectures [de sensibilisation] que l'employé devait faire dans son temps de travail* » ; et des tests d'hameçonnage : « *ils envoient beaucoup plus de tests d'hameçonnage par courriel [qu'avant]* ». Les tests d'hameçonnage sont une méthode d'identification des maillons faibles en sécurité des données, soit les individus vulnérables aux *phishing attacks* et qui nécessitent un encadrement supplémentaire. Ces tests sont généralement menés sur une base récurrente ou avant une formation spécifique, pour cadrer ces maillons faibles et offrir un apprentissage personnalisé, en fonction des compétences individuelles. « *Une fois par mois, nous avons de fausses tentatives de phishing. Au début, je me faisais prendre quelques fois et, en réponse, mon gérant m'envoyait en formation* » (P3). Quand elles sont adéquatement implantées, les meilleures pratiques permettent de renforcer le collectivisme des groupes par l'établissement d'une confiance entre les membres qui les composent. Elles favorisent une culture de responsabilité partagée, où chaque individu est impliqué dans les enjeux de sécurité informationnelle et où tout le monde contribue à sa protection. Quand les pratiques sont contraignantes ou intrusives, les individus se sentent surveillés et limités dans leur capacité à communiquer et travailler efficacement. Un rapport coercitif s'établit, entre les télétravailleurs et les gestionnaires

intermédiaires, affectant ainsi la collaboration individuelle, par crainte de représailles de non-respect des normes préétablies.

Ceci nous amène donc à considérer notre second mécanisme de gestion, recensé au niveau du groupe : la culture de sécurité[4]. Le rôle des groupes dans le développement d'une culture de sécurité informationnelle à l'échelle de l'organisation est indéniable et les gestionnaires en sont conscients. « *Présentement, l'effort d'établissement de la culture de sécurité repose entièrement sur la direction, mais je comprends qu'il s'agit également de ma responsabilité et que je devrais en faire plus* » (P2). Cette responsabilisation à un niveau granulaire réduit l'incidence des conséquences de l'adoption forcée du télétravail par une conscientisation accentuée des individus alors que le sentiment d'imputabilité individuelle est élargi par un environnement de proximité, comme celui d'une équipe. La culture de sécurité, qui résulte de cette proximité, contribue à réduire l'individualisme des membres puisqu'elle accroît la communication, la confiance, l'inclusion et l'engagement individuel vis-à-vis les activités de sécurité des données. Fréquemment, les participants accusent ces activités de « *banaliser l'importance de la sécurité informationnelle, car les notions présentées sont évidentes* » (P6), ce qui réduit inévitablement la pertinence des efforts de sensibilisation. Cet argument fut soulevé à plusieurs occasions alors que les participants, qui témoignent d'une aisance informatique dans le cadre de leurs obligations professionnelles, ne voient pas l'utilité des activités concernées. « *Étant donné que je suis dans le domaine des TI et que je suis à la base de nature très sceptique, je ne crois pas que le télétravail a eu un impact sur ma sensibilisation* » (P3).

Au niveau **individuel**, les réponses des participants formulent un mécanisme de gestion, soit l'adaptation individuelle[5]. Ce mécanisme exerce un rôle déterminant sur les attitudes, les comportements et les motivations intrinsèques des individus puisqu'il impacte le degré de *fit*, les tensions et les conséquences de l'adoption forcée du télétravail sur la sécurité des

[4] La culture de groupe réfère aux « *systèmes de connaissances, de croyances, de comportements et de coutumes partagés entre les membres d'une équipe, auxquels ces derniers peuvent se référer et utiliser comme base pour une interaction ultérieure* » Fine, Gary Alan (1979). « Small groups and culture creation: The idioculture of little league baseball teams », *American sociological review*, vol. 44, no 5, p. 733-745.
[5] L'adaptation individuelle réfère aux « *actes performés par les utilisateurs pour faire face aux conséquences perçues, résultantes d'une adoption technologique* » Beaudry, Anne et Alain Pinsonneault (2005). « Understanding user responses to information technology: A coping model of user adaptation », *MIS quarterly*, p. 493-524.

données. Un individu qui maîtrise les défis du télétravail, par une adaptation individuelle, sera disposé à favoriser son implantation en premier lieu. Cet individu sera plus susceptible de trouver cette forme de travail confortable et efficace, ce qui peut se traduire par une plus grande satisfaction au travail, une meilleure productivité et, inévitablement, l'adoption de comportements favorables à une sécurité informationnelle adéquate. Il sera également plus apte à comprendre les outils et les technologies introduites en télétravail, ce qui réduira son niveau de « *technostress* » et améliorera subséquemment son bien-être. Dans notre étude, tous les participants affirment avoir eu recours à des mécanismes d'adaptation, comme des pauses obligatoires : « *Avec ma copine, vu que nous sommes tous les deux en télétravail, nous prenons des pauses ensemble alors ça recrée cette ambiance de bureau. Nous essayons de ne pas parler de travail pendant ces pauses pour nous détacher pour 15 minutes. »* (P10) ; des marches à l'extérieur du domicile « *En télétravail, au lieu de prendre la voiture, je profitais de mes déplacements nécessaires pour prendre l'air. Alors je marchais plus souvent* » (P3) ; de l'entraînement physique « *Grâce au télétravail, je fais plus d'activités physiques parce que le temps que je sauve sur le déplacement, je peux l'allouer dans l'entraînement. En retour, cet entraînement me permet de mieux me sentir* » (P12) ; et des événements entre amis en soirée « *Je vais m'organiser des activités sociales après le travail, je vais faire plus d'activités physiques, je vais m'habiller proprement, même si je reste à la maison […]* » (P6).

4.4. Les conséquences

Les conséquences sur la sécurité informationnelle, qui découlent du *misfit* au télétravail et qui furent recensées dans le **Tableau 3**, ont été adaptées aux réponses de nos participants. Ainsi, similairement aux constats précédents, nous notons une variance des conséquences en fonction du secteur d'activités d'une organisation alors que les individus qui proviennent d'un secteur bureaucratique dénotent une numérisation des outils davantage importante que les individus qui dérivent d'autres secteurs. « *Non, vu qu'on est dans une organisation où le télétravail était déjà adopté, tout était déjà en place même avant la transition* » (P4). Nos participants mentionnent également que la virtualisation des formations, qui était liée supposément à l'adoption forcée du télétravail, était en fait établie même avant la pandémie. « *Dans notre cas, c'était plutôt la fuite de données de [nom de l'organisation],*

qui a incité notre organisation a rendre les formations plus accessibles, en faisant des capsules vidéo et des pages Sharepoint sur la sécurité des données » (P10). Ces découvertes nous mènent donc à négliger ces conséquences dans notre modèle conceptuel amélioré puisqu'elles sont ultimement liées à d'autres phénomènes que l'adoption forcée du télétravail.

Au niveau **organisationnel**, les participants nous indiquent la présence d'une conséquence qui résulte d'une gouvernance des données inadéquate : des procédures de sécurité qui sont inadaptées aux réalités du télétravail. Des procédures inadaptées détiennent une incidence négative sur le roulement organisationnel, car les individus sont mécontents des modalités restrictives. Il est important de comprendre que la liberté du télétravail, admise au début de l'adoption organisationnelle, est dorénavant perçue, par les individus, comme une norme sociétale préétablie. « *On plaisante parfois que, si jamais ça revient à cinq jours de travail en présentiel, je vais probablement quitter l'organisation. Pour moi, retourner en arrière, jamais* » (P2). Les participants justifient ce phénomène de démotivation par des facteurs, comme l'épuisement professionnel : « *On remarque que, sur du long terme, les burnouts augmentent beaucoup et le taux de roulement est élevé* » (P10) ; l'inefficacité de l'intégration : « *j'ai changé d'emploi en pandémie et j'avais peur de ne pas être inclus dans les gangs* » (P4) ; et le manque de proximité au travail : « *Le ¾ de mon équipe, je ne les ai jamais vus* » (P8). D'ailleurs, il advient qu'un de nos participants a quitté son organisation, en période d'adoption forcée du télétravail, sous l'effet de « *deadlines trop lousses et d'un manque d'implication du gestionnaire* » (P4). Il affirme explicitement que « *c'est une des raisons qui a motivé cette décision* » (P4). Un taux de roulement élevé détient un impact négatif sur la sécurité informationnelle, alors qu'il est difficile de maintenir une culture de sécurité, à long terme, qui assure que tous les employés soient conscients des protocoles établis dans une organisation. Les nouveaux arrivants sont généralement prônes aux erreurs humaines et les anciens, qui quittent l'organisation, emportent des données confidentielles. Pour mitiger ces risques, les organisations édifient des procédures de sécurité strictes, qui sont axées sur la supervision et le contrôle. Cependant, il en dérive généralement une sous-conséquence, traduite par une divergence des intérêts dans une organisation. Par exemple, avec l'allégement des mesures de distanciation obligatoire, relatives au contexte de crise, les organisations promeuvent dorénavant un retour forcé au présentiel, en instaurant un

modèle de travail *hybride*, qui conjugue le télétravail au présentiel. Des politiques sont alors émises pour inciter un retour au bureau, à une fréquence moyennant deux fois par semaine, ce qui ne fait pas l'unanimité au sein des télétravailleurs : « *d'après un sondage effectué par notre gestionnaire, seulement cinq personnes sur dix-sept étaient en faveur du deux fois par semaine* » (P10). Un renforcement de contrôle, comme le retour au présentiel, a un impact négatif sur la sécurité informationnelle puisqu'il oblige les télétravailleurs à déplacer leurs matériels informatiques, contenant des données confidentielles, d'un endroit à un autre, ce qui produit un risque de vol ou de perte informationnelle. L'instauration du modèle hybride produit également une insatisfaction des télétravailleurs, qui les incitent à perpétrer des actes de malveillance, d'omettre les normes de sécurité et d'adopter des comportements illicites. Il est donc nécessaire, au niveau organisationnel, de promulguer des procédures de sécurité qui sont adaptées aux réalités du télétravail, afin de maximiser la satisfaction des individus tout en respectant les objectifs organisationnels.

Au niveau de **groupe**, les participants soulèvent une conséquence qui résulte des tensions, soit l'émergence d'une gestion transactionnelle dans leur équipe de télétravail. Bien qu'elle alloue une liberté considérable, la gestion transactionnelle accentue aussi l'individualisme dans les équipes concernées. « *En télétravail, il y a une peur de déranger les autres, surtout lorsque nous travaillons en silo. Il faut être proactifs pour cogiter avec nos collègues*. *Je pense que ça devrait être la responsabilité du gestionnaire de faire en sorte que tout le monde se sent inclus.* » (P11). P8 soutient notamment que cette forme de gestion impose souvent une charge de travail excessive, qui ne considère pas les contraintes de faisabilité. « *Cette liberté vient certainement avec une forme de délaissement du gestionnaire. Je crois que c'est la mentalité du télétravail. "Moi je t'ai donné cette liberté, tu gères ton horaire et le reste ne m'appartient pas."* » (P8). Caractérisé par une supervision diminuée, ce délaissement fut également considéré par cinq autres participants. Or, lorsque les individus sont moins surveillés, cela peut aussi mener à l'adoption de comportements illicites, car ils ressentent moins les effets coercitifs d'un environnement de travail traditionnel. « *Je crois qu'en télétravail, loin des yeux de ses collègues et des gestionnaires, il est naturel pour des gens d'être moins freiné à adopter un comportement illicite, comme jeter un coup d'œil à de l'information sensible* » (P4). La gestion transactionnelle mène parfois à une négligence des protocoles de sécurité informationnelle, alors que les individus sont encouragés à se

concentrer uniquement sur l'accomplissement de leurs tâches professionnelles. Ils peuvent donc négliger des activités qui sont nécessaires au maintien de la sécurité, comme la mise à jour de logiciels, la protection de mots de passe et le transfert sécuritaire de données sensibles. « *Nous avons un portail, développé par le TI, que nous devons utiliser pour transférer des documents confidentiels, mais personne ne l'utilise, parce qu'il est trop lent* » (P6). Ce problème est inhérent au télétravail, alors que plusieurs outils déployés par les équipes TI, en adoption forcée, nécessitent une attention supplémentaire avant d'être intégrés dans les procédures organisationnelles. Dans le cas de l'organisation de P6, la lenteur du portail de transfert de documents incite les travailleurs à trouver des moyens plus rapides et pratiques, mais généralement moins sécuritaires.

Au niveau **individuel**, les participants nous indiquent la présence de deux conséquences introduites par une adaptation individuelle insuffisante, soit une interférence du télétravail et une distance psychologique. « *[En télétravail], il est facile de continuer de travailler. La pandémie a créé une sorte d'urgence qui n'est pas toujours nécessaire. Avant quand tu faisais ton 8 à 4, les gens faisaient véritablement leur 8 à 4* » (P2). Suscité par l'hyperconnectivité du télétravail, le défi d'établir une séparation entre les obligations professionnelles et personnelles devient davantage flou. Certains y perçoivent néanmoins du positif, alors que le travail à distance « *enlève un stress de savoir qu'on peut avancer dans nos travaux plus tard. En présentiel, je me sentais pressée de finir à l'intérieur des heures de bureau* » (P9). Le temps additionnel que passent les individus au travail accroît le sentiment d'épuisement et conséquemment l'éventualité d'une erreur humaine, qui pose un enjeu considérable pour la sécurité des données, qu'elle soit volontaire ou involontaire. Il se pourrait qu'un individu, croyant qu'il ne fait rien de mal, ne respecte pas les procédures de sécurité établies par une organisation en raison d'une concentration diminuée. Après tout, un geste aussi banal que l'utilisation d'un appareil personnel non sécurisé peut menacer la sécurité informationnelle d'une organisation. « *Nous n'avions pas de VPN, vu qu'on travaille principalement sur les réseaux des clients, on dirait que l'entreprise ne jugeait pas l'importance d'avoir un VPN. J'utilisais alors parfois mon Mac, vu que je suis plus confortable dessus* » (P4). Cet argumentaire soulève l'importance de former les employés sur les comportements à adopter en télétravail, de sorte à réduire l'impact des conséquences de l'adoption forcée du télétravail sur la sécurité informationnelle.

L'adaptation individuelle inadéquate semble également accroître la distance psychologique entre les individus, particulièrement s'ils proviennent de différentes équipes de travail. La distance psychologique peut se manifester par une démotivation, une diminution de qualité du travail, ou encore par une réticence à communiquer avec des membres de l'organisation, qui n'appartiennent pas à l'équipe immédiate d'un télétravailleur. Pour éviter cet effet, les individus doivent être proactifs dans la communication avec leurs collègues. « *Parfois, ma collègue et moi on fait juste s'appelle et on travaille chacune sur nos tâches, mais en se gardant en vidéoconférence en arrière-plan* » (P8). Or, comme mentionné précédemment, ce n'est pas tout le monde qui fait preuve de cette proactivité, ce qui impacte la perception de distance physique entre les individus. La distance psychologique a un impact important sur la sécurité informationnelle, car les individus en isolement sont plus vulnérables aux attaques de *phishing* et d'ingénierie sociale. Par exemple, un individu, qui travaille en silo, peut être davantage enclin à divulguer des informations confidentielles à un malfaiteur, qui se fait passer pour un collègue de travail, alors que l'individu n'est pas habitué à échanger via télécommunication.

4.5. Développement du modèle conceptuel amélioré

Les résultats des entrevues semi-structurées permettent de complémenter notre conception de l'impact des conséquences de l'adoption forcée du télétravail sur la sécurité des données d'une organisation. Ce chapitre développe donc une évolution du modèle initial, avec des éléments d'amélioration provenant des informations collectées auprès des participants. Ces éléments seront élaborés en détail dans la discussion des résultats, présentés au cinquième chapitre de ce mémoire, en respect à la méthode de « *pattern matching* » (Sinkovics, 2019).

4.5.1. Conceptualisation améliorée du *misfit*

Le *fit* est un élément fondamental en adoption technologique ou de processus respectif, tel que le télétravail. Il est défini comme étant un ensemble de facteurs qui dispose un individu, un groupe ou une organisation à favoriser l'adoption d'une nouveauté technologique. Dans notre conception initiale, son opposé, soit le *misfit*, n'était pas divisé par niveau d'étude, alors qu'il paraît maintenant évident qu'une telle distinction est nécessaire, car chaque niveau dispose d'une spécificité qui occasionne des tensions respectives. Au niveau du groupe, un *misfit* augmente l'individualisme qui régit les activités par une détérioration de

la communication et de la collaboration entre les membres qui le composent. Au niveau organisationnel, P2 établit une relation entre le *misfit* et le secteur d'activités d'une organisation donnée. Les organisations en santé, par exemple, qui ont traditionnellement une gestion inefficace du changement, possèdent un *misfit* plus considérable, que les organisations avancées technologiquement. Au niveau individuel, un contexte familial spécifique, comme la parenté, altère la performance et forme un facteur déterminant du *misfit* pour l'individu. Néanmoins, nous avons supposé initialement qu'une distinction par niveau d'étude n'était pas nécessaire en contexte d'adoption forcée puisque l'aspect obligatoire du contexte suggère une adoption forcée nonobstant des facteurs de *fit* des différents niveaux. Autrement dit, peu importe le degré de *fit* considéré, les individus, les groupes et les organisations doivent adopter le télétravail. Cependant, les réponses des participants nous permettent de comprendre que le *misfit* au télétravail impacte les tensions résultantes et que ces tensions agissent sur les mécanismes et les conséquences en sécurité informationnelle, de sorte à former une boucle itérative, telle qu'illustrée par les flèches du modèle.

4.5.2. Conceptualisation améliorée des tensions

Les tensions constituent les intrants de l'étape de *planification* du modèle d'évaluation des risques en sécurité informationnelle (*PDCA*). Cette étape identifie les risques qui découlent du *misfit* des trois niveaux d'étude et élabore un plan de mitigation grâce aux mécanismes de gestion disponibles. Comme dans notre conceptualisation initiale, trois tensions ont été évoquées : le *bien-être* et le *mal-être*, pour l'individu ; l'*individualisme* et le *collectivisme*, pour le groupe ; et le *contrôle* et la *liberté*, pour l'organisation. Ces tensions sont liées au *misfit* au télétravail, dont disposent les différents niveaux d'étude. Au niveau de l'individu, par exemple, nous dénotons l'influence du *misfit* sur le bien-être en télétravail. Cet effet est illustré par les flèches distinctives, qui relient le *misfit* aux différents éléments de tensions, présentés également par niveaux d'études. Des flèches lient également les mécanismes de gestion aux tensions, définies dans le présent paragraphe. Ainsi, cette relation indique que les tensions recensées, pour un niveau d'étude particulier, peuvent être mitigées par les mécanismes de gestion relatifs à ce même niveau. Par exemple, pour atténuer les effets du *misfit* sur l'individu et bonifier son bien-être en télétravail (*tension*), un télétravailleur doit

adapter son comportement (*mécanisme de gestion*) aux difficultés résultantes de l'adoption forcée du télétravail (*misfit*).

4.5.3. Conceptualisation améliorée des mécanismes de gestion

Les mécanismes de gestion, comme soulevés précédemment, constituent les outils qui sont disponibles pour diminuer les tensions résultantes du *misfit* au télétravail, pour les niveaux d'étude considérés. Ces mécanismes forment l'étape d'*action* du modèle *PDCA*, impliquant la mise en œuvre du plan de mitigation, qui est formulé à l'étape précédente. Notre modèle conceptuel amélioré introduit deux mécanismes de gestion supplémentaires, soit la culture de sécurité, au niveau du groupe, et l'adaptation individuelle, au niveau individuel. Dans ce contexte, l'adaptation individuelle réfère à un processus où les employés effectuent des actions pour relever les conséquences de l'adoption forcée du télétravail. Elle est nécessaire pour la pérennité organisationnelle, sur un horizon allant au-delà du contexte de crise, parce qu'un individu qui s'adapte accroît inévitablement les bienfaits du télétravail, comme une réduction de la distanciation et de l'interférence du télétravail. Cette adaptation pourrait hypothétiquement s'appliquer aux trois niveaux d'étude, mais les résultats de notre collecte de données sont limités à l'individu.

La culture de sécurité informationnelle, au niveau du groupe, est définie comme étant un ensemble de normes, qui régissent l'identité, la synergie et la composition d'un groupe. Ce mécanisme est soulevé par P2 qui considère sa nécessité dans un contexte de délaissement organisationnel et en adoption forcée du télétravail. « *Bâtir une culture du bas, vers le haut, au lieu d'attendre les directives* » (P2) (aussi nommée *bottom-up culture*). Comme dans le cas de *misfit*, cet élément de réponse est justifié par l'immaturité technologique de certains secteurs d'activités, comme la santé ou l'enseignement supérieur. De cette perspective, une culture de sécurité informationnelle au niveau du groupe exerce un rôle complémentaire à une culture organisationnelle et réduit les incidences qui résultent de l'adoption forcée du télétravail. Elle est particulièrement nécessaire lorsque les groupes sont dispersés du point de vue géographique, car elle comble les lacunes d'une culture organisationnelle, qui sont généralement nombreuses en contexte de télétravail. « *On ne socialise plus vraiment avec les autres départements, à moins que tu travailles sur un projet commun* » (P8). Considérant que le télétravail limite les interactions entre les différents départements, le

développement d'une culture de sécurité informationnelle, au niveau du groupe, devient plus significatif.

4.5.4. Conceptualisation améliorée des conséquences

Les conséquences constituent les extrants des deux étapes précédentes du modèle *PDCA*, alors qu'elles caractérisent la qualité du plan établi initialement et des actions entamées pour pallier les tensions. Il s'agit donc de l'étape de *révision*, où les organisations évaluent leur approche au télétravail et repositionnent leur plan, grâce à une boucle de rétroactivité des conséquences. La rétroactivité des conséquences est une idée soutenue par les réponses des nos participants alors qu'il s'agit de la capacité à altérer les résultats de la mise en place d'un processus, comme le télétravail, en utilisant les résultats des processus d'implantation précédents. Ces résultats disposent d'un impact itératif sur les mécanismes qui ont été optés initialement. Par exemple, un individu qui perçoit une hausse de la distance psychologique en télétravail (*résultat*) reconsidérera sa stratégie d'adaptation comportementale préalable (*mécanisme*). Une logique comparable est imputée aux organisations et aux groupes.

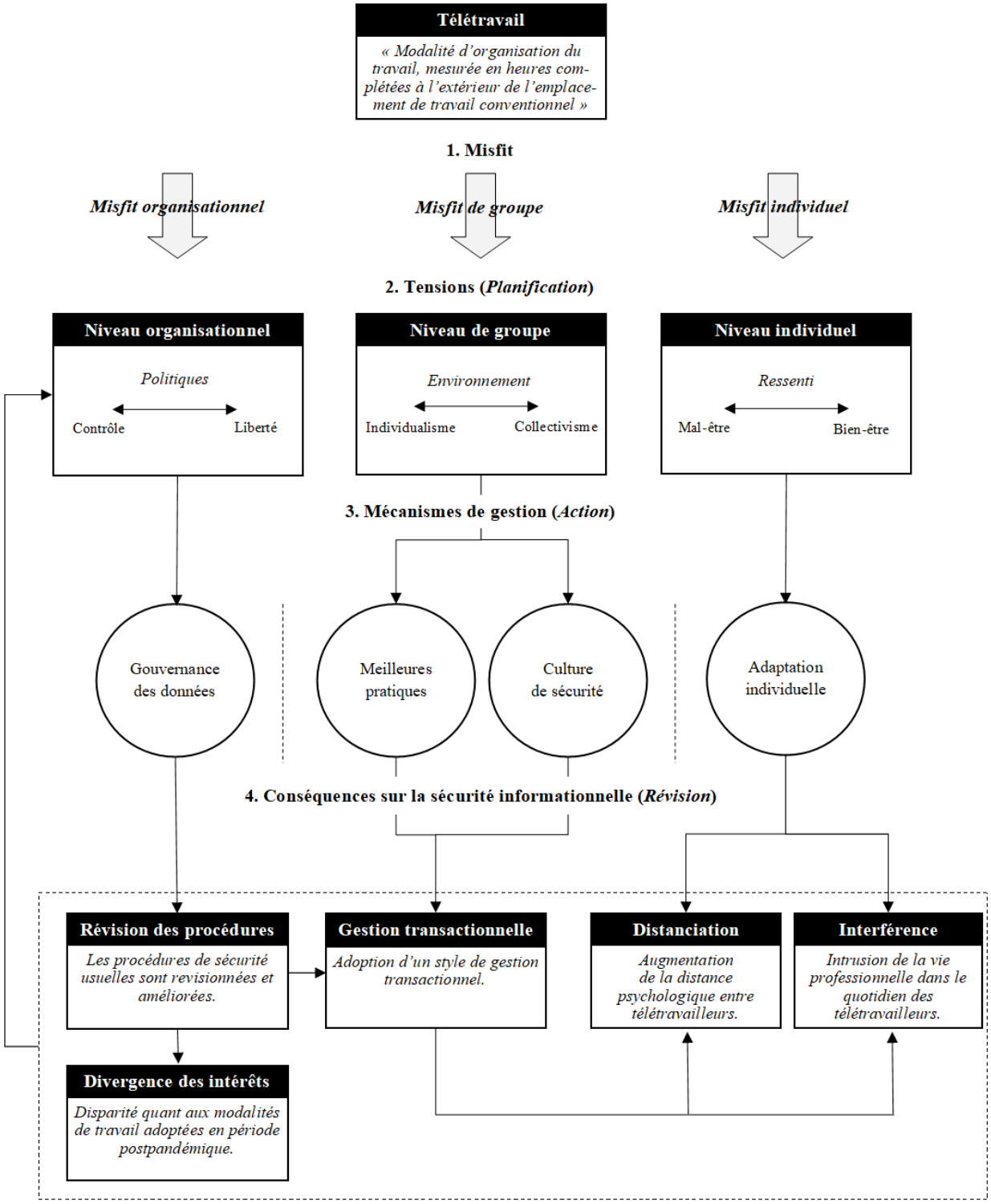
Notre modèle conceptuel amélioré exclut deux conséquences réfutées, soit la virtualisation des formations et la numérisation des outils. La numérisation des outils a été retirée, car les participants croient qu'elle était déjà fortement présente en période de préadoption forcée. « *Les technologies étaient déjà implantées. C'est plutôt l'utilisation qui était différente. Elle était moins fréquente* » (P11). De même, la virtualisation des formations a été écartée puisque, contrairement à la conjecture érigée par la littérature, quelques organisations ont entièrement négligé les activités de formation, en télétravail. « *Quand je suis arrivé dans ma nouvelle job, j'ai reçu l'ordi par la poste et une feuille qui illustrait comment configurer mon espace de travail virtuel, et c'est tout* » (P4). Les technologies d'apprentissage en ligne ont entraîné une baisse de la responsabilité organisationnelle en matière de formation des employées, ce qui mène à une diminution de la motivation individuelle, particulièrement lorsqu'un individu se joint à une entreprise. La procrastination s'installe alors et détient un impact négatif sur la sécurité informationnelle par une diminution de l'engagement et de la motivation de l'individu. « *[Il y a] les comportements inadéquats, comme partager son mot de passe avec un membre de la famille. À part former et sensibiliser les gens, les organisations n'ont pas de contrôle là-dessus* » (P9). La formation est une activité centrale

pour pallier le manque de sensibilisation des nouveaux employés, mais elle est bien souvent omise par les organisations en télétravail.

Notre modèle produit tout de même deux éléments de nouveauté, comparativement à notre modèle initial, soit l'interférence du télétravail, au niveau individuel, et la divergence des intérêts, au niveau organisationnel. L'interférence du télétravail réfère à la manière dont l'engagement dans un rôle spécifique, comme le télétravail, affecte négativement l'efficacité et la satisfaction liées à un autre rôle, comme la vie personnelle. La frontière entre les activités professionnelles et personnelles devient davantage floue en raison de l'hyperconnectivité qui est engendrée par le télétravail. « *La pandémie a créé une sorte d'urgence qui n'est pas toujours nécessaire* » (P2). D'autre part, la divergence des intérêts invoque la disparité, entre les trois niveaux d'étude, relative aux procédures de sécurité établies en période de post-adoption forcée. Cette période est marquée par la promotion du présentiel et de l'*hybride* alors que les organisations tentent d'inciter un retour forcé au présentiel, mais les individus ne partagent l'enthousiasme, alors que dans certaines équipes « *seulement cinq personnes sur dix-sept étaient en faveur du deux fois par semaine* » (P10).

Les réponses des participants indiquent aussi qu'il y a une relation d'interdépendance entre les conséquences recensées alors que les procédures de sécurité incitent généralement une gestion transactionnelle et que celle-ci détient un impact subséquent sur la distanciation et l'interférence du télétravail. Les participants soulèvent, qu'en adoption forcée du travail à distance, les procédures de sécurité misent sur le contrôle et l'achèvement des obligations professionnelles, plutôt que sur le développement des compétences, ce qui nuit à la qualité du milieu de travail. De ces procédures résulte une culture transactionnelle, qui émane une incidence négative sur la distanciation entre individus, car elle néglige les interactions sociales et augmente le sentiment de déconnexion des individus par rapport à leur équipe immédiate. Cette approche managériale peut également interférer dans la vie personnelle des individus puisqu'elle met l'accent sur la performance au détriment du bien-être et de l'équilibre des télétravailleurs. « *Moi je t'ai donné cette liberté, tu gères ton temps et le reste ne m'appartient pas.* » (P8). Les réponses des participants indiquent qu'ils se sentent souvent obligés de travailler des heures supplémentaires pour atteindre les objectifs et les attentes de leur employeur. « *[En télétravail], il est facile de continuer de travailler* » (P2).

Figure 6 Modèle conceptuel amélioré



5. Discussion des résultats

Contrairement aux préconceptions répandues dans la littérature associée au télétravail, bien des organisations allouaient cette modalité avant la crise pandémique (Desilver, 2020). La nouveauté fut plutôt observée au niveau de la démocratisation alors que maintenant tous les employés qui n'avaient pas besoin d'être en contact avec les clients pouvaient exercer leur travail depuis leur domicile. Notre étude exploratoire conçoit l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle en organisation qui requiert des études confirmatrices pour valider la conception théorique, présentée en **Figure 6**. Cette incidence est soulignée dans notre modèle, qui relie les concepts théoriques de *misfit*, de tensions, de mécanismes de gestion et des conséquences.

Au niveau du *misfit*, nous avons décelé une nécessité de considération par niveau d'étude, puisque les individus, les groupes et les organisations disposent de facteurs d'indisposition spécifiques à l'adoption du télétravail (Mokhtarian *et al.*, 1993). Pour les groupes, la composition, la synergie et la collaboration constituent des facteurs de prédisposition ; pour les organisations, le secteur d'activité et la culture organisationnelle ; pour les individus, les attitudes, les intérêts et le sociodémographique. Bien que l'aspect sociodémographique soit récurrent dans la littérature existante (Chung *et al.*, 2020), notre étude n'est pas en mesure de confirmer que le sexe ait une incidence sur la préférence du télétravail au détriment d'autres modalités. Il est tout de même inclus dans le modèle, car la présence d'enfants dans un ménage fut un thème soulevé par nos participants. Ultimement, le *misfit* mène à des tensions et des mécanismes de gestion respectifs. Pour l'individu, le *misfit* résulte en une tension opposant le mal-être au bien-être, qui est mitigée par l'adaptation individuelle ; pour le groupe, l'individualisme au collectivisme, qui est mitigé par la culture de sécurité et les meilleures pratiques ; pour l'organisation, le contrôle à la liberté, qui est mitigée par la gouvernance des données. Par exemple, malgré les défis associés au télétravail, les individus apprécient néanmoins cette modalité de travail, en raison de la commodité et de l'efficacité du bureau à domicile. Ils en perçoivent une amélioration de la qualité de vie, par une réduction du temps de déplacement, une attention portée aux proches et une hausse de productivité (Wang *et al.*, 2021). Cependant, ces bénéfices sont observés sur un court horizon temporel, alors qu'à long terme, nos participants affirment que des

sentiments d'isolement et de démotivation professionnelle s'installent tranquillement et impactent les comportements individuels vis-à-vis la sécurité des données. Ils peuvent négliger le respect des protocoles de sécurité, comme l'utilisation de mots de passe adéquats ou la mise à jour des logiciels de sécurité, et être moins vigilants dans la détection de menaces à la sécurité. Ils peuvent également fournir involontairement un accès aux données sensibles à des membres de la famille, des colocataires ou des visiteurs alors qu'ils échangent avec des collègues sur *Teams* ou qu'ils laissent leur ordinateur déverrouillé après avoir quitté leur poste de travail. Le télétravail peut poser des défis en termes de contrôle d'accès, considérant qu'il est plus difficile pour les équipes TI de contrôler les accès illicites. Le mécanisme de gestion individuel, soit l'adaptation individuelle, mitige ces tensions et atténue le mal-être en télétravail. Par exemple, un individu, qui adopte des pauses régulières pour atténuer les tensions résultantes du *misfit* au télétravail, réduit l'impact des conséquences de l'adoption forcée en socialisant davantage avec ses proches, ce qui diminue son sentiment d'isolement et favorise sa vigilance vis-à-vis la sécurité informationnelle.

Dans notre conception méthodologique, pour déceler les éléments d'incidence et répondre au « *pourquoi?* » (Whetten, 1989) l'adoption forcée du télétravail détient une incidence sur la sécurité informationnelle, nous avons entamé l'induction analytique. Aux termes de ce processus, nous avons noté une catégorie de risques strictement relative à l'adoption forcée du télétravail sur la sécurité informationnelle, à savoir le facteur humain. Les conséquences présentées dans cette étude relèvent de cette catégorie. Pour l'individu, une incidence est observée au niveau de l'interférence du télétravail, qui mène à la fatigue professionnelle et accroît l'éventualité d'une erreur humaine en sécurité informationnelle. Pour le groupe, une conséquence est observée par l'adoption d'une gestion transactionnelle des télétravailleurs, qui émane d'un contrôle diminué et des interactions ponctuelles. Une gestion transactionnelle mène parfois à des comportements illicites, comme les nombreux qui ont été préalablement énumérés. Pour l'organisation, un impact est recensé au niveau des procédures de sécurité et de la divergence des intérêts en post-adoption forcée du télétravail. Des procédures trop strictes incitent les individus à négliger les outils numériques déployés par l'organisation. Ces conséquences possèdent un effet rétroactif sur les mécanismes de gestion initialement adoptés, alors qu'un niveau d'étude qui perçoit un

impact des conséquences de l'adoption forcée du télétravail aura intérêt à reconsidérer sa stratégie de mitigation préalable.

5.1. Mécanismes de gestion

Notre conceptualisation initiale de l'incidence de l'adoption forcée du télétravail au niveau de la sécurité informationnelle conçoit une notion de dépendance entre les tensions et les mécanismes de gestion adoptés, mais omet une séparation distinctive des niveaux d'étude. Cette distinction est nécessaire puisque les tensions d'un niveau spécifique ne peuvent qu'être réduites par des mécanismes qui agissent au niveau d'étude considéré. Autrement dit, un individu ne peut pas influencer la gouvernance des données et une organisation ne peut pas obliger les télétravailleurs à adapter leur mode de vie au télétravail. Les réponses des participants nous ont donc mis à l'évidence que tous les niveaux d'étude disposent de mécanismes de gestion, qui leur sont spécifiquement attribués. Dans cette section, nous couvrons uniquement les mécanismes d'*adaptation individuelle* et la *culture de sécurité, au niveau du groupe*, car ils sont particulièrement pertinents dans le contexte de la question de recherche et contribuent grandement à la littérature académique existante. L'adaptation individuelle, par exemple, contrairement aux études préalables (Beaudry *et al.*, 2005), est élargie de sorte à englober la vie personnelle des télétravailleurs, en ajout aux difficultés qui résultent du télétravail.

5.1.1. Adaptation individuelle

L'introduction de nouveautés technologiques et de processus respectifs, comme l'adoption forcée du télétravail, mène à plusieurs conséquences imprévisibles dans l'environnement des individus concernés (Griffith, 1999). En adoption forcée, l'introduction de technologies de communication, comme *Teams*, *Slack* ou *Outlook*, produit des conséquences imprévues en sécurité informationnelle, sous l'effet de comportements illicites et de procrastination, qui démotivent les télétravailleurs. Considérant les investissements majeurs attribués à ce niveau, les organisations aimeraient prédire ces conséquences avant d'adopter lesdites technologies. Le degré de *fit* est généralement un bon prédicteur, mais sa variabilité produit un enjeu important pour les chercheurs, les gestionnaires et les professionnels TI (Beaudry *et al.*, 2005). Deux courants académiques sont alors formulés pour pallier cette complexité :

un premier, fondé sur la variance, et un second, sur le processus. Le premier est axé sur les éléments du *misfit*, qui formes les facteurs d'adoption, et sur l'utilisation d'une technologie donnée (Venkatesh *et al.*, 2003). Ce courant formule une réponse à pourquoi certaines des technologies, qui répondent à tous les besoins d'une organisation, ne sont ni comprises, ni utilisées en organisation (King et He, 2006). Ceci s'applique également aux technologies de sécurité, comme les VPN, qui ont été soulevés précédemment. Un individu, qui accède à des données organisationnelles et n'utilise pas un VPN sécurisé, produit une vulnérabilité informatique alors que l'information accédée peut être interceptée par des malfaiteurs. Ces facteurs d'adoption sont représentés dans le Modèle d'Acceptation Technologique (Davis, 1989), qui prédit la perception d'utilité et de facilité d'utilisation d'une technologie par ses utilisateurs [Annexe 12]. Bien qu'il soit largement utilisé, ce modèle contient des variables insuffisantes pour expliquer le phénomène considéré et doit éventuellement être complété de variables additionnelles, à savoir les conséquences, les précurseurs et le contexte d'une adoption technologique (Beaudry *et al.*, 2005). Dans notre étude, nous explorons les facteurs d'adoption, à titre de forces et de faiblesses, qui incitent les individus à favoriser l'adoption du télétravail et à minimiser les tensions résultantes (Mokhtarian *et al.*, 1993) L'accès au matériel de qualité, par exemple, constitue un facteur soulevé dans notre étude alors qu'un manque à ce niveau détient un impact négatif sur la sécurité informationnelle. Un individu qui utilise un appareil personnel dans le cadre de ses fonctions professionnelles nuit à l'organisation puisque ces appareils ne sont habituellement pas équipés de logiciels de sécurité adéquats et constituent des points de vulnérabilité au système informatique. Les facteurs d'adoption de sorte définissent la prédilection d'un individu à choisir le télétravail, au détriment d'autres méthodes d'organisation, lorsqu'un tel choix se présente.

Le second courant, fondé sur le processus de mitigation des tensions, introduit l'adaptation individuelle (Orlikowski, 1996) et son incidence sur les conséquences de l'adoption (Poole et DeSanctis, 1990). L'adaptation individuelle est définie comme « *les actes performés par les utilisateurs pour faire face aux conséquences perçues, résultantes d'une adoption technologique* » (Beaudry *et al.*, 2005). Elle est établie en deux étapes, soit l'évaluation des conséquences et l'adaptation comportementale. Les conséquences peuvent être, à la fois, des menaces et des opportunités, tout dépendamment de l'adaptation subséquente (Beaudry *et al.*, 2005). Par exemple, les individus, qui disent que le matériel informatique à domicile

est inadéquat pour correspondre aux normes de sécurité informationnelle de l'organisation (*conséquence*), exigent une compensation additionnelle dans le but d'aménager leur espace de travail à domicile (*adaptation comportementale*). Le processus d'adaptation commence lorsqu'un individu prend conscience des conséquences et les évalue conformément à leur pertinence à son égard (Folkman, 1992). Cependant, puisque tous les individus détiennent des facteurs de prédisposition variables, ce point de départ est également porté à varier, d'un individu à un autre. Certains vont altérer leur comportement avant l'occurrence même d'un événement, tandis que d'autres, uniquement au moment de subir les premiers effets (Beaudry *et al.*, 2005). Cette altération est d'habitude produite au niveau de l'engagement professionnel, des compétences, des aspirations, des croyances et des attitudes (Majchrzak et Cotton, 1988). Nous confirmons cet argumentaire puisque nous dénotons une certaine amélioration des compétences informatiques, auprès des participants interrogés, en réponse à l'adoption forcée du télétravail. Rappelons-le que pour minimiser les risques associés aux attaques d'hameçonnage, les organisations doivent entre autres développer les compétences informatiques des individus (Vayansky *et al.*, 2018), ce qui réduit nettement l'incidence des conséquences l'adoption forcée du télétravail sur la sécurité. Ce développement est le résultat d'efforts cognitifs et comportementaux, employés par les individus en contexte d'une stratégie d'adaptation à ces conséquences. Il existe deux types de stratégies : une, orientée sur l'émotion, et une seconde, centrée sur le problème (Beaudry *et al.*, 2005). Quand un individu minimise l'incidence de l'adoption forcée du télétravail sur l'isolement, nous considérons cet élément comme une stratégie d'adaptation émotionnelle, ayant pour objectif de préserver un état de tranquillité. Quand un individu emploie plutôt des actions spécifiques pour combattre l'isolement, par ailleurs, nous considérons cet élément comme une stratégie d'adaptation au problème, ayant pour cible de maximiser les bénéfices qui découlent du télétravail. Généralement, les deux stratégies sont employées subséquemment (Lazarus et Folkman, 1984). Au niveau de la sécurité informationnelle, cependant, seules les stratégies d'adaptation au problème sont pertinentes puisqu'elles produisent un résultat tangible, comme l'adoption des comportements aux enjeux du télétravail et le respect des procédures de sécurité établies par l'organisation.

En télétravail, l'adaptation individuelle est particulièrement pertinente puisqu'elle permet de mitiger les tensions qui influencent la sécurité informationnelle (*conséquences*) par des

mécanismes de gestion, au niveau individuel (*adaptation comportementale*). Notre étude déduit que le télétravail semble véritablement détenir un impact sur le bien-être individuel, car il renforce les rôles de genre traditionnels, affecte les relations professionnelles, accroît la démotivation et la procrastination au travail. Ce sentiment est éventuellement traduit par un épuisement au travail qui, en raison d'une concentration diminuée associée à la fatigue, peut diminuer la sécurité informationnelle au niveau de l'organisation. Les télétravailleurs peuvent être potentiellement distraits par les tâches domestiques, les enfants et les animaux, ce qui produit des erreurs de saisies de données et des décisions hâtives, qui compromettent la sécurité informationnelle. Il advient que certaines femmes interrogées éprouvent un sentiment de « *deuxième quart de travail* » alors qu'elles disposent de tâches domestiques plus nombreuses et importantes que celles de leur conjoint (Hochschild *et al.*, 1989). Toutefois, contrairement aux études préalables, nous n'avons pas noté de divergence au niveau de la prédilection au télétravail, basée sur le sexe (Bianchi *et al.*, 2012), car tous nos participants étaient initialement favorables à son adoption en organisation. Nous postulons que cela relève du fait que, dans la culture nord-américaine actuelle, les femmes détiennent des responsabilités domestiques plus partagées que dans les cultures qui étaient à l'étude préalablement (Bianchi *et al.*, 2012). Ceci étant dit, il est possible d'attribuer les conséquences de l'adoption forcée du télétravail à la distanciation entre les télétravailleurs (Lojeski *et al.*, 2008) alors que la distance diminue la qualité des relations professionnelles et augmente l'isolement social (Bavik *et al.*, 2020). Il paraîtrait même qu'un individu sur cinq n'aurait jamais rencontré son gestionnaire immédiat, lorsqu'en télétravail (Lojeski *et al.*, 2008), ce qui produit un parallèle avec les réponses de nos participants. Inévitablement, ces éléments détiennent une incidence sur la sécurité informationnelle, sous l'effet d'une baisse de communication entre individus, qui est non seulement nécessaire à l'instauration d'une culture de sécurité, mais qui permet aussi aux équipes TI d'avoir les renseignements nécessaires sur les activités des différents groupes.

5.1.2. Culture de sécurité informationnelle au niveau du groupe

La sécurité informationnelle doit être incluse dans la façon dont les choses sont faites au sein d'une organisation (Da Veiga *et al.*, 2010). C'est une caractéristique organisationnelle qui rassemble les individus autour de valeurs communes en gouvernance de données et qui

forment les comportements de sécurité au niveau de l'individu, de groupe et de l'organisation (Robbins, 2001). Dans notre étude, cependant, nous ne détaillons que la culture de sécurité informationnelle, au niveau du groupe, conformément aux réponses des participants à notre étude. Nous définissons cette culture comme « *systèmes de connaissances, de croyances, de comportements et de coutumes partagés entre les membres d'une équipe, auxquels ces derniers peuvent se référer et utiliser comme base pour une interaction ultérieure* » (Fine, 1979). Surprenamment, en contexte d'adoption forcée du télétravail, une culture de sécurité informationnelle au niveau du groupe est plus importante qu'une culture organisationnelle. Nos résultats nous démontrent que les individus accordent plus d'importance à leur équipe de travail immédiate, qu'à leur organisation, lorsqu'ils sont en télétravail. Nous postulons que cela relève du fait qu'ils collaborent plus souvent avec les individus qui forment cette équipe, à l'inverse d'individus qui proviennent d'autres départements et qui semblent loin. Comme mentionné préalablement, cette distance impacte la sécurité informationnelle, sous l'effet d'une diminution de la confiance entre les individus et d'une vulnérabilité prononcée aux attaques de *phishing*. Il existe quatre différents types de culture au niveau du groupe : autocratique, bureaucratique, orientée sur la tâche et individualiste (Da Veiga *et al.*, 2010). Dans une culture bureaucratique, par exemple, les individus ont une description explicite de leurs responsabilités et doivent se conformer aux normes préétablies vis-à-vis la sécurité informationnelle. Cela implique une définition des règles qui régissent les comportements et les attitudes des individus à cet égard, pour un groupe considéré. Il en résulte souvent une réticence en adoption du changement puisque le changement mène à une reformulation desdites règles et à une complexité respective. Similairement aux éléments préalables, ce constat théorique est soutenu par nos observations, qui suggèrent que les secteurs bancaires et publics, comme la santé, résident dans cette catégorie et furent réticentes à adopter le télétravail en premier lieu (Da Veiga *et al.*, 2010), ce qui s'est traduit négativement sur la sécurité informationnelle en contexte d'adoption forcée. Les organisations qui avaient déjà introduit le télétravail avaient probablement sensibilisé leurs télétravailleurs aux meilleures pratiques et aux comportements sécuritaires, ce qui a amélioré leur réponse en situation de crise.

Une culture de sécurité informationnelle au niveau du groupe est établie conformément aux comportements de ses membres et aux composantes environnementales qui influencent ces comportements [Annexe 3]. La gestion des utilisateurs est une composante qui produit une incidence sur la sécurité des données, au niveau du groupe, en deux volets : une *formation améliorée* et une hausse de la *confiance* intragroupe (Da Veiga *et al.*, 2010). La confiance, en contexte organisationnel, est définie comme « *la volonté d'un individu à être vulnérable aux actions d'un autre individu, en respect aux attentes d'engagements, sans supervision ni contrôle* » (Mayer, Davis et Schoorman, 1995). Quand les individus ont une confiance partagée, les normes de sécurité sont mieux assimilées et les comportements, ajustés à la vision de l'organisation (Martins et Elofe, 2002). En télétravail, les gestionnaires ont intérêt à forger des politiques flexibles pour que les valeurs organisationnelles demeurent intègres et crédibles auprès des télétravailleurs. Les procédures, comme le retour forcé au présentiel, briment certainement cette crédibilité et impacte la sécurité informationnelle résultante, en instaurant une attitude défavorable à son égard (Bulgurcu *et al.*, 2010). Au contraire, pour minimiser les effets de la distance, les gestionnaires devraient miser plus sur une confiance (Madlock, 2013) et une communication transparente (Lautsch, 2009) que la restriction. La confiance est séparée en trois dimensions, soit la *compétence*, la *bénévolence* et l'*intégrité* (Mayer *et al.*, 1995). La *compétence* correspond à l'expertise et aux caractéristiques d'un individu qui exécute une action, également nommé « mandataire ». Elle est spécifique aux domaines de compétences d'un individu puisqu'une expertise dans un domaine ne garantit pas une expertise dans un autre (Mayer *et al.*, 1995). La *bénévolence* correspond à la mesure dans laquelle le mandataire souhaite le bien-être de l'individu qui reçoit l'action, également nommé « mandateur ». Cette dimension présume que le mandataire dispose d'un sentiment d'attachement au mandateur, supérieur au motif de profit égocentrique (Mayer *et al.*, 1995). La dimension d'*intégrité* réfère à la perception que le mandataire adhère aux principes et aux valeurs acceptées par le mandateur, ce qui est similaire au concept de *réputation*. Cette dimension est fondée sur les antécédents du mandataire, dont la cohérence des actions et la crédibilité constituent les éléments fondamentaux. Dans notre étude, nous discernons des traces des trois dimensions à travers les réponses des participants. Un travailleur, conscient des enjeux de sécurité informationnelle, est en état de déceler les courriels d'hameçonnage, grâce aux tests et aux formations auxquels il a été soumis en

période d'adoption forcée du télétravail (*compétence*). Un gestionnaire, qui diminue les inquiétudes de son équipe et qui considère les volontés des membres qui la composent, au-delà du profit égocentrique, érige une intégrité fondée sur le respect des télétravailleurs (*bénévolence* et *intégrité*). Toutes ces conséquences de l'adoption forcée constituent des intrants nécessaires au développement d'une confiance et d'une culture de sécurité informationnelle au niveau du groupe.

Les comportements, par ailleurs, constituent simultanément des intrants et des extrants de la culture de sécurité informationnelle, au niveau du groupe, puisque les actions façonnent les croyances et les croyances façonnent les actions (Bulgurcu *et al.*, 2010). Considérant une réduction du contrôle des télétravailleurs, cet élément de la culture est particulièrement pertinent en contexte de télétravail, alors que les individus disposent d'une supervision diminuée et peuvent adopter des comportements illicites, comme ce fut souligné par nos participants. Ces comportements résultent généralement en une motivation diminuée des employés, qui caractérise les défis de l'adoption forcée du télétravail (Wang *et al.*, 2021), et sont groupés en deux catégories, à savoir les comportements intentionnels et non intentionnels. Dans les études préalables, menées en sécurité informationnelle, les modèles comportementaux complexes incorporent une multitude de facteurs qui incitent l'adoption de ces comportements, comme la maîtrise de soi, le *leadership*, la peur, les responsabilités, la culture organisationnelle, les croyances morales et le mécontentement (Crossler *et al.*, 2013). Or, en contexte d'adoption forcée du télétravail, ces facteurs sont influencés par la distanciation psychologique entre individus alors que le sentiment d'imputabilité est réduit considérablement. Un défaut de support social accroît l'isolement des individus (Wang *et al.*, 2021) et diminue inévitablement le bien-être (*mécontentement*) (Bavik *et al.*, 2020). En réponse à cet isolement, les individus sont parfois fatigués par leurs responsabilités au travail (Wang *et al.*, 2021), ce qui diminue conséquemment leur contrôle émotionnel au quotidien (*maîtrise de soi*). Pour pallier ces conséquences, les organisations diminuent souvent leur supervision (*peur*) (Wang *et al.*, 2021) et introduisent une approche de gestion transactionnelle (*leadership* et *culture organisationnelle*) (Abidoye, 2021). Cette approche est toutefois perçue tel un délaissement de l'organisation alors que plusieurs ne comprennent plus la nature de leur implication dans les activités de sécurité des données (*responsabilité*) et altèrent leurs attitudes à cet égard (*croyance morale*). Il en résulte que

les comportements illicites fleurissent alors et impactent la culture de sécurité des données résultante (Bulgurcu *et al.*, 2010).

5.2. Conséquences sur la sécurité informationnelle

5.2.1. Divergence des intérêts organisationnels

Pour les télétravailleurs, l'introduction d'un modèle de travail hybride implique une baisse des libertés admise en période d'adoption forcée du télétravail. Le travail **hybride** réfère à « *une modalité de travail dans laquelle les individus partagent leur temps entre le domicile et le bureau, dans le but de maximiser les bénéfices des deux méthodes* » (Babapour Chafi, Hultberg et Bozic Yams, 2022). Près de la moitié des individus apprécient la possibilité de sélectionner leur jour du bureau préféré (*bénéfice*) pour s'aligner avec les disponibilités de leurs collègues (Wang *et al.*, 2021). Cependant, les réponses de nos participants sous-entendent qu'en période de post-adoption forcée du télétravail, les organisations sont souvent réticentes à accorder cette flexibilité, car elles estiment que les libertés octroyées initialement étaient trop permissives et ont instauré un débalancement de pouvoir, qui a favorisé les employés. Ce débalancement de pouvoir a permis aux télétravailleurs d'adopter des comportements et des attitudes qui ont favorisé leurs intérêts personnels au détriment des intérêts organisationnels, comme la sécurité des données. Les individus perçoivent le télétravail comme une norme à laquelle les organisations doivent agréer pour demeurer compétitives, car les télétravailleurs sont dorénavant habitués à la commodité et à l'efficacité du bureau à domicile. Ils apprécient la réduction du temps de déplacement (*bénéfice*), qui est utilisé pour des activités familiales ou de l'exercice physique, comme la marche, la course et l'entraînement. Ils apprécient également un contrôle diminué qui permet l'adoption de comportements non sécuritaires, mais facilitateurs au travail, comme le partage de documents confidentiels via des outils non sécurisés, dont *Teams*, *Slack* et *Outlook*. Pour les travailleurs, un retour au bureau constitue une inquiétude, considérant que ces politiques sont généralement liées à une réduction d'autonomie et de liberté, qui a une incidence sur leur productivité (Babapour Chafi *et al.*, 2022). Lorsqu'un individu se présente occasionnellement au travail, le besoin de socialisation est augmenté par l'isolement social du travail à domicile, ce qui constitue souvent un fardeau contre-productif, déclenchant un effet de recul auprès des télétravailleurs (Babapour Chafi *et al.*,

2022). Certains soutiennent également que trouver un équilibre entre les deux méthodes forge une difficulté en soi, alors que l'effort d'adaptation à une structure changeante est considérable. Des problèmes d'arrimage entre le matériel informatique des environnements différents peuvent advenir considérant l'incompatibilité de certains systèmes opérationnels (Wang *et al.*, 2021). En plus de ces problèmes, nos participants soutiennent que le retour au présentiel augmenterait les risques de vols et pertes de données au moment de déplacement du matériel informatique entre les différents emplacements de travail, justifiant également pourquoi ils seraient réticents à revenir au bureau.

Pour les gestionnaires, la réalité est différente alors que le télétravail produit une incidence négative, sous l'effet d'heures de travail prolongées, des réunions consécutives, une limite des relations professionnelles et une difficulté à assurer un environnement de travail adapté aux besoins des employés (Babapour Chafi *et al.*, 2022). Ces effets découlent d'une culture « toujours active », appelée « *always-on culture* », et s'appliquent principalement aux cadres intermédiaires. Le *always-on culture*, qui réfère à la pratique d'être constamment en ligne, détient une conséquence subséquente sur la sécurité informationnelle en organisation. Elle force les gestionnaires à travailler en dehors des heures de travail régulières et à utiliser des appareils personnels pour accéder aux informations confidentielles, par des moyens qui ne sont pas sécuritaires. Elle encourage également une attitude de « réponses immédiates » aux demandes de communication, ce qui incite les gestionnaires à appliquer des raccourcis en matière de sécurité des données, et suscite leur épuisement à long terme. Il n'est donc pas surprenant que les gestionnaires souhaitent partiellement rétablir un rythme de travail balancé, par un retour au présentiel, alors que l'hybride amoindrit ces effets et reproduit la cohésion, l'apprentissage collectif et la collaboration dans les équipes (Babapour Chafi *et al.*, 2022). Quand les membres d'une équipe collaborent et démontrent une cohésion de groupe, ils sont plus prompts à partager de l'information importante, relative à la sécurité des données, ce qui promeut la culture de sécurité informationnelle, au niveau du groupe, et satisfait les inquiétudes des gestionnaires. Nous pouvons donc cerner une divergence entre les intérêts des individus et ceux des gestionnaires, en post-adoption forcée du télétravail, qui nécessite d'établir un équilibre pour assurer une pérennité organisationnelle.

Trouver un équilibre entre ces deux perspectives constitue un facteur déterminant pour la pérennité du modèle hybride, alors que les gestionnaires doivent offrir plus de flexibilité, quand les travailleurs sont à domicile ; et améliorer l'environnement de travail, lorsque les travailleurs sont au bureau (Babapour Chafi *et al.*, 2022). Cela permet ultimement de créer une solution hybride qui bénéficie les individus, mais qu'en est-il des organisations? Pour les organisations, les bénéfices du modèle hybride sont produits essentiellement au niveau de la communication et du support social (Babapour Chafi *et al.*, 2022). Après tout, sans la contextualisation d'une communication présentielle, il est difficile d'acquitter des enjeux professionnels, de prendre des décisions et de bâtir une culture de sécurité informationnelle. Une amélioration de la communication via une modalité hybride permet aussi d'améliorer les activités de formations et d'intégration des individus, ce qui réduit le taux de roulement (Gajendran *et al.*, 2007) et les erreurs commises par les nouveaux arrivants. Des travailleurs adéquatement intégrés et formés développent un sentiment d'appartenance important alors qu'ils entretiennent une relation informelle avec leurs collègues (Wang *et al.*, 2021). Une similarité peut être établie à travers les réponses de nos participants quand ils soulèvent des enjeux d'intégration dans en contexte d'adoption forcée et l'incidence de ces enjeux sur le taux de roulement des organisations. Bien que l'hybride permette de résoudre quelques-uns de ces enjeux, il en suscite également des nouveaux, à savoir l'ambiguïté des règles organisationnelles, l'accommodation des cas particuliers[6], les non-conformistes[7], la gestion d'une logistique incertaine et l'inclusion envers l'égalité des chances, peu importe l'emplacement de travail d'un individu (Babapour Chafi *et al.*, 2022). Comment gérer les individus qui ont été engagés en période d'adoption forcée quand les politiques étaient plus flexibles? Devons-nous leur attribuer un statut particulier (*ambiguïté des règles organisationnelles*)? Dans une situation contraire, les organisations risquent de perdre des télétravailleurs précieux simplement parce qu'ils ne peuvent pas se présenter physiquement au bureau, à défaut d'habiter trop loin (*accommodation des cas particuliers*). Ces ambiguïtés produisent une divergence des intérêts et impactent la sécurité des données par un mécontentement des individus et d'une démotivation professionnelle.

[6] Ex. : Individu dont le lieu de résidence fait en sorte qu'il est impossible de se rendre au bureau.
[7] Individu qui ne se conforme pas aux modalités de travail (*présentiel*, *hybride* ou *télétravail*), devancées par son organisation.

6. Conclusion

6.1. Contributions

Le but de cette étude était de formuler les facteurs explicatifs du « *pourquoi?* » et de sonder les concepts théoriques du « *comment?* » (Whetten, 1989) afin de répondre à notre question de recherche : **comment ET pourquoi l'adoption forcée du télétravail impacte-t-elle la sécurité informationnelle en organisation?** Au chapitre précédent, nous avons élaboré les nouveautés, recensées à travers les réponses de nos participants, et avons conclu une compréhension exhaustive du phénomène étudié. Le chapitre de conclusion débute par une formulation des contributions, qui résident dans le développement d'un modèle conceptuel et érigent l'incidence des conséquences de l'adoption forcée du télétravail sur la sécurité des données. Cette contribution est distinguée par son apport théorique et pratique, relatif à l'étude de phénomènes sociaux, comme l'adoption forcée du télétravail, et à l'avancement des sciences informatiques.

6.1.1. Contributions théoriques

Plus précisément, une contribution théorique fondamentale découle de la **séparation du concept** de *misfit* par niveau d'étude. Cette séparation est nécessaire puisque, inversement aux études préalables (Bélanger *et al.*, 2013), chaque niveau dispose d'un impact spécifique sur la sécurité des données, en fonction de son *misfit* respectif. Par exemple, pour évaluer l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle, au niveau du groupe, il est nécessaire de comprendre préalablement les facteurs d'indisposition au télétravail qui caractérisent le groupe en question. Ainsi, chaque niveau d'étude détient des facteurs de prédisposition qui leur sont spécifiques et qui sont illustrés séparément. Pour l'individu, le sociodémographique, les attitudes et la nature des intérêts constituent ces facteurs ; pour le groupe, la collaboration, la composition et la synergie ; pour l'organisation, la culture organisationnelle et le secteur d'activités. Dans une culture bureaucratique, d'ailleurs, telle une organisation publique ou bancaire, les individus sont davantage réticents à adopter le changement, car le changement entraîne une reformulation des règles organisationnelles préétablies et une complexité respective.

Notre étude vient également enrichir les notions relatives aux mécanismes de gestion, en élaborant une conception des comportements adoptés pour mitiger les tensions résultantes du télétravail. Par exemple, nous avons vu qu'au niveau individuel, le *misfit* est un facteur de non-prédisposition qui impacte le bien-être, qui à son tour est mitigé par l'adaptation de comportements. Subséquemment, l'effort associé à cette adaptation aura une incidence sur les conséquences résultantes, qui exercent une rétroactivité sur les mécanismes adoptés initialement. Un individu qui perçoit une croissance de la distance psychologique en milieu de travail à domicile aura intérêt reconsidérer sa stratégie d'adaptation initiale. Une logique similaire est attribuée aux organisations et aux groupes. Cette **boucle rétroactive** constitue notre deuxième contribution. La rétroactivité en sécurité informationnelle est un élément fondamental, car elle accélère le repérage des failles des systèmes informatiques, motive les télétravailleurs à participer dans le développement de pratiques sécuritaires et améliore globalement la sécurité des systèmes (Abidoye, 2021). Certaines conceptions précédentes (Bélanger *et al.*, 2013) établissent une fonction similaire en implantation organisationnelle du télétravail, mais n'appliquent pas cette rétroactivité à la sécurité informationnelle. Nous pallions ce manque.

Une troisième contribution théorique découle de l'introduction de deux **conséquences**, soit la divergence des intérêts et l'interférence du télétravail, et de deux **mécanismes** de gestion, soit l'adaptation individuelle et la culture de sécurité informationnelle au niveau du groupe. Les mécanismes de gestion, nouvellement introduits, sont nécessaires à l'implantation du télétravail sur un horizon temporel, allant au-delà du contexte pandémique, car ils assurent une mitigation des conséquences relatives à cet événement. L'adaptation individuelle, par exemple, augmente inévitablement la perception de proximité avec les collègues, améliore la productivité et accentue le niveau de bien-être d'un individu précis. La culture de sécurité informationnelle au niveau du groupe, par ailleurs, exerce une fonction complémentaire, en bâtissant une *bottom-up culture*. Similairement au *misfit*, ce mécanisme de gestion est fortement lié au secteur d'activités de l'organisation concernée, alors que l'adaptation est souvent tardive dans les environnements bureaucratiques. Les conséquences, nouvellement introduites, sont issues des acquis informationnels des entrevues semi-structurées, alors qu'elles furent abordées par tous nos participants et détiennent une incidence sur la sécurité informationnelle en organisation.

6.1.2. Contributions pratiques

Les résultats de notre étude sont d'une grande contribution aux individus, aux gestionnaires et aux organisations au niveau de la compréhension des phénomènes étudiés en télétravail. Dans cette sous-section, nous détaillons les contributions pratiques qui peuvent être utiles pour un gestionnaire d'équipe afin de mitiger l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle en organisation.

Les résultats de notre étude étendent la compréhension du gestionnaire relatif aux facteurs explicatifs de l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle en organisation. Cette compréhension est fondamentale pour la mitigation des tensions, dans un environnement où le phénomène étudié est observé. Dans notre étude, nous avons recensé trois conséquences dans les réponses des participants, soit l'adoption d'une gestion transactionnelle, la révision des procédures de travail et la distanciation des télétravailleurs. Cette suite est complétée de deux conséquences additionnelles : l'interférence du télétravail et la divergence des intérêts. Une compréhension exhaustive des cinq conséquences fournit aux gestionnaires les outils nécessaires pour mitiger ces conséquences par les mécanismes de gestion respectifs. Par exemple, en prenant connaissance des résultats de cette analyse exploratoire, un gestionnaire peut reconnaître les difficultés de son équipe, tel un non-respect des normes de sécurité (*conséquence*), et adopter les mécanismes de gestion qui permettent de les mitiger, comme la promotion de meilleures pratiques et d'une culture de sécurité informationnelle (*mécanisme*).

Notre modèle conceptuel amélioré réfère également aux relations interconceptuelles, où le *misfit* forme les facteurs d'indisposition ; les tensions résultent du *misfit* au télétravail ; les mécanismes de gestion régulent les tensions ; et finalement, la qualité d'implantation de ces mécanismes mitige les conséquences sur la sécurité informationnelle. Ces relations entre les quatre concepts offrent aux gestionnaires une compréhension des causes sous-jacentes d'une sécurité diminuée et leur permettent d'implanter des solutions pour y remédier. En analysant les résultats de notre étude, le gestionnaire peut donc comprendre comment le *misfit* au télétravail déteint sur les conséquences de son adoption forcée. Notre étude permet aux gestionnaires de positionner leur équipe, comparativement aux autres équipes, de sorte à introspecter sur les mesures qu'ils emploient. En ayant cette vision

comparative, les gestionnaires peuvent mieux cerner le degré de *fit* de leur équipe, comparativement aux autres équipes. Finalement, notre étude conscientise également les gestionnaires sur la nécessité de considérer le facteur humain dans la gestion en télétravail. En favorisant une communication motivante, les gestionnaires encouragent les télétravailleurs à respecter les protocoles de sécurité et à signaler les comportements suspects. La transparence, quant à elle, permet aux télétravailleurs de mieux comprendre les motifs derrière les politiques de sécurité informationnelle et de se sentir davantage impliqués à cet égard.

6.2. Limites de l'étude

Comme tout processus académique, la présente étude admet des limites qui requièrent une attention à l'égard des méthodes sélectionnées et des résultats recensés. Malgré les efforts déployés pour minimiser les biais, qui forment les analyses de données qualitatives, nous devons être transparents dans les limites respectives.

Une première limite est établie au niveau de l'**horizon temporel**, qui sépare les différentes étapes de traitement des données (*collecte* et *analyse*) et l'occurrence du phénomène étudié. Puisque nous étudions un phénomène datant au-delà de deux ans, soit l'adoption forcée du télétravail qui a débuté au printemps 2020, les questions de notre guide d'entrevue ont un élément de rappel dans leur formulation. Rappelons-le que nos questions ont été formulées en deux temporalités distinctes, soit la préadoption forcée et la post-adoption forcée. Il est donc inévitable que, lors de nos entrevues semi-structurées, nous avons rencontré des éléments de réponses, comme « *je ne me rappelle plus* », « *je ne suis pas sûr* » et « *il me semble que* ». Ces notions ont un effet importun sur la qualité des données, alors qu'elles sont possiblement teintées d'inexactitude, due à un mauvais rappel des événements. Pour éviter ce biais de rappel (Raphael, 1987), une étude qui minimise l'écart du temps entre le phénomène d'intérêt et le moment de collecte de données serait davantage appropriée considérant notre question de recherche.

Une seconde limite est établie en vertu d'une **perspective méthodologique**, alors que les analyses exploratoires de données qualitatives, comme l'analyse thématique et l'induction analytique, n'allouent pas une inférence des résultats au-delà de l'ensemble des répondants

interrogés dans notre étude (Yin, 2003). Les propositions résultantes de notre analyse permettent de formuler des pistes à explorer, grâce aux analyses confirmatrices de données quantitatives, et de complémenter la littérature académique existante (Eisenhardt, 1989). Les études qualitatives admettent également un certain nombre de biais, comme les biais relatifs aux chercheurs et les biais relatifs aux participants. Ces biais influencent tous les acteurs impliqués, considérant l'aspect incontrôlé des études qualitatives. Dans notre étude, nous dénotons trois biais méthodologiques considérables : le biais de *désirabilité sociale*, soit l'adaptation du participant à l'individu qui l'interroge, de sorte que les réponses sont altérées pour plaire aux chercheurs ; le biais de *confirmation*, soit la mesure selon laquelle les résultats sont interprétés conformément à une opinion préétablie du chercheur sur le sujet étudié ; et finalement, le biais de *sélection*, soit généralement une conséquence d'un échantillonnage non aléatoire, lorsque certains participants sont écartés injustement. Notre méthodologie conçoit le processus de sélection des participants comme étant la source prédominante de biais de notre étude, car l'échantillonnage par convenance admet forcément une discrimination de certains individus, basée sur des critères injustifiés. Toutefois, nous devons souligner que la conception méthodologique d'analyse des données collectées est optimale pour l'étude de comportements humains et surtout dans un contexte d'environnement inédit, comme celui de la pandémie (Guba et Lincoln, 1994).

Une troisième limite est justement attribuée à cet **environnement inédit**. Il est certain que le contexte pandémique a alloué une démocratisation du télétravail, alors qu'en printemps 2020, près de 557 millions d'individus travaillaient à distance (Berg *et al.*, 2021), mais il a également introduit des éléments qui influencent la perception des participants. Effectuer une étude qualitative des perspectives individuelles dans un contexte stressant, comme la pandémie, peut affecter les réponses des participants de plusieurs façons. D'abord, nous croyons que l'incertitude et l'anxiété ont eu une incidence positive sur la prédisposition des participants au télétravail puisque cette méthode d'organisation alloue une grande flexibilité et autonomie d'emploi, qui sont nécessaires lorsque les garderies sont fermées, les contacts sociaux sont diminués et que le confinement est en vigueur. Ensuite, nous croyons également que les expériences précédentes, en matière d'implantation du télétravail, influencent l'expérience individuelle relative à cette méthode d'organisation. Or, les participants dont les organisations disposent de facteurs de

prédisposition favorables, telles une infrastructure technologique adéquate, une culture organisationnelle non bureaucratique et des pratiques managériales conformes, auront tendance à avoir une perspective davantage favorable au télétravail et aux effets de son imposition sur la sécurité informationnelle.

6.3. Pistes de recherches futures

Par la juxtaposition des résultats de nos entrevues semi-structurées et des concepts issus de la revue de littérature, ce mémoire complète une analyse exploratoire du télétravail et son incidence sur la sécurité informationnelle en organisation. Puisque cette approche n'alloue pas d'inférence statistique au-delà des répondants sélectionnés (Yin, 2003), nous dressons plusieurs pistes des recherches futures, qui peuvent être complémentaires à la présente.

Une première piste de recherche constitue la poursuite d'une **analyse confirmatoire**, basée sur les prémisses énoncées dans l'étude. Considérant la sécurité informationnelle, comme une métrique quantifiable, nous sommes en mesure de valider l'incidence des mécanismes supplémentaires recensés, soit l'adaptation individuelle (Beaudry *et al.*, 2005) et la culture de groupe (Da Veiga *et al.*, 2010), sur la sécurité informationnelle des organisations par une analyse confirmatoire subséquente. Les études exploratoires et confirmatrices sont complémentaires et doivent être utilisées conjointement pour que l'étude d'un phénomène soit véritablement complète (Tukey, 1980). Effectivement, l'analyse exploratoire sert une fonction d'identification des relations dans les données collectées, qui peuvent être validées uniquement par le caractère rigoureux d'une analyse confirmatoire (Tukey, 1980). Dans ce mémoire, nous formulons les relations interconceptuelles pour inciter les futurs chercheurs à quantifier le niveau de sécurité informationnelle, afin de fournir une évaluation davantage objective des éléments qui constituent notre question de recherche. Ceci est conforme aux principes de l'analyse confirmatoire, qui vise à tester des hypothèses spécifiques et émettre des conclusions inférentielles à l'échelle d'une population (Eisenhardt, 1989). La méthode quantitative permet également d'éviter les biais du chercheur, énoncés précédemment, soit le biais de *confirmation*.

Cependant, pour mener une étude confirmatoire efficiente, nous devons faire une multitude d'études exploratoires, préalablement (Tukey, 1980). Cela nous amène à considérer notre

seconde piste de recherche, soit l'utilisation d'une **différente méthodologie** pour une étude exploratoire, fondée sur une vraie perspective longitudinale, où des entrevues subséquentes sont entreprises avec les mêmes participants à plusieurs moments dans le temps. Les études longitudinales tiennent leur pertinence dans la compréhension approfondie des facteurs explicatifs et des relations interconceptuelles entre le *misfit*, les tensions, les mécanismes et les conséquences sur la sécurité. Ces études révèlent les changements comportementaux, particulièrement pertinents en contexte de sécurité informationnelle, procurant une compréhension exhaustive des notions abordées. Rappelons-le qu'une culture de sécurité informationnelle est composée de deux constituants fondamentaux : les comportements individuels et les composants contextuels (Da Veiga *et al.*, 2010). L'utilisation d'une étude longitudinale permet de mieux comprendre la dynamique des effets relatifs à la temporalité du phénomène étudié. Idéalement, les études futures devraient collecter les données à deux moments distincts, soit avant et après l'adoption forcée du télétravail, ce qui permettra de tester les prémisses établies par notre étude, comme l'incidence négative du télétravail sur le bien-être individuel, tel que soulevé par plusieurs de nos participants.

Une troisième piste de recherche constitue l'étude du phénomène donné dans un **contexte différent**, caractérisé par des participants aux fonctions différentes, des secteurs d'activité spécifiques ou un contexte désassocié de la pandémie. Une étude qualitative en contexte pandémique influence les réponses des participants d'une perspective anxiogène, caractère à un tel environnement. Pour éviter cette limite, nous estimons l'importance d'émettre une question de recherche, qui désassocie le télétravail du contexte pandémique. En explorant une question de recherche dans un autre environnement, avec des participants aux fonctions différentes et des secteurs spécifiques, nous pouvons acquérir une compréhension nuancée de l'incidence du télétravail sur la sécurité informationnelle. Certes, dans notre étude, nous souhaitions évaluer spécifiquement le volet *obligatoire* du télétravail, ce qui explique notre formulation initiale de la question de recherche. Cependant, il serait dorénavant pertinent de contextualiser nos résultats avec ceux, issus d'un environnement davantage stable. Les recherches futures devraient également concevoir une diversité des participants interrogés, car notre étude est limitée à ce niveau, considérant notre méthode d'échantillonnage simple et convenable. Effectivement, tous nos participants exercent des fonctions similaires, alors qu'ils interagissent quotidiennement avec les systèmes informatiques de leur organisation.

Cependant, la sécurité informationnelle est évaluée par le maillon le plus faible de la chaîne des opérations des systèmes informatiques, d'où l'importance de considérer un bassin plus diversifié de télétravailleurs.

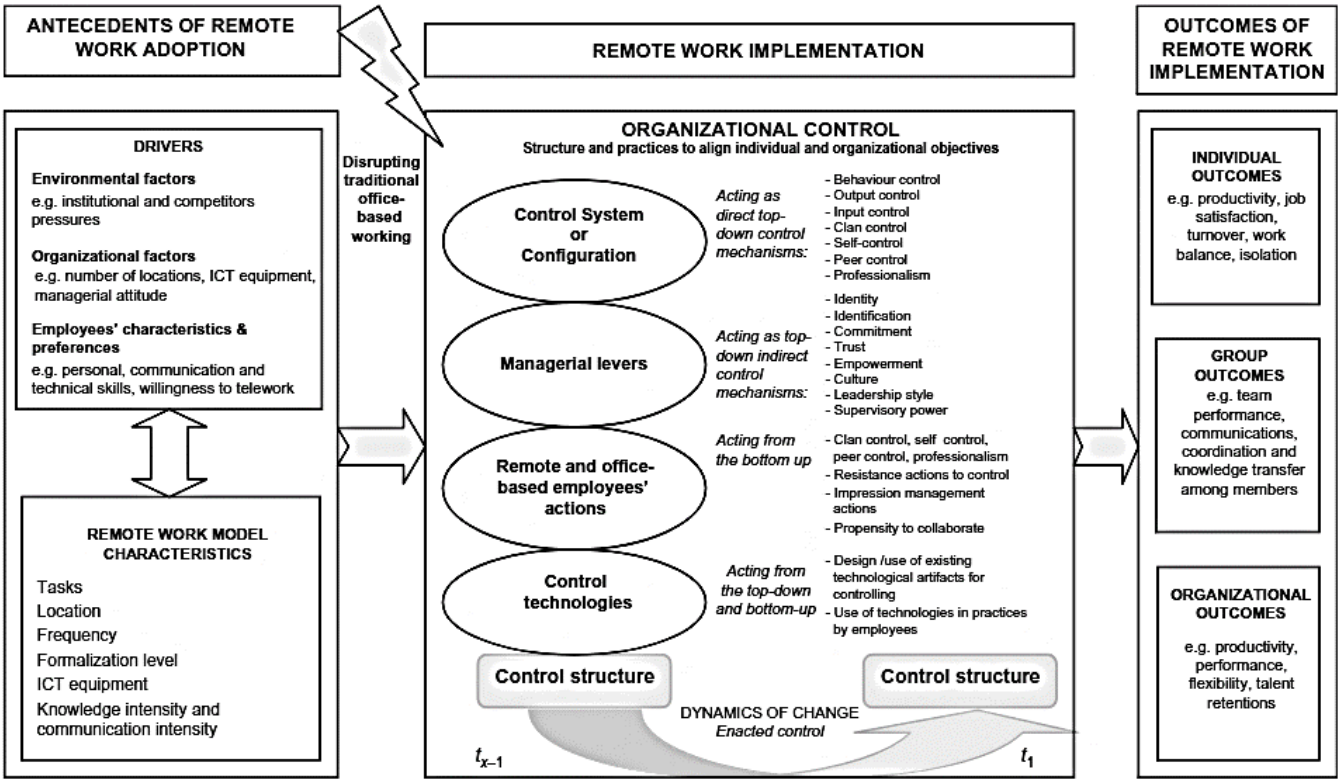
Une quatrième, et finale, piste de recherche constitue l'étude du phénomène considéré, par une **fragmentation** du modèle conceptuel amélioré, en isolant les trois niveaux d'étude, à savoir l'individu, le groupe et l'organisation. Cette fragmentation allouera une mobilisation de différents types d'étude, comme la psychologie au niveau individuel, le comportemental au niveau du groupe et la culture au niveau organisationnel. Elle examinera en profondeur les enjeux de sécurité informationnelle, qui sont spécifiques à chaque niveau considéré. La profondeur associée à cette granularité est nécessaire, alors que chaque niveau d'étude peut être considéré comme une entité autonome qui nécessite une attention spécifique en termes de recherche et d'analyse. Les individus, les groupes et les organisations disposent tous de caractéristiques et de dynamiques particulières, qui influencent la sécurité informationnelle qui résulte de l'adoption forcée du télétravail. De plus, cette fragmentation permettrait aussi d'élaborer des concepts non considérés dans notre étude, comme des facteurs de *misfit*, des tensions, des mécanismes et des conséquences supplémentaires. Au niveau individuel, par exemple, une étude fragmentée pourrait possiblement révéler des facteurs de *misfit*, comme l'indiscipline des individus (Wang *et al.*, 2021). Au niveau du groupe, des mécanismes de gestion inconsidérés, comme l'adoption de technologies de communication qui maximisent l'efficacité des interactions, pourraient être recensés et analysés (Lojeski *et al.*, 2008). Au niveau organisationnel, une étude fragmentée pourrait illustrer des incidences potentielles, qui découlent des procédures de travail adoptées et qui sont en ajout à la divergence des intérêts postpandémiques, que nous avons énoncée dans notre conceptualisation.

Compte tenu des pistes de recherche suggérées dans cette sous-section du mémoire, nous espérons que les études futures puissent complémenter les éléments du modèle conceptuel théorique, présenté en **Figure 6**. Nous souhaitons également que les contributions pratiques et les contributions théoriques, formulées dans cette étude, puissent servir aux académiques et aux professionnels des différents domaines, telles les sciences informatiques et les sciences sociales, pour résoudre conjointement les enjeux du futur.

Annexes

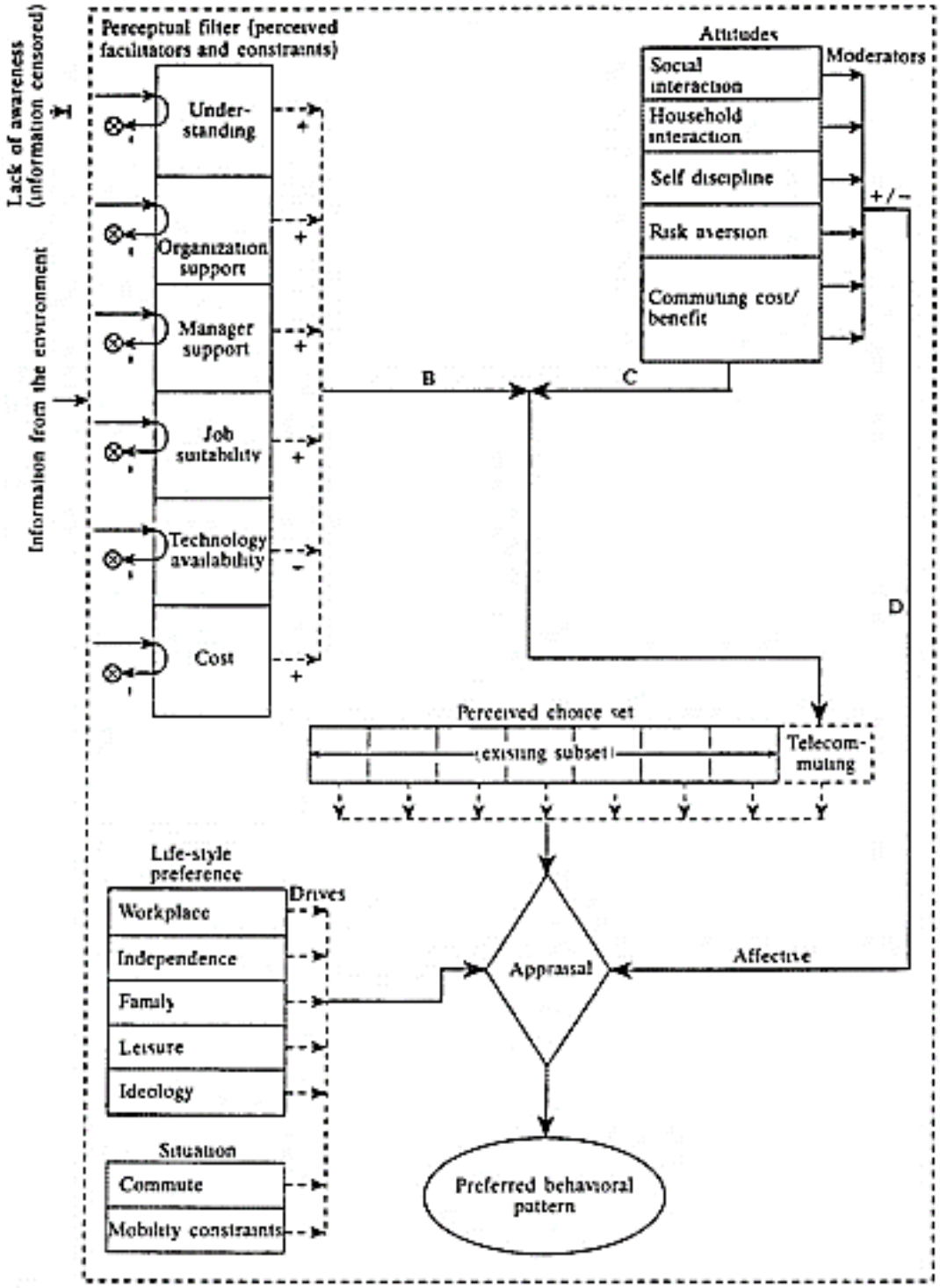
Annexe 1 Implantation du télétravail (Errichiello *et al.*, 2016)

Cette conception d'intégration organisationnelle du télétravail présente le processus en trois étapes : (1) l'adoption, caractérisée par des facteurs contextuels, (2) l'implantation, soit les pratiques d'alignement d'intérêts individuels aux intérêts organisationnels et (3) les résultats d'implantation, divisés par niveau d'étude (individu, groupe et organisation).



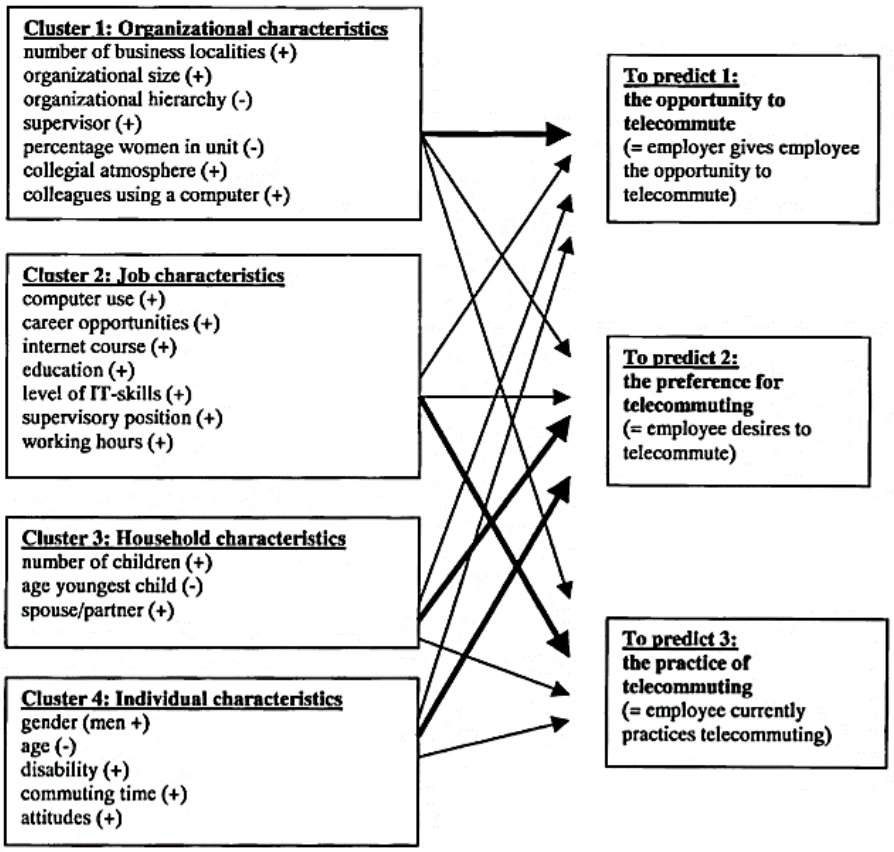
Annexe 2 Facteurs d'adoption du télétravail (Mokhtarian *et al.*, 1993)

Le schéma ci-dessous est une version complète du modèle des facteurs d'adoption du télétravail, présenté par Mokhtarian et Salomon, en 1993. Ultimement, les facteurs d'adoption représentée sont explicitement cités dans le schéma et sont divisés en quatre catégories : (1) les attitudes, (2) les préférences du style de vie, (3) la situation contextuelle et (4) les facteurs facilitants ou complexifiant.



Annexe 3 Facteurs prédictifs de préférence du télétravail (Peters *et al.*, 2004)

Similairement à l'annexe précédent, le modèle de Peters (2004) représente schématiquement les facteurs qui prédisent trois probabilités interdépendantes : (1) la probabilité d'avoir une opportunité de télétravailler, (2) la probabilité d'aimer le télétravail et (3) la probabilité de pratiquer le télétravail. La nature interdépendante des probabilités est soulignée par la multitude de flèches intercroisées. L'étude était réalisée avec un *scope* du groupe et les facteurs prédictifs ont été classés en quatre catégories,



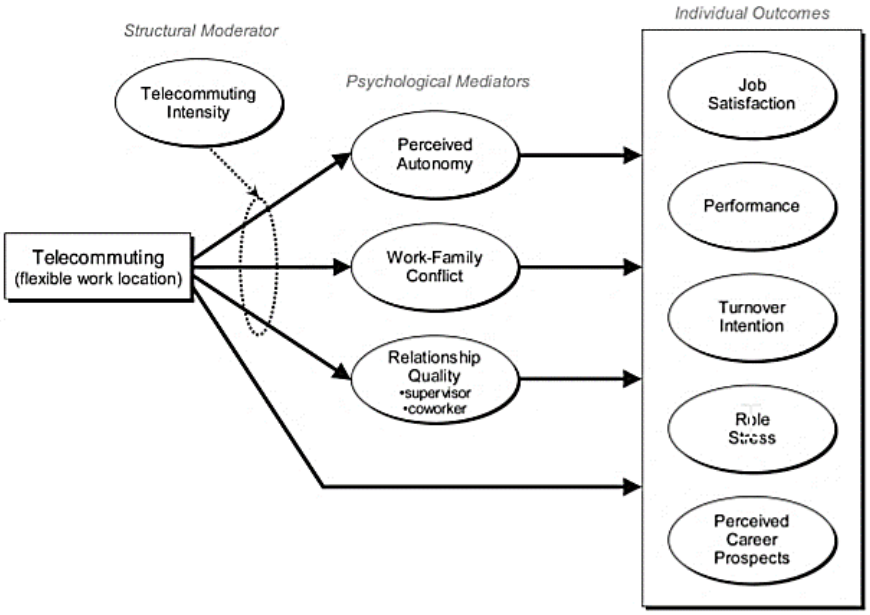
Note: *(+) A positive effect is expected*

(-) A negative effect is expected

A bold line indicates the most important effects, according to the hypotheses.

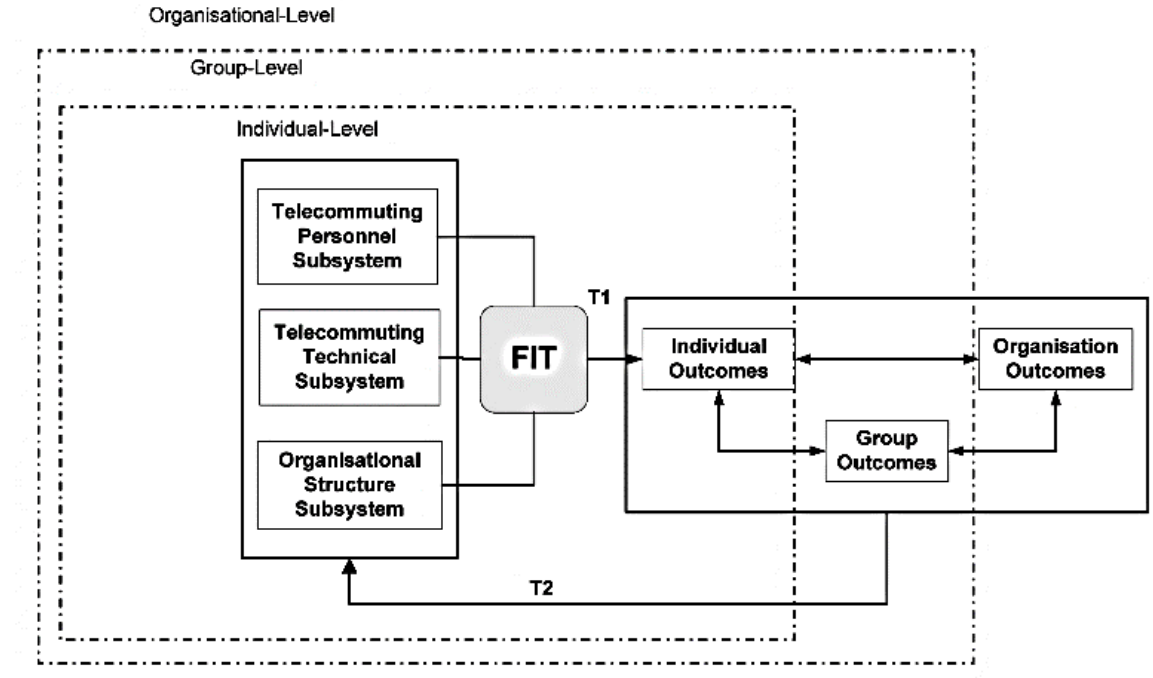
Annexe 4 Impact du télétravail sur l'individu (Gajendran *et al.*, 2007)

Le modèle de Gajendran et Harrison est suffisamment explicite, alors qu'il représente visuellement les conséquences directes de l'adoption organisationnelle du télétravail sur les télétravailleurs.



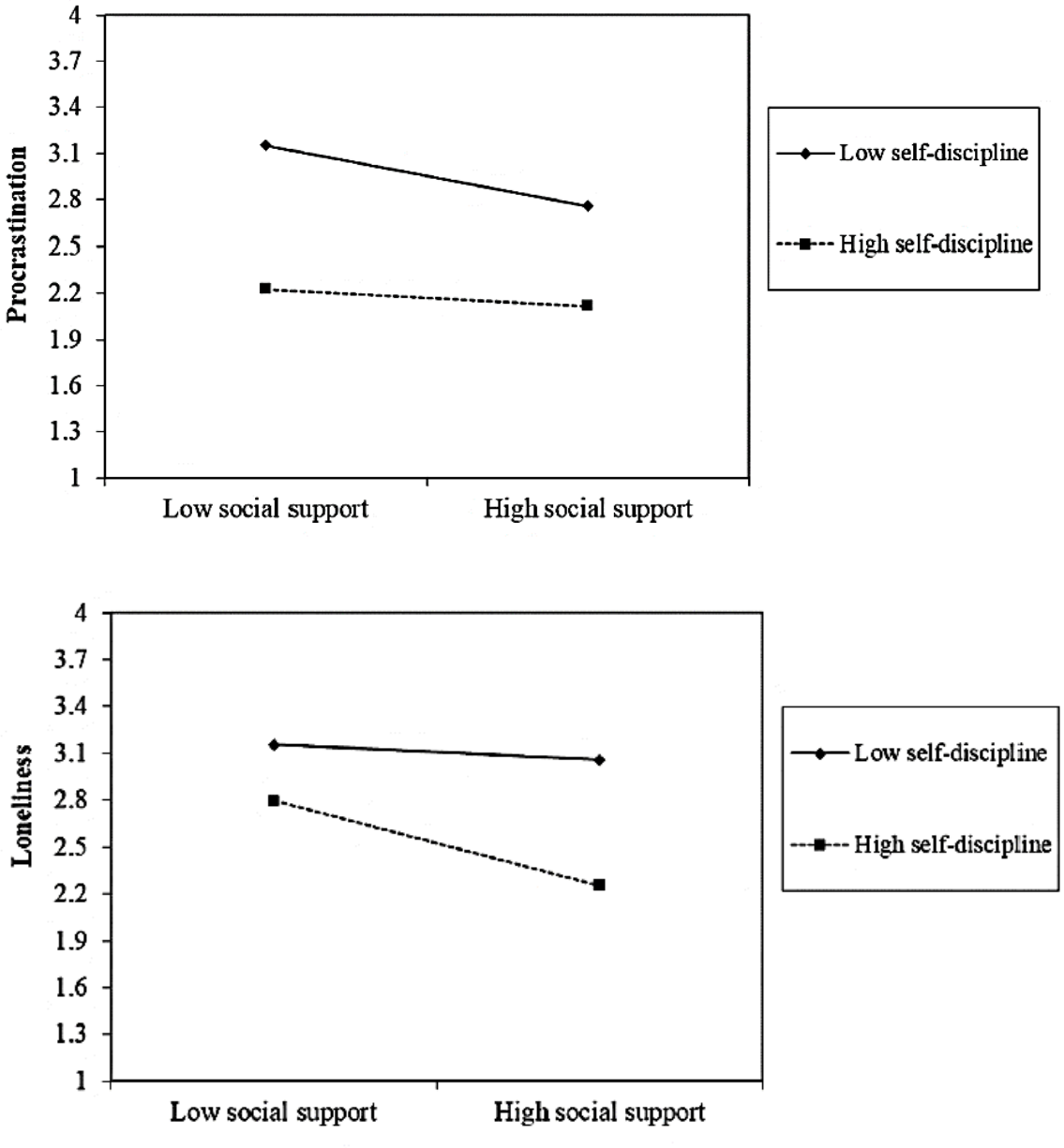
Annexe 5 Implantation organisationnelle du télétravail (Bélanger *et al.*, 2013)

Le processus d'implantation organisationnelle du télétravail, présenté par Bélanger (2013), contribue au développement d'une dimension additionnelle intéressante au modèle de Collins (1998). Non seulement il considère le concept de *fit*, mais il attribue également une notion d'interdépendance entre les conséquences d'implantation et les trois niveaux d'étude. Il s'agit d'un modèle plus dynamique que ceux qui l'ont précédé.



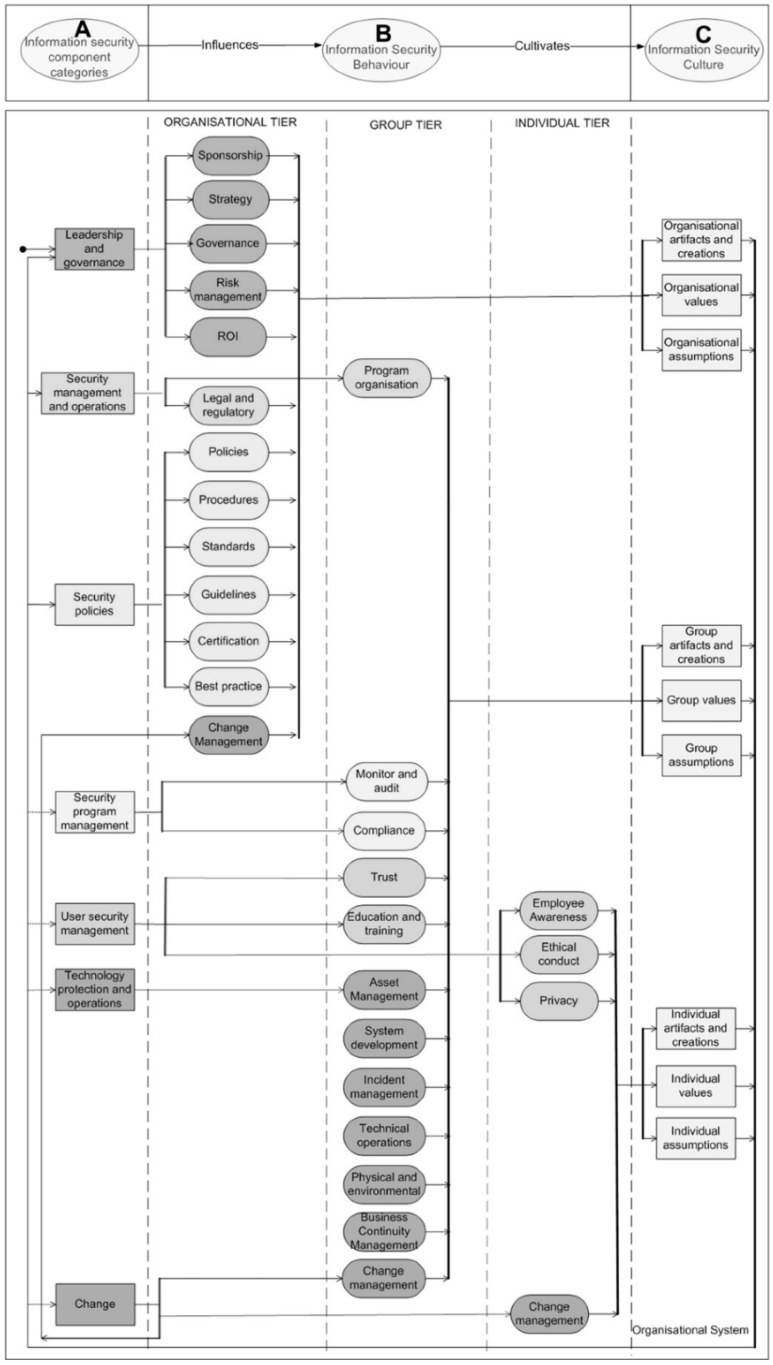
Annexe 6 Effet du social sur la procrastination et l'isolement (Wang *et al.*, 2021)

L'étude réalisée par Wang (2021) détaille les relations quantifiées entre les différentes caractéristiques d'un environnement en télétravail sur les défis qui découlent de cet environnement, comme la procrastination et l'isolement. Le graphique du haut correspond à la procrastination et le graphique du bas, à l'isolement.



Annexe 7 Une culture de sécurité informationnelle (Da Veiga, 2010).

Le présent modèle est une élaboration du schéma simplifié, présenté à la **Figure 3**. Il constitue un ajout de valeur académique par une démonstration détaillée (1) des composantes intrants d'une culture de SI, (2) des comportements divisés par niveau d'étude et (3) des composantes extrants d'une culture de SI.



Annexe 8 Table d'encodage des données qualitatives

La présente table est produite manuellement et sert d'outil à l'analyse des données qualitatives collectées. Les quatre lignes, en gris foncé, ont été introduites, à la suite de la complétion du processus d'analyse des données. Il s'agit d'éléments soulevés par les participants qui étaient inconsidérés initialement.

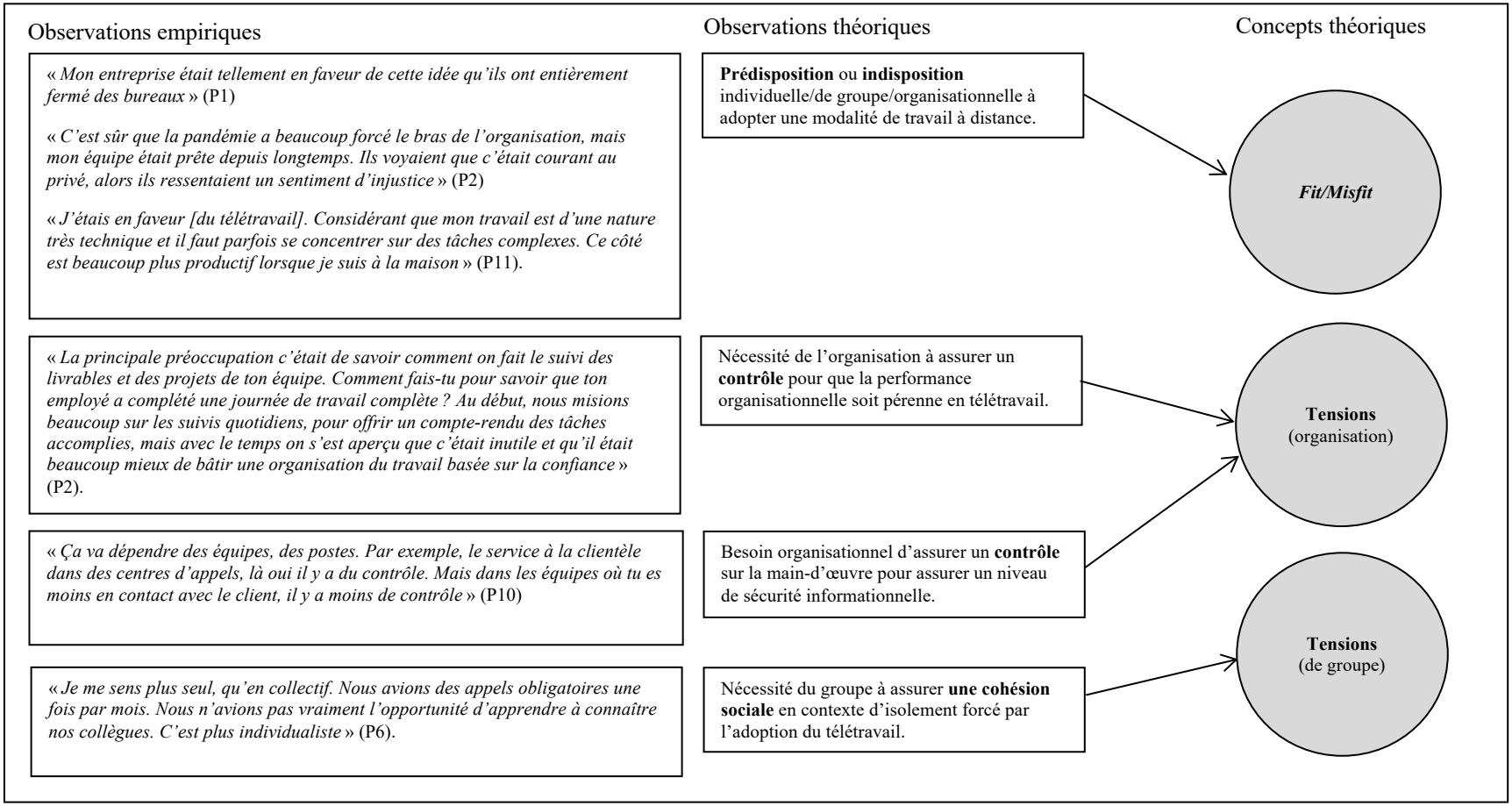
Thème	Section	Sous-section	Code	Définition	Références principales
Télétravail	Adoption organisationnelle	Fit/Misfit	TLTR-ADOP-FIT	Éléments identificatoires d'un *fit* ou d'un *misfit* entre le télétravail et le niveau d'étude considéré	(Desilver, 2020);(Mokhtarian *et al.*, 1993);(Peters *et al.*, 2004);(Bélanger *et al.*, 2013)
Télétravail	Implantation organisationnelle	Procédures de sécurité	TLTR-IMPL-PROC	Éléments associés aux procédures de sécurités adoptées en post-adoption.	(Cooper *et al.*, 1990);(Collins, 1998);(Wang *et al.*, 2021)
Sécurité informationnelle	Implantation organisationnelle	Sensibilisation	SI-IMPL-SENS	Éléments associés à la sensibilisation à la sécurité informationnelle.	(Da Veiga *et al.*, 2010);(Bulgurcu *et al.*, 2010)
Tensions	Politiques	Contrôle et Liberté	TENS-POL-CONT-LIB	Éléments associés à la tension découlant du *misfit* organisationnel, opposant le contrôle et la liberté.	(Wang *et al.*, 2021)
Tensions	Environnement	Individualisme et Collectivisme	TENS-ENV-IND-COL	Éléments associés à la tension découlant *misfit* de groupe, opposant l'individualisme et de collectivisme.	(Wang *et al.*, 2021)
Tensions	Ressenti	Mal-être et Bien-être	TENS-RESS-MAL-BIEN	Éléments associés à la tension découlant du *misfit* individuel, opposant le mal-être et le bien-être.	(Wang *et al.*, 2021)
Mécanismes de gestion	Implantation organisationnelle	Utilisation des TIC	GEST-IMPL-TIC	Éléments associés à l'utilisation des TIC, à titre de mécanisme de gestion, en implantation du télétravail.	(Wang *et al.*, 2021);(Hill, 1995);(Beasley *et al.*, 2000) ; (Vivadelli, 2005)

Mécanismes de gestion	Implantation organisationnelle	Gestion transactionnelle	GEST-IMPL-MNGT	Éléments relatifs à l'approche managériale à titre de mécanisme de gestion.	(Wang *et al.*, 2021);(Abidoye, 2021);(Zhang *et al.*, 2010)
Mécanismes de gestion	Implantation organisationnelle	Adaptation individuelle	GEST-IMPL-ADPT	Éléments associés à l'adaptation individuelle à titre de mécanisme de gestion.	(Beaudry *et al.*, 2005)
Mécanismes de gestion	Implantation organisationnelle	Culture SI de groupe	GEST-IMPL-GRP	Éléments associés à la culture SI de groupe à titre de mécanisme de gestion des tensions.	(Da Veiga *et al.*, 2010)
Conséquences	Performance	Indicateurs	CONS-PERF-IND	Éléments associés aux indicateurs de performance à titre de conséquences de l'implantation du télétravail.	(Errichiello *et al.*, 2016)
Conséquences	Niveau SI	Sensibilisation	CONS-NIV-SENS	Éléments associés à la sensibilisation à titre de conséquences de l'implantation du télétravail.	(Errichiello *et al.*, 2016)
Conséquences	Niveau SI	Risques	CONS-NIV-RISQ	Éléments associés à la perception des risques en SI comme conséquences de l'adoption forcée.	(Errichiello *et al.*, 2016);(Bulgurcu *et al.*, 2010)
Conséquences	Niveau SI	Divergence intérêts	CONS-NIV-DIV	Éléments associés à la divergence des intérêts, en post-adoption forcée, comme conséquences de l'adoption forcée.	(Errichiello *et al.*, 2016)
Conséquences	Niveau SI	Interférence du télétravail	CONS-NIV-INT	Éléments associés à l'interférence du télétravail comme conséquences de l'adoption forcée.	(Wang *et al.*, 2021);(Abidoye, 2021);(Zhang *et al.*, 2010)

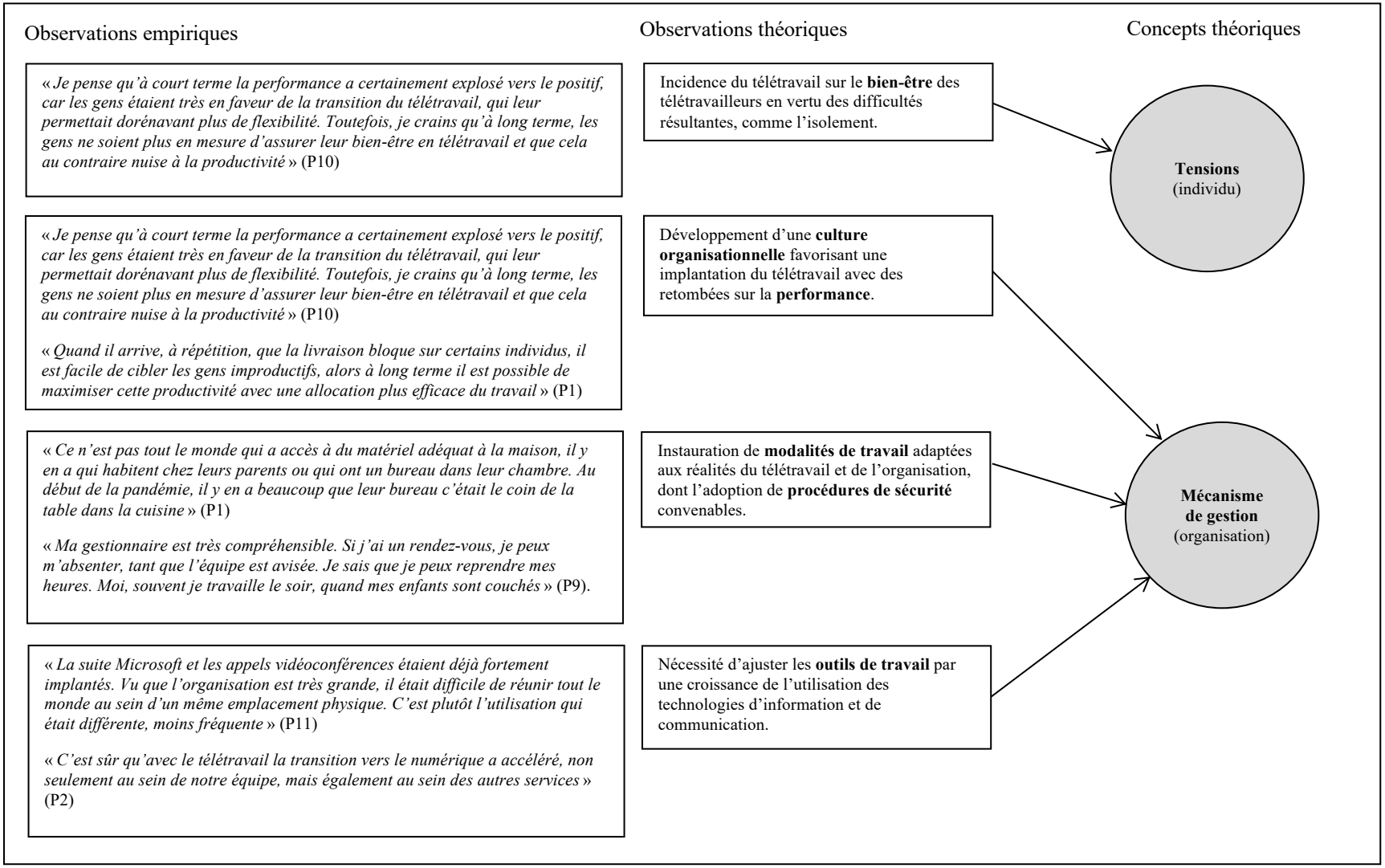
Annexe 9 Structures de données et chaînes de preuves

Cette annexe reflète les citations des participants qui soutiennent les théories sous-jacentes de notre modèle conceptuel final à travers des chaînes de preuve entre les différentes structures de données.

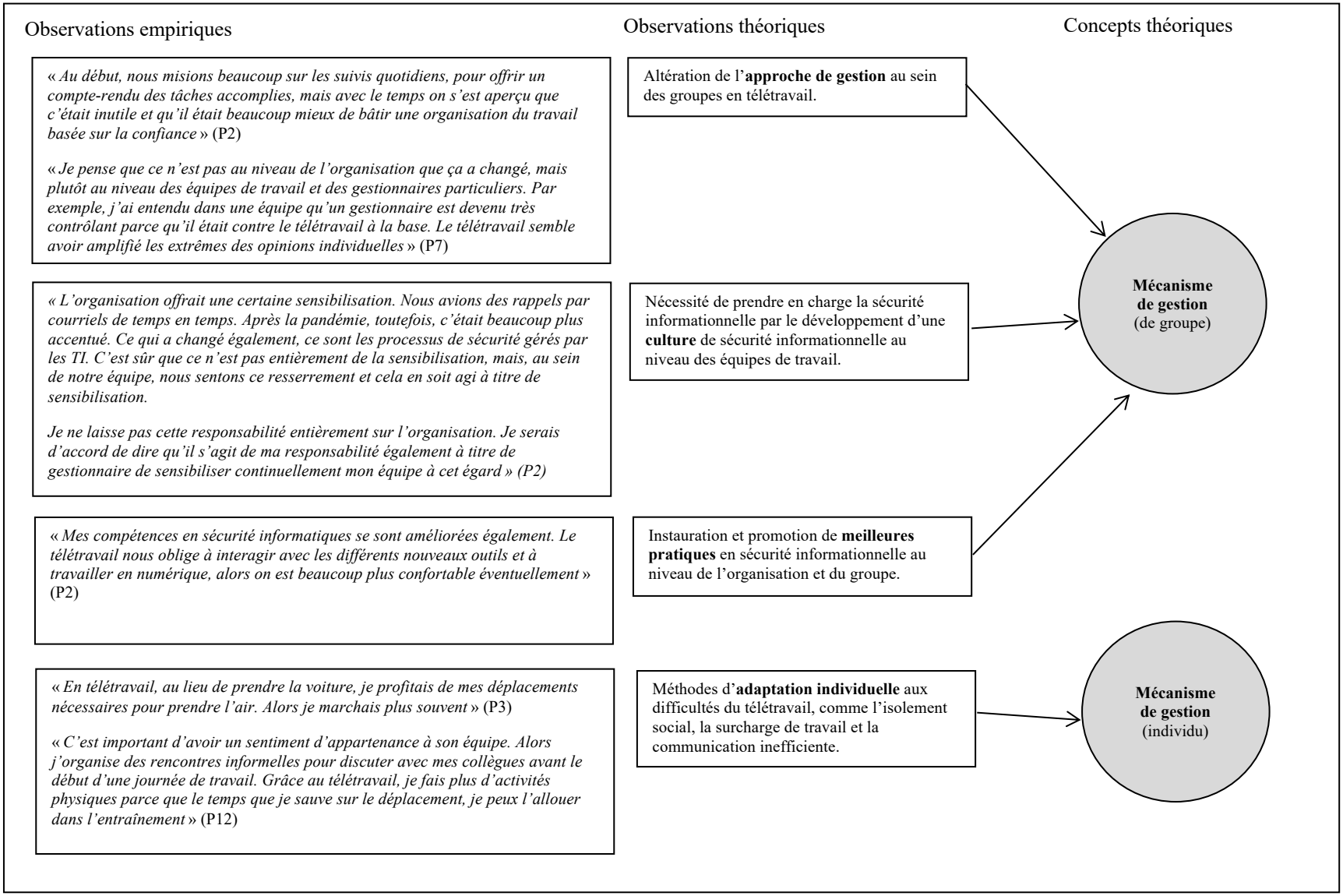
Structures de données pour la notion de télétravail et l'incidence sur la sécurité informationnelle



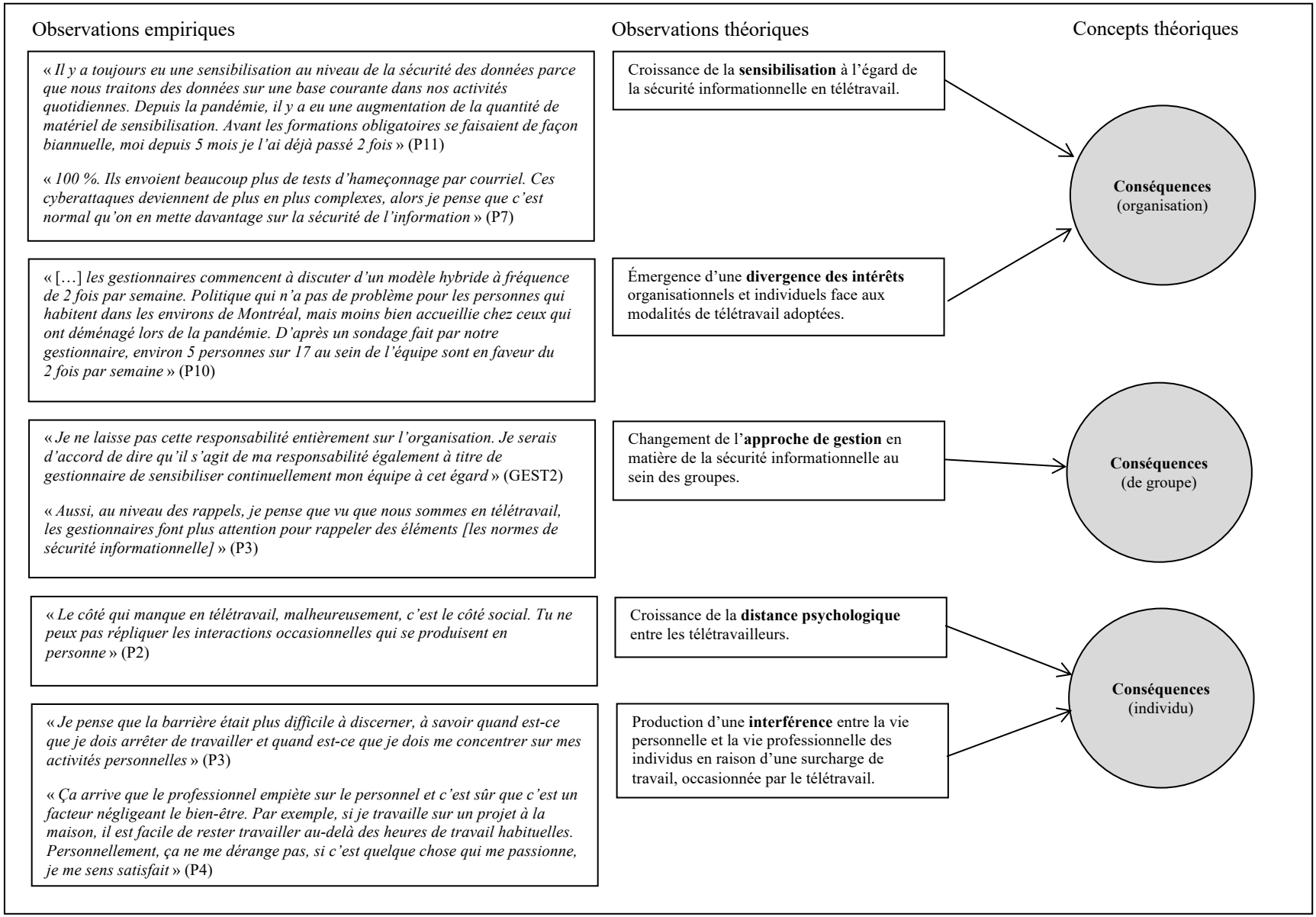
Structures de données pour la notion de télétravail et l'incidence sur la sécurité informationnelle (suite)



Structures de données pour la notion de télétravail et l'incidence sur la sécurité informationnelle (suite)



Structures de données pour la notion de sécurité informationnelle (suite)



Annexe 10 Guide d'entrevue utilisé pour la collecte des données

Le présent guide d'entrevue fut développé dans la perspective d'évaluer les concepts théoriques découlant de la revue de littérature, élaborée au chapitre 2. Puisque nous souhaitions ultimement évaluer l'incidence de l'adoption forcée du télétravail sur la sécurité informationnelle, à travers du « *pourquoi?* » et du « *comment?* », nous avons décidé de diviser nos questions en trois temporalités : préadoption, adoption et post-adoption. Ces parties sont subséquemment divisées en quatre sections thématiques : (1) le misfit, (2) les tensions, (3) les mécanismes de gestion, (4) les conséquences en SI.

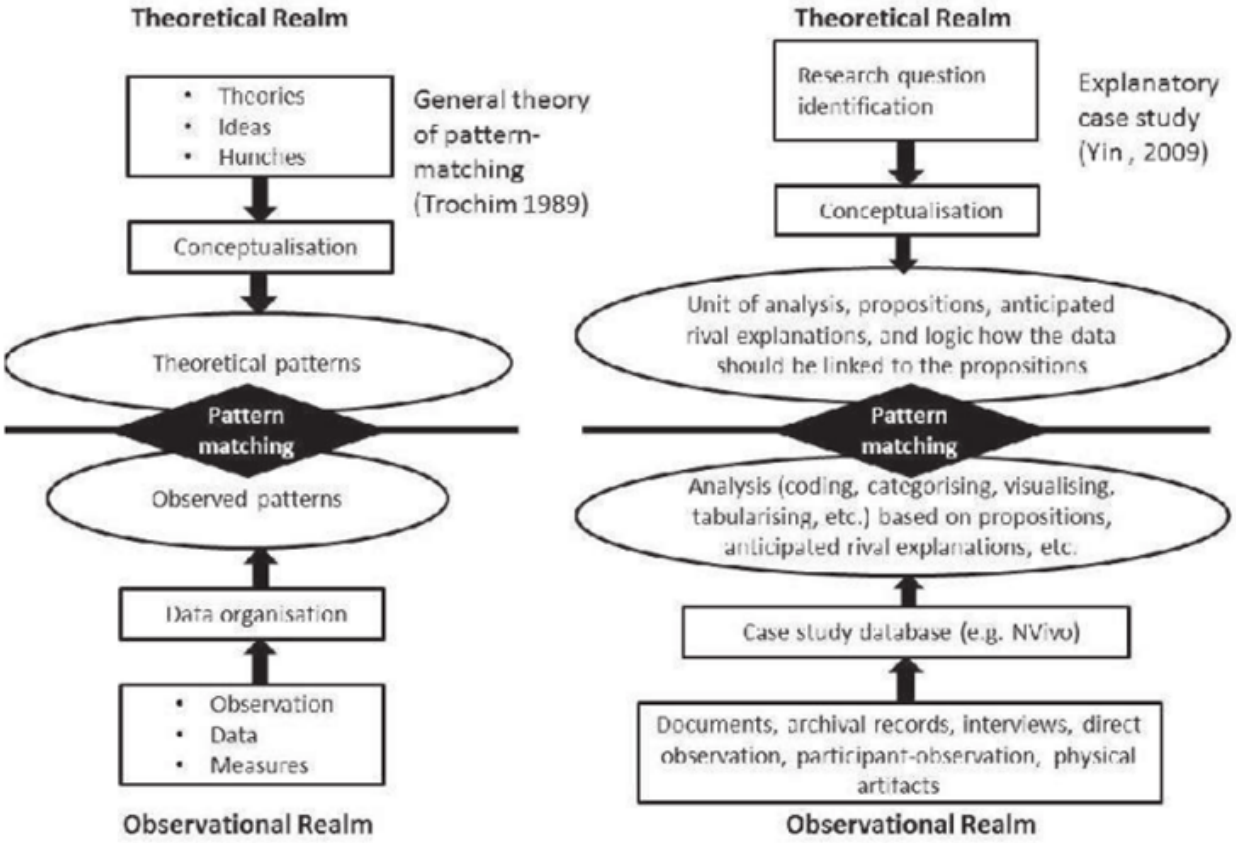
Période considérée	No.	Thème	Question	Objectif	Référence
Préadoption forcée	1	(1) Fit/Misfit	*Avant la pandémie, votre organisation permettait-elle le télétravail?*	Déterminer la présence d'un fit organisationnel, traduit par l'adoption hâtive du télétravail.	(Desilver, 2020)
Post-adoption forcée	2	(1) Fit/Misfit	*Actuellement, à quelle fréquence vous/votre équipe/votre organisation alloue le télétravail?*	Déterminer la présence d'un fit organisationnel, traduit par les modalités d'implantation actuelle.	(Desilver, 2020)
Adoption forcée	3	(1) Fit/Misfit	*Vous/votre équipe/votre organisation étiez-vous en faveur de l'implantation du télétravail, quand l'adoption forcée s'est fait? Quelles étaient vos principales attentes à cet égard?*	Déterminer la présence d'un fit du niveau d'étude qui est en entrevue. Pour un télétravailleur, demander « vous », pour un gestionnaire, « votre équipe » et ainsi de suite.	(Collins, 1998; Cooper *et al.*, 1990)
Préadoption forcée	4	(3) Mécanismes de gestion	*Avant l'adoption forcée, quelle importance vous/votre équipe/votre organisation accordiez-vous à l'utilisation des TIC et des données?*	Évaluer l'importance des systèmes d'information préalablement à l'implantation du télétravail.	(Pandey *et al.*, 2020)
Adoption forcée	5	(3) Mécanismes de gestion	*Vous/votre équipe/votre organisation a-t-elle adopté de nouvelles technologies suite à l'adoption forcée?*	Déterminer l'impact de l'implantation du télétravail sur les TIC.	(Clipper, 2020)
Préadoption forcée	6	(4) Conséquences en SI (1) Fit/Misfit	*Avant l'adoption forcée, diriez-vous que votre organisation offrait une sensibilisation adéquate à l'égard de la sécurité informationnelle? Si oui, quelles formes prenait cette sensibilisation?*	Déterminer l'importance de la culture de la sécurité informationnelle en organisation préalablement à l'implantation du télétravail.	(Beasley *et al.*, 2000)

Pré/Post-adoption forcée et période d'adoption forcée	7	(4) Conséquences en SI	*Au cours des trois dernières années, votre organisation a-t-elle déjà été impactée par une cyberattaque ou une fuite informationnelle? Quelle en était la cause? (Humaine ou technique)*	Déterminer l'occurrence des infiltrations et des fuites informationnelles avant le télétravail. Déterminer également la conscience des participants à cet égard.	(Kruse *et al.*, 2017).
Adoption forcée	8	(2) Tensions	*En adoption forcée, les modalités de travail offertes par votre organisation étaient-elles flexibles ou restrictives? (Contrôle — Liberté)*	Déterminer le positionnement organisationnel au niveau des tensions résultantes.	(Wang *et al.*, 2021)
Adoption forcée	9	(2) Tensions	*En adoption forcée…* *(1) Comment qualifieriez-vous l'environnement de travail au sein de votre équipe? (Communication, collaboration, support social)* *(2) Comment qualifieriez-vous le niveau d'isolement social? (Individualisme — Collectivisme)*	Déterminer le positionnement du groupe au niveau des tensions résultantes.	(Wang *et al.*, 2021)
Adoption forcée	10	(2) Tensions	*En adoption forcée…* *(1) Comment définiriez-vous votre niveau de bien-être en télétravail? Vous sentez-vous mieux qu'au bureau conventionnel?* *(2) Comment juriez-vous l'interférence entre la vie personnelle et le télétravail? (Mal-être — Bien-être)*	Déterminer le positionnement individuel au niveau des tensions résultantes.	(Wang *et al.*, 2021)
Adoption forcée	11	(3) Mécanismes de gestion	*En adoption forcée, comment vous/votre équipe/votre organisation gériez les difficultés résultantes de l'adoption forcée du télétravail?*	Déterminer les mécanismes de gestion des tensions résultantes des tensions.	(Wang *et al.*, 2021)
Adoption forcée	12	(3) Mécanismes de gestion (4) Conséquences en SI	*En adoption forcée, croyiez-vous que le style de gestion ait changé au sein de votre organisation/votre équipe? Si oui, de quelle façon?*	Déterminer l'impact du télétravail sur l'approche managériale.	(Abidoye, 2021)

Adoption forcée	13	(4) Conséquences en SI	*En adoption forcée…* *(1) Comment qualifieriez-vous la performance de vous/votre équipe/votre organisation?* *(2) Quels étaient les facteurs impératifs?*	Déterminer l'impact l'adoption forcée télétravail sur la performance organisationnelle, soit une conséquence soulevée à maintes reprises.	(Noble, 2007)
Post-adoption forcée	14	(4) Conséquences en SI	*Suite à la pandémie et l'adoption forcée du télétravail, diriez-vous que votre organisation offre davantage de sensibilisation à l'égard de la SI? Si oui, quelles formes prend cette sensibilisation?*	Déterminer l'importance de la culture de la sécurité informationnelle en organisation préalablement et suivant l'adoption forcée du télétravail.	(Da Veiga *et al.*, 2010)
Post-adoption forcée	15	(3) Mécanismes de gestion (4) Conséquences en SI	*(1) Jugez-vous que votre capacité à reconnaître les tentatives d'infiltrations des systèmes informatiques s'est améliorée ou détériorée?* *(2) Qu'en est-il de vos compétences informatiques?*	Évaluer l'impact de l'adoption forcée télétravail sur le niveau d'habiletés techniques individuelles et sur la vigilance.	(Wang *et al.*, 2021)
Pré/Post-adoption forcée	16	(4) Conséquences en SI	*(1) Au sein de votre organisation, quelles catégories de risques SI connaissez-vous?* *(2) Comment évalueriez-vous l'ordre de priorisation de ces risques?*	Évaluer la perception des risques informatiques et évaluer le niveau de sensibilisation des employés à l'égard des risques.	(Zhang *et al.*, 2010)
Ouverture	17	N/A	*En sommes, que pensez-vous de l'impact du télétravail sur la sécurité informationnelle au sein de votre organisation?*	Question d'ouverture pour offrir de nouvelles pistes, qui n'étaient pas explorées par les études préalables.	N/A

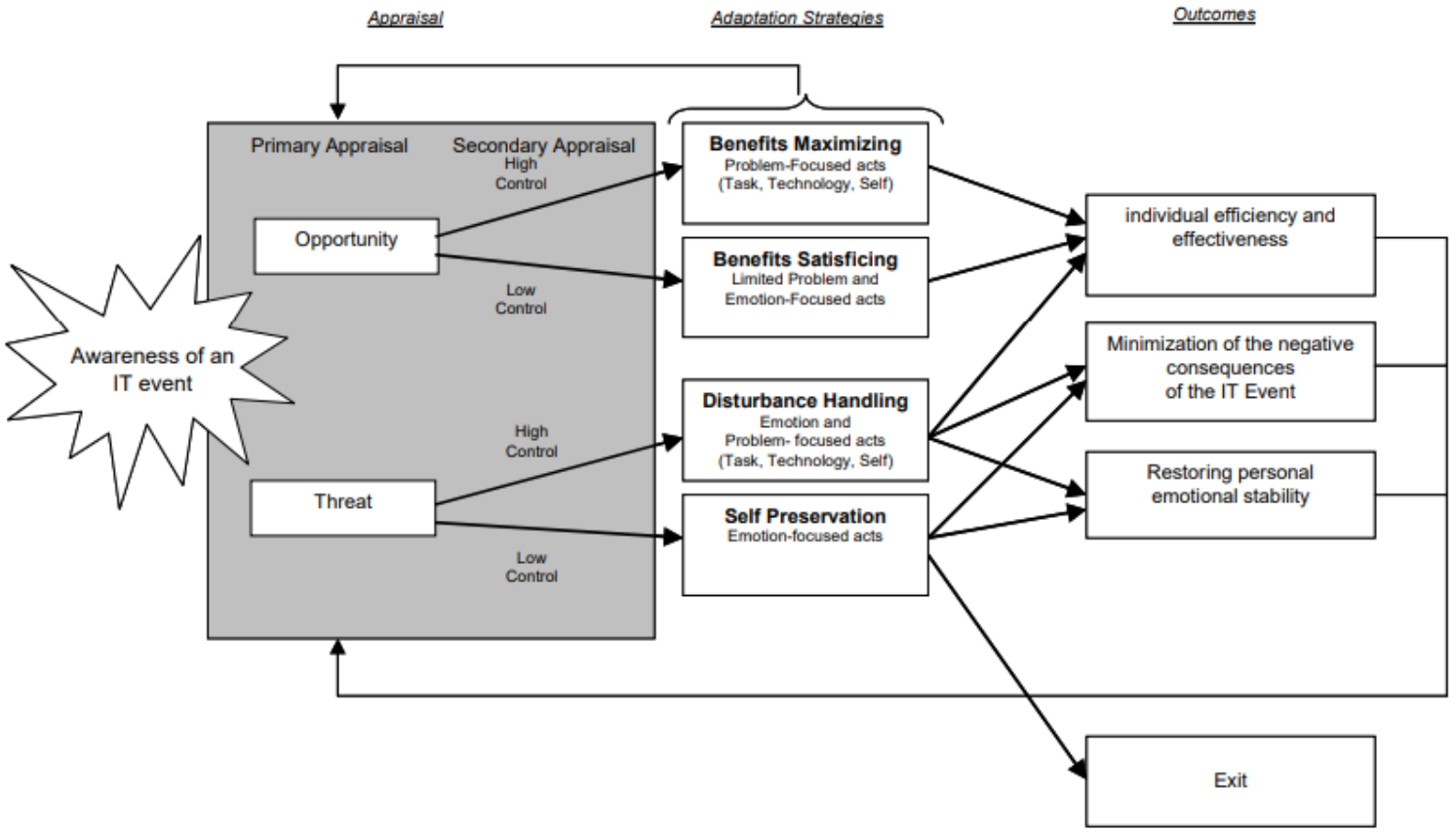
Annexe 11 Schématisation du *pattern-matching* (Sinkovics, 2019)

Le modèle ci-dessous présente la méthode de juxtaposition des patrons théoriques aux patrons observés, communément appelée « *pattern-matching* » (Sinkovics, 2018). Comme illustrée, elle est divisée en deux parties : (1) la partie théorique soit les intuitions, les idées et les concepts existants ; (2) la partie observée, soit les données issues des observations, des mesures et des entrevues.



Annexe 12 Adaptation individuelle (Beaudry *et al.*, 2005)

Ce modèle conceptuel schématise le processus d'adaptation individuelle des utilisateurs face à l'adoption d'une nouvelle technologie ou d'un événement d'implantation technologique, comme le télétravail. Ce processus est divisé en trois parties : (1) l'évaluation des conséquences ; (2) l'adoption de stratégies de contrôle des conséquences ; et (3) les conséquences des stratégies adoptées.



To simplify the illustration, we present pure forms of appraisal, i.e., where an IT event is monolithically appraised as constituting either a threat or an opportunity.

Bibliographie

Abidoye, Olurotimi (2021). *The significance of leadership style on the information security culture of mid-sized california law firms: A qualitative delphi study*, Capella University.

Abraham, Rene, Johannes Schneider et Jan Vom Brocke (2019). « Data governance: A conceptual framework, structured review, and research agenda », *International journal of information management*, vol. 49, p. 424-438.

Alberts, Christopher J et Audrey J Dorofee (2003). *Managing information security risks: The octave approach*, Addison-Wesley Professional.

Anderson, Deirdre et Clare Kelliher (2020). « Enforced remote working and the work-life interface during lockdown », *Gender in Management: An International Journal*, vol. 35, no 7/8, p. 677-683.

Anderson, James M (2003). « Why we need a new definition of information security », *Computers & security*, vol. 22, no 4, p. 308-313.

Angell, Robert Cooley (1936). « The family encounters the depression ».

Babapour Chafi, Maral, Annemarie Hultberg et Nina Bozic Yams (2022). « Post-pandemic office work: Perceived challenges and opportunities for a sustainable work environment », *Sustainability*, vol. 14, no 1, p. 294.

Bavik, Yuen Lam, Jason D Shaw et Xiao-Hua Wang (2020). « Social support: Multidisciplinary review, synthesis, and future agenda », *Academy of Management Annals*, vol. 14, no 2, p. 726-758.

Beaudry, Anne et Alain Pinsonneault (2005). « Understanding user responses to information technology: A coping model of user adaptation », *MIS quarterly*, p. 493-524.

Bélanger, France, Mary Beth Watson-Manheim et Bret R Swan (2013). « A multi-level socio-technical systems telecommuting framework », *Behaviour & Information Technology*, vol. 32, no 12, p. 1257-1279.

Bianchi, Suzanne M, Liana C Sayer, Melissa A Milkie et John P Robinson (2012). « Housework: Who did, does or will do it, and how much does it matter? », *Social forces*, vol. 91, no 1, p. 55-63.

Braun, Virginia et Victoria Clarke (2012). *Thematic analysis*, American Psychological Association.

Bulgurcu, Burcu, Hasan Cavusoglu et Izak Benbasat (2010). « Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness », *MIS quarterly*, p. 523-548.

Caspi, Gil, Uri Shalit, Søren Lund Kristensen, Doron Aronson, Lilac Caspi, Oran Rossenberg*, et al.* (2020). « Climate effect on covid-19 spread rate: An online surveillance tool », *MedRxiv*, p. 2020.2003. 2026.20044727.

Chung, Heejung et Tanja Van der Lippe (2020). « Flexible working, work–life balance, and gender equality: Introduction », *Social Indicators Research*, vol. 151, no 2, p. 365-381.

Clipper, Bonnie (2020). « The influence of the covid-19 pandemic on technology: Adoption in health care », *Nurse leader*, vol. 18, no 5, p. 500-503.

Collins, France Belanger Rosann Webb (1998). « Distributed work arrangements: A research framework », *The information society*, vol. 14, no 2, p. 137-152.

Cooper, Randolph B et Robert W Zmud (1990). « Information technology implementation research: A technological diffusion approach », *Management science*, vol. 36, no 2, p. 123-139.

Craigen, Dan, Nadia Diakun-Thibault et Randy Purse (2014). « Defining cybersecurity », *Technology Innovation Management Review*, vol. 4, no 10.

Cressey, Donald R (1950). « The criminal violation of financial trust », *American sociological review*, vol. 15, no 6, p. 738-743.

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.

Da Veiga, Adéle et Jan HP Eloff (2010). « A framework and assessment instrument for information security culture », *Computers & security*, vol. 29, no 2, p. 196-207.

Davis, Fred D (1989). « Perceived usefulness, perceived ease of use, and user acceptance of information technology », *MIS quarterly*, p. 319-340.

de Souza, Luciano Brandão et Michael Pidd (2011). « Exploring the barriers to lean health care implementation », *Public Money & Management*, vol. 31, no 1, p. 59-66.

Desilver, Drew (2020). « Before the coronavirus, telework was an optional benefit, mostly for the affluent few ».

Dhillon, Gurpreet et Ella Kolkowska (2011). « Can a cloud be really secure? A socratic dialogue », *Computers, privacy and data protection: an element of choice*, p. 345-360.

Di Martino, Vittorio et Linda Wirth (1990). « Telework: A new way of working and living », *Int'l Lab. Rev.*, vol. 129, p. 529.

Edmondson, Amy C et Stacy E McManus (2007). « Methodological fit in management field research », *Academy of management review*, vol. 32, no 4, p. 1246-1264.

Eisenhardt, Kathleen M (1989). « Building theories from case study research », *Academy of management review*, vol. 14, no 4, p. 532-550.

Ellison, Nicole B (1999). « Social impacts: New perspectives on telework », *Social science computer review*, vol. 17, no 3, p. 338-356.

Errichiello, Luisa et Tommasina Pianese (2016). « Organizational control in the context of remote work arrangements: A conceptual framework », dans *Performance measurement and management control: Contemporary issues*, Bradford, Emerald Group Publishing Limited, p. 273-305.

Fine, Gary Alan (1979). « Small groups and culture creation: The idioculture of little league baseball teams », *American sociological review*, vol. 44, no 5, p. 733-745.

Folkman, Susan (1992). « Making the case for coping ».

Gajendran, Ravi S et David A Harrison (2007). « The good, the bad, and the unknown about telecommuting: Meta-analysis of psychological mediators and individual consequences », *Journal of applied psychology*, vol. 92, no 6, p. 1524.

Grant-Vallone, Elisa J et Stewart I Donaldson (2001). « Consequences of work-family conflict on employee well-being over time », *Work & stress*, vol. 15, no 3, p. 214-226.

Griffith, Term L (1999). « Technology features as triggers for sensemaking », *Academy of management review*, vol. 24, no 3, p. 472-488.

Guba, Egon G et Yvonna S Lincoln (1994). « Competing paradigms in qualitative research », *Handbook of qualitative research*, vol. 2, no 163-194, p. 105.

Gudykunst, William B (1997). « Cultural variability in communication: An introduction », *Communication research*, vol. 24, no 4, p. 327-348.

He, Wu et Zuopeng Zhang (2019). « Enterprise cybersecurity training and awareness programs: Recommendations for success », *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no 4, p. 249-257.

Hill, E Jeffrey (1995). « The perceived influence of mobile telework on aspects of work life and family life: An exploratory study ».

Hochschild, Arlie et Anne Machung (1989). « Working parents and the revolution at home », *New York: Viking*.

Kaplan, Bonnie et Kimberly D Harris-Salamone (2009). « Health it success and failure: Recommendations from literature and an amia workshop », *Journal of the American Medical Informatics Association*, vol. 16, no 3, p. 291-299.

Katz, Jack (2001). « Analytic induction », *International encyclopedia of the social and behavioral sciences*, vol. 1, p. 480-484.

King, William R et Jun He (2006). « A meta-analysis of the technology acceptance model », *Information & management*, vol. 43, no 6, p. 740-755.

Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson et D Kyle Monticone (2017). « Cybersecurity in healthcare: A systematic review of modern threats and trends », *Technology and Health Care*, vol. 25, no 1, p. 1-10.

Ladan, Sh, A Yari et H Khodabandeh (2008). « Combination of information security standards to cover national requirements », *International Journal of Industrial and Manufacturing Engineering*, vol. 2, no 1, p. 36-40.

Lapointe, Liette et Suzanne Rivard (2005). « A multilevel model of resistance to information technology implementation », *MIS quarterly*, p. 461-491.

Lautsch, Brenda A, Ellen Ernst Kossek et Susan C Eaton (2009). « Supervisory approaches and paradoxes in managing telecommuting implementation », *Human Relations*, vol. 62, no 6, p. 795-827.

Lazarus, Richard S et Susan Folkman (1984). *Stress, appraisal, and coping*, Springer publishing company.

Lewis, James A (2006). « Cybersecurity and critical infrastructure protection », *Center for Strategic and International Studies*, vol. 9.

Lindesmith, Alfred R (1947). « Opiate addiction ».

Lojeski, Karen Sobel et Richard R Reilly (2008). *Uniting the virtual workforce: Transforming leadership and innovation in the globally integrated enterprise*, vol. 2, John Wiley & Sons.

Ma, Qingxiong, Allen C Johnston et J Michael Pearson (2008). « Information security management objectives and practices: A parsimonious framework », *Information Management & Computer Security*, vol. 16, no 3, p. 251-270.

Madlock, Paul E (2013). « The influence of motivational language in the technologically mediated realm of telecommuters », *Human Resource Management Journal*, vol. 23, no 2, p. 196-210.

Majchrzak, Ann et John Cotton (1988). « A longitudinal study of adjustment to technological change: From mass to computer-automated batch production », *Journal of Occupational Psychology*, vol. 61, no 1, p. 43-66.

Manzo, Lidia Katia C et Alessandra Minello (2020). « Mothers, childcare duties, and remote working under covid-19 lockdown in italy: Cultivating communities of care », *Dialogues in Human Geography*, vol. 10, no 2, p. 120-123.

Martins, Adéle et Jan Elofe (2002). *Information security culture*, Springer.

Mayer, Roger C., James H. Davis et F. David Schoorman (1995). « An integrative model of organizational trust », *Academy of management review*, vol. 20, no 3, p. 709-734.

Mokhtarian, PL et I Salomon (1993). *Modeling the choice of telecommuting: Setting the context. Working paper*.

Molino, Monica, Emanuela Ingusci, Fulvio Signore, Amelia Manuti, Maria Luisa Giancaspro, Vincenzo Russo*, et al.* (2020). « Wellbeing costs of technology use during covid-19 remote working: An investigation using the italian translation of the technostress creators scale », *Sustainability*, vol. 12, no 15, p. 5911.

Nanjundeswaraswamy, Terakanambi Shivashankar et Devappa Renuka Swamy (2014). « Leadership styles », *Advances in management*, vol. 7, no 2, p. 57.

Nilles, Jack M (1988). « Traffic reduction by telecommuting: A status review and selected bibliography », *Transportation Research Part A: General*, vol. 22, no 4, p. 301-317.

Noble, Bernard J (2007). *An investigation of the attitudes, costs and benefits of telework for information systems employees*, Nova Southeastern University.

Orlikowski, Wanda J (1996). « Improvising organizational transformation over time: A situated change perspective », *Information systems research*, vol. 7, no 1, p. 63-92.

Pandey, Neena et Abhipsa Pal (2020). « Impact of digital surge during covid-19 pandemic: A viewpoint on research and practice », *International journal of information management*, vol. 55, p. 102171.

Patton, Michael Quinn (1990). *Qualitative evaluation and research methods*, SAGE Publications, inc.

Pemble, Sara D (2020). *Factors associated with enhanced productivity of remote workers: A mixed method study*, University of Phoenix.

Peters, Pascale, Kea G Tijdens et Cecile Wetzels (2004). « Employees' opportunities, preferences, and practices in telecommuting adoption », *Information & management*, vol. 41, no 4, p. 469-482.

Poole, Marshall Scott et G DeSanctis (1990). « Of group decision support systems: The theory of adaptive structuration », *Organizations and communication technology*, vol. 173.

Raphael, Karen (1987). « Recall bias: A proposal for assessment and control », *International journal of epidemiology*, vol. 16, no 2, p. 167-170.

Robbins, Stephen P (2001). *Organisational behaviour: Global and southern african perspectives*, Pearson South Africa.

Saltzer, Jerome H et Michael D Schroeder (1975). « The protection of information in computer systems », *Proceedings of the IEEE*, vol. 63, no 9, p. 1278-1308.

Samonas, Spyridon et David Coss (2014). « The cia strikes back: Redefining confidentiality, integrity and availability in security », *Journal of Information System Security*, vol. 10, no 3.

Seemma, PS, S Nandhini et M Sowmiya (2018). « Overview of cyber security », *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no 11, p. 125.

Singer, Peter W et Allan Friedman (2014). *Cybersecurity: What everyone needs to know*, oup usa.

Sinkovics, Noemi (2019). « Pattern matching in qualitative analysis », *Sage Publications*.

Sweeney, Kathleen (2016). « Why the c-suite needs to get smart about cybersecurity », *Harvard Business Review*.

Taherdoost, Hamed (2016). « Sampling methods in research methodology; how to choose a sampling technique for research », *How to choose a sampling technique for research (April 10, 2016)*.

Tsohou, Aggeliki, Spyros Kokolakis, Costas Lambrinoudakis et Stefanos Gritzalis (2010). « A security standards' framework to facilitate best practices' awareness and conformity », *Information Management & Computer Security*, vol. 18, no 5, p. 350-365.

Tukey, John W (1980). « We need both exploratory and confirmatory », *The American Statistician*, vol. 34, no 1, p. 23-25.

Vargo, Deedra, Lin Zhu, Briana Benwell et Zheng Yan (2021). « Digital technology use during covid-19 pandemic: A rapid review », *Human Behavior and Emerging Technologies*, vol. 3, no 1, p. 13-24.

Vayansky, Ike et Sathish Kumar (2018). « Phishing–challenges and solutions », *Computer Fraud & Security*, vol. 2018, no 1, p. 15-20.

Velavan, Thirumalaisamy P et Christian G Meyer (2020). « The covid-19 epidemic », *Tropical medicine & international health*, vol. 25, no 3, p. 278.

Venkatesh, Viswanath, Michael G Morris, Gordon B Davis et Fred D Davis (2003). « User acceptance of information technology: Toward a unified view », *MIS quarterly*, p. 425-478.

Vivadelli, John H (2005). « The network of space (tm) and continuity of operations », *Public Manager*, vol. 34, no 3, p. 20.

Von Solms, Rossouw et Johan Van Niekerk (2013). « From information security to cyber security », *Computers & security*, vol. 38, p. 97-102.

Wang, Bin, Yukun Liu, Jing Qian et Sharon K Parker (2021). « Achieving effective remote working during the covid-19 pandemic: A work design perspective », *Applied psychology*, vol. 70, no 1, p. 16-59.

Warner, Michael (2012). « Cybersecurity: A pre-history », *Intelligence and National Security*, vol. 27, no 5, p. 781-799.

Watson-Manheim, Mary Beth et France Bélanger (2007). « Communication media repertoires: Dealing with the multiplicity of media choices », *MIS quarterly*, p. 267-293.

Whetten, David A (1989). « What constitutes a theoretical contribution? », *Academy of management review*, vol. 14, no 4, p. 490-495.

Wontorczyk, Antoni et Bohdan Rożnowski (2022). « Remote, hybrid, and on-site work during the sars-cov-2 pandemic and the consequences for stress and work engagement », *International Journal of Environmental Research and Public Health*, vol. 19, no 4, p. 2400.

Yakovleva, Maria, Richard R Reilly et Robert Werko (2010). « Why do we trust? Moving beyond individual to dyadic perceptions », *Journal of applied psychology*, vol. 95, no 1, p. 79.

Yin, Robert K (2003). « Designing case studies », *Qualitative research methods*, vol. 5, no 14, p. 359-386.