Université de Montréal

Gestionnaire de vie privée : un cadre pour la protection de la vie privée dans les interactions entre apprenants

par

Mouna Selmi

Département d'Informatique et de Recherche Opérationnelle

Faculté des Arts et des Sciences

Thèse présentée à la Faculté des Arts et des Sciences

en vue de l'obtention du grade de Philosophiae Doctor (Ph.D.)

en Informatique

Février, 2016

Résumé

L’évolution continue des besoins d’apprentissage vers plus d’efficacité et plus de personnalisation a favorisé l’émergence de nouveaux outils et dimensions dont l’objectif est de rendre l’apprentissage accessible à tout le monde et adapté aux contextes technologiques et sociaux. Cette évolution a donné naissance à ce que l’on appelle l'apprentissage social en ligne mettant l'accent sur l’interaction entre les apprenants.

La considération de l’interaction a apporté de nombreux avantages pour l’apprenant, à savoir établir des connexions, échanger des expériences personnelles et bénéficier d’une assistance lui permettant d’améliorer son apprentissage. Cependant, la quantité d'informations personnelles que les apprenants divulguent parfois lors de ces interactions, mène, à des conséquences souvent désastreuses en matière de vie privée comme la cyberintimidation, le vol d’identité, etc.

Malgré les préoccupations soulevées, la vie privée en tant que droit individuel représente une situation idéale, difficilement reconnaissable dans le contexte social d’aujourd’hui. En effet, on est passé d'une conceptualisation de la vie privée comme étant un noyau des données sensibles à protéger des pénétrations extérieures à une nouvelle vision centrée sur la négociation de la divulgation de ces données.

L’enjeu pour les environnements sociaux d’apprentissage consiste donc à garantir un niveau maximal d’interaction pour les apprenants tout en préservant leurs vies privées. Au meilleur de nos connaissances, la plupart des innovations dans ces environnements ont porté sur l'élaboration des techniques d’interaction, sans aucune considération pour la vie privée, un élément portant nécessaire afin de créer un environnement favorable à l’apprentissage.

Dans ce travail, nous proposons un cadre de vie privée que nous avons appelé « gestionnaire de vie privée». Plus précisément, ce gestionnaire se charge de gérer la protection des données personnelles et de la vie privée de l’apprenant durant ses interactions avec ses co-apprenants.

En s’appuyant sur l’idée que l’interaction permet d’accéder à l’aide en ligne, nous analysons l’interaction comme une activité cognitive impliquant des facteurs contextuels, d’autres apprenants, et des aspects socio-émotionnels. L'objectif principal de cette thèse est donc de revoir les processus d’entraide entre les apprenants en mettant en œuvre des outils nécessaires pour trouver un compromis entre l’interaction et la protection de la vie privée.

Ceci a été effectué selon trois niveaux : le premier étant de considérer des aspects contextuels et sociaux de l'interaction telle que la confiance entre les apprenants et les émotions qui ont initié le besoin d'interagir. Le deuxième niveau de protection consiste à estimer les risques de cette divulgation et faciliter la décision de protection de la vie privée. Le troisième niveau de protection consiste à détecter toute divulgation de données personnelles en utilisant des techniques d'apprentissage machine et d'analyse sémantique.

Mots-clés : apprentissage informel, vie privée, émotions, présence sociale, interactions sociales, protection de données personnelles, divulgation de données.

Abstract

The emergence of social tools and their integration in learning contexts has fostered interactions and collaboration among learners. The consideration of social interaction has several advantages for learners, mainly establishing new connections, sharing personal experiences and receiving assistance which may improve learning. However, the amount of personal information that learners disclose in these interactions, raise several privacy risks such as identity theft and cyberbullying which may lead to serious consequences.

Despite the raised concerns, privacy as a human fundamental right is hardly recognized in today's social context. Indeed, the conceptualization of privacy as a set of sensitive data to protect from external intrusions is no longer effective in the new social context where the risks come essentially from the self-disclosing behaviors of the learners themselves.

With that in mind, the main challenge for social learning environments is to promote social interactions between learners while preserving their privacy. To the best of our knowledge, innovations in social learning environments have only focused on the integration of new social tools, without any consideration of privacy as a necessary factor to establish a favorable learning environment. In fact, integrating social interactions to maintain learners' engagement and motivation is as necessary as preserving privacy in order to promote learning. Therefore, we propose, in this research, a privacy framework, that we called privacy manager, aiming to preserve the learners' privacy during their interactions.

Considering social interaction as a strategy to seek and request peers' help in informal learning contexts, we analyze learners' interaction as a cognitive activity involving contextual, social and emotional factors. Hence, our main goal is to consider all these factors in order to find a tradeoff between the advantages of interaction, mainly seeking peer feedback, and its disadvantages, particularly data disclosure and privacy risks.

This was done on three levels: the first level is to help learners interact with appropriate peers, considering their learning competency and their trustworthiness. The second level of protection is to quantify potential disclosure risks and decide about data disclosure. The third level of protection is to analyze learners' interactions in order to detect and discard any personal data disclosure using machine learning techniques and semantic analysis.

Keywords: informal learning, privacy, emotions, social presence, social interaction, personal data protection, data disclosure.

Table des matières

Table des matières ..... **iv**

Liste des tableaux ..... **viii**

Liste des figures ..... **ix**

Chapitre 1 : Introduction **1**

1.1. Contexte 1

1.2. Motivations 2

1.3. Objectifs de recherche 4

1.4. Organisation du document 5

Chapitre 2 : Environnements d'apprentissage et vie privée **7**

2.1. Environnements d'apprentissage en ligne 7

2.1.1. Apprentissage en ligne : théories et évolutions 7

2.1.2. Interaction dans les environnements d'apprentissage 10

2.1.3. Analyse des interactions 15

2.1.4. Présence sociale, socio-affective et apprentissage informel 17

2.1.5. Synthèse 20

2.2. Vie privée 21

2.2.1. Définitions et propriétés 21

2.2.2. Menaces en ligne 23

2.2.3. Nouvelles pratiques, nouvelles menaces 25

2.2.4. Problématiques de vie privée dans le contexte d'apprentissage en ligne 27

2.2.5. Protection de la vie privée : lois et outils 31

2.2.6. Conclusion 35

Chapitre 3 : Problématiques de recherche **37**

3.1. Paradoxe de vie privée 38

3.2. Problématiques 41
3.3. Gestionnaire de vie privée : une solution en trois axes 44
3.3.1. Cadres et fondements théoriques 45
3.3.2. Solution proposée 47
3.4. Conclusion 49
Chapitre 4 : Sélection des pairs 51
4.1. Interaction sociale, confiance et réputation 51
4.2. Systèmes de recommandation et apprentissage en ligne 52
4.3. Le module de sélection des pairs 54
4.3.1. Exigences d'un module de sélection des pairs 54
4.3.2. Architecture 55
4.3.3. Profil apprenant 58
4.3.4. Filtrage basé sur le contenu 59
4.3.5. Filtrage collaboratif basé sur la mémoire 61
4.3.6. Evaluateur de confiance 65
4.4. Implémentation du prototype 66
4.5. Tests et validation 68
4.6. Résultats 71
4.7. Conclusion 73
Chapitre 5 : Décision de divulgation de données 75
5.1. Divulgation de données : décision et facteurs 75
5.1.1. Prise de décision de divulgation/protection de vie privée 75
5.1.2. Facteurs influençant la décision de divulgation 76
5.1.3. Paradoxe de vie privée : solutions 77
5.2. Module de décision de divulgation proposé 77
5.2.1. Aperçu général du module décision 78

5.2.2. Modèle d'attaquant 79
5.2.3. Anonymisation des données 81
5.2.4. Estimation du risque 83
5.2.5. Décision de divulgation 86
5.3. Implémentation et prototype 91
5.4. Tests et validation 93
5.5. Conclusion 97
Chapitre 6 : Analyse d'interactions entre apprenants 99
6.1. Analyse d'interactions entre apprenants 99
6.1.1. Rôle des émotions dans l'interaction 100
6.1.2. Rôle de la protection de la vie privée dans l'interaction 101
6.2. Module d'analyse d'interactions proposé 102
6.2.1. Étape de fouille 102
6.2.2. Étape de composition 104
6.3. Expérimentations 111
6.3.1. Caractéristiques du corpus étudié 112
6.3.2. Protocole expérimental 113
6.3.3. Évaluation de l'étape de fouille 114
6.3.4. Évaluation de l'étape de composition 115
6.4. Résultats et discussion 116
6.4.1. Résultats de l'étape de fouille 116
6.4.2. Résultats de l'étape de composition 118
6.5. Conclusion 121
Chapitre 7 : Étude de cas de la cyberintimidation 123
7.1. Interaction et cyberintimidation 123
7.2. Hypothèses et modèle de recherche 124

7.2.1. Personnalité, comportement en ligne et perpétration d'actes de cyberintimidation 125
7.2.2. Personnalité, comportement en ligne et victimisation 126
7.2.3. Impact de la victimisation sur la perpétration d'actes de cyberintimidation..... 127
7.3. Méthodologie 129
7.3.1. Objectif de la présente étude 129
7.3.2. Données et Échantillon..... 129
7.3.3. Instruments de mesures 131
7.4. Résultats 134
7.4.1. Présentation des résultats préliminaires 135
7.4.2. Test des modèles de mesure 136
7.4.3. Test du modèle structurel 139
7.5. Discussion 143
7.6. Conclusion..... 145
Chapitre 8 : Conclusions..... 147
8.1. Contributions..... 147
8.2. Travaux futurs 150
Bibliographie..... 153
Publications..... 164

Liste des tableaux

Table 1– Exemple de données du profil apprenant 59

Table 2 – Exemple de table d'apprenants non anonyme 82

Table 3 – Table anonymisée par généralisation et suppression 82

Table 4 – Exemple de pairs sélectionnés 89

Table 5 – Scénario d'exécution et données à divulguer 94

Table 6 – Scénario d'exécution et pairs sélectionnés 94

Table 7 – Scénario d'exécution et première itération du calcul 95

Table 8 – Scénario d'exécution et itérations du calcul 96

Table 9 – Scénario d'exécution et décision de divulgation 96

Table 10 – Comparaison avec des travaux similaires 97

Table 11 – Exemple de matrice d'occurrences 106

Table 12 – Exemple d'interactions entre apprenants 113

Table 13 – Corrélation entre variables indépendantes et scores humains 116

Table 14 – Résultats de la classification des feedbacks 117

Table 15 – Caractéristiques démographiques des participants 131

Table 16 – Cohérence interne des facteurs 138

Table 17 – Matrice de corrélation des facteurs et racine carrée de l'AVE 139

Table 18 – Valeurs de AFC et MES des indices d'ajustement du modèle 140

Table 19 – Résultats de test d'hypothèses 140

Liste des figures

Figure 1 – Types d'apprentissage basés sur l'interaction 11

Figure 2 – Facteurs entourant l'apprentissage informel (Balsam et Tomie, 2014) 12

Figure 3 – Exemple d'activité d'aide entre apprenants sur Livemocha 13

Figure 4 – Les trois dimensions de la présence (Jézégou, 2010) 16

Figure 5 – Architecture générale du cadre proposé 48

Figure 6 – Architecture du module proposé 57

Figure 7 – Exemple de matrice de filtrage basé sur le contenu 60

Figure 8 – Matrice Apprenants x Apprenants connectés 62

Figure 9 – Exemple de filtrage collaboratif 63

Figure 10 – Interface d'écriture d'une requête 67

Figure 11 – Interface de réponse à une requête 68

Figure 12 – Exemple des notes attribuées par deux apprenants initiaux 69

Figure 13 – Attribution des notes par les apprenants supplémentaires de a_1 (b_1,…, b_{10}) 70

Figure 14 – Résultat de comparaison de MAE 71

Figure 15 – Interprétation de MAE MOY 73

Figure 16 – Aperçu général du module décision de divulgation proposé 79

Figure 17 – Croisement de deux bases de données par Sweeney (2002) 81

Figure 18 – Aperçu de l'algorithme du module décision de divulgation 90

Figure 19 – Préférences de divulgation 91

Figure 20 – Notification du risque élevé 92

Figure 21 – Pseudocode de Datafly (Sweeney, 1998) 92

Figure 22 – Architecture du module composition des feedbacks 102

Figure 23 – Exemple de matrice de valeurs singulières 107

Figure 24 – Exemple de matrice approchée de A au rang 3 108

Figure 25 – Interaction entre dimensionnalité et pondération 118

Figure 26 – Interaction entre dimensionnalité et mesure de similarité 119

Figure 27 – Modèle et hypothèses de recherche 128

Figure 28 – Formulaire de consentement 130

Figure 29 – Modèle final estimé de la victimisation 141

Figure 30 – Modèle structurel de la perpétration d'actes de cyberintimidation 142

À mes parents

Remerciements

Mes premiers remerciements vont à Professeure Esma Aïmeur, ma directrice de thèse, pour son encadrement scientifique pendant toutes ces années. Je lui témoigne ma reconnaissance pour sa confiance, sa disponibilité, son soutien et ses précieux conseils et critiques.

Je lui suis, par ailleurs, reconnaissante de nos échanges enrichissants et de m'avoir fait confiance pour la réalisation de plusieurs tâches : tout cela a contribué à faire de ces années de doctorat une expérience passionnante.

Mes seconds remerciements sont dus à celui qui a codirigé mes recherches, Docteur Hicham Hage, pour sa disponibilité, ses feedback pertinents et ses relectures critiques : je lui suis reconnaissante pour son précieux soutien tout au long de ce travail.

Je souhaite remercier également Thierry Eude d'avoir accepté d'être examinateur de cette thèse, Louis Salvail et Claude Frasson d'avoir accepté d'être président et membre du jury.

Je souhaite remercier infiniment le gouvernement Tunisien et la Mission Universitaire de Tunisie en Amérique du Nord de m'avoir accordée la bourse d'excellence sans quoi cette recherche n'aurait jamais eu lieu.

Ce parcours de doctorat m'a offert la chance d'intégrer le laboratoire HERON qui a été un cadre idéal pour la recherche. Ma reconnaissance va vers les membres de ce laboratoire de recherche pour le soutien qu'ils m'ont apportée et la sympathie qu'ils m'ont témoignée.

J'adresse des remerciements particuliers à Rémi, Nicolas, et Djamel qui ont contribué à certains travaux.

Un grand merci à mes collègues doctorants et jeunes chercheurs qui m'ont encouragée et avec qui j'ai partagé tous les états d'âme que seule la recherche doctorale peut susciter.

Enfin, je remercie infiniment ma sœur pour ses relectures, son soutien et sa présence rassurante pour moi bien plus que je ne saurais l'exprimer ici.

Chapitre 1 : Introduction

1.1. Contexte

Ce travail trouve ses origines dans la participation à un projet de recherche mené au sein de notre laboratoire. Le projet, intitulé « *Privacy in the age of exposure* », s'intéresse à la protection de la vie privée dans le contexte actuel de socialisation numérique qui s'articule autour de deux tendances : *divulguer* et *interagir*. En effet, les individus *divulguent* des *informations personnelles* et exposent une part toujours croissante et sensible de leurs données personnelles sur les réseaux sociaux et dans leurs *interactions sociales*.

La banalisation de ces pratiques d'auto-divulgation et d'exposition de soi pose plusieurs risques en matière de vie privée et conduit à son érosion progressive. Malgré le flou épistémologique, juridique, éthique et social qui entoure cette notion de vie privée (Latzko-Toth et Pastinelli, 2014), l'apparition des technologies de socialisation numérique a conduit à sa remise en question comme étant un droit individuel et fondamental (Tubaro *et al.*, 2014). En effet, elle est vue aujourd'hui comme une contrainte à la liberté d'expression, à la liberté de l'information et à la visibilité sociale. Ainsi, après avoir été encouragé à se protéger et à préserver sa vie privée, l'individu est aujourd'hui poussé à divulguer et à révéler de plus en plus des données pour accéder à des services (Aïmeur *et al.*, 2016).

Une réflexion sur la transmission de cette pratique de divulgation et les risques inhérents dans les contextes d'apprentissage nous a conduits, pour notre recherche, à limiter notre analyse de la divulgation de données personnelles aux situations d'apprentissage social et plus particulièrement à l'apprentissage social *non formel*. Nous nous intéressons donc aux problèmes de la vie privée et sa préservation lorsque la divulgation de données personnelles est le produit d'interactions sociales dont le but est de s'entraider et de coopérer pour comprendre et construire de nouvelles connaissances (par exemple les réseaux sociaux d'apprentissage des langues tels que *Babbel*, *Livemocha*, les communautés de questions réponses telles que Quora, Stack Overflow, etc.). Dans cette thèse, nous utilisons les termes *non formel* ou *informel* pour renvoyer à ce type d'apprentissage.

L'étude de l'interaction et l'entraide dans les situations d'apprentissage non formel (ou informel) nous amène à discuter les principales motivations de cette recherche que nous détaillons dans la section suivante.

1.2. Motivations

Cette recherche s'articule principalement autour de deux thématiques, à savoir : **(1)** *les interactions entre apprenants dans les contextes d'apprentissage social non formel* **(2)** *la divulgation de données personnelles dans ces interactions et les risques encourus en matière de vie privée*. Pour expliquer la relation entre ces deux thématiques et l'intérêt de les étudier nous commençons par souligner le rôle de l'interaction dans l'apprentissage et ensuite nous évoquons les risques de vie privée que posent les interactions sociales dans les contextes d'apprentissage non formel.

L'environnement social dans lequel l'apprenant évolue influence le processus cognitif en motivant l'apprenant ou non à résoudre le déséquilibre interindividuel lié à la construction de la connaissance. Dans cette optique, Johnson *et al.* (2000) ont avancé que les relations sociales ont un grand impact sur le type d'interactions dans un contexte d'apprentissage, car elles présentent généralement un caractère conflictuel. La résolution des conflits prend alors des formes distinctes selon la situation d'interaction : une situation *coopérative* autorise une résolution saine et constructive des conflits interindividuels, tandis qu'une situation *compétitive* est à l'origine d'une résolution malsaine et négative de ces mêmes conflits.

Les interactions sociales entre apprenants constituent une pertinence et une spécificité en tant qu'objets d'étude scientifique, surtout depuis l'apparition des environnements d'apprentissage social informel en ligne utilisés en marge des contextes institutionnels tels que les forums de discussion, les réseaux sociaux d'apprentissage et les communautés virtuelles.
Bien que ces environnements aient l'avantage d'élargir l'espace de coopération entre apprenants, ils ont apporté un certain nombre de pratiques qui peuvent être source de *stress* et de *vulnérabilité* chez les apprenants et peuvent générer des *risques en matière de vie privée*. Parmi ces pratiques, nous nous intéressons principalement à la **divulgation de données personnelles**.

Dans les faits, beaucoup d'apprenants croient que la divulgation de données dans les contextes d'apprentissage informel est sans risque et qu'ils sont encouragés à partager plus de renseignements personnels afin de renforcer leur présence sociale et de maximiser leurs

opportunités d'apprentissage. Pourtant l'atteinte de la vie privée provient aujourd'hui surtout de la divulgation de données dans les interactions sociales en ligne (Steeves, 2009).

Pour mieux illustrer notre propos, prenons l'exemple d'un apprenant *Bob* qui s'est inscrit sur un réseau social pour apprendre l'Anglais. Afin de maximiser ses chances de trouver des partenaires d'apprentissage de même langue, âge, origine, etc., Bob (1) *a divulgué* de nombreuses informations à propos de lui-même incluant des **données non nécessaires** pour son objectif d'apprentissage comme sa date de naissance et son courriel.

À chaque fois qu'il rencontrait un problème durant son apprentissage, Bob (2) *ne savait pas à qui s'adresser pour avoir de l'aide*. Ainsi, il n'avait que la possibilité de poser une question que ses co-apprenants pouvaient la voir ainsi que toutes ses données divulguées.

En réponse à ses demandes d'aide, Bob (3) *recevait un grand nombre de feedbacks* donnés par ses co-apprenants dont certains étaient *pertinents répondant à sa requête* et d'autres *non pertinents affectant négativement son apprentissage*. En guise d'exemples, en réponse à l'une des requêtes de Bob, un co-apprenant lui répondait : « *Encore une question débile...*», un autre lui écrivait : « *ça me rassure que tu ne viennes pas du Québec* ».

La réception de ces *feedbacks négatifs* le ridiculisant suite à sa demande d'aide a découragé Bob d'adresser d'autres requêtes à ses pairs et a créé un espace socio-affectif non favorable à l'entraide entre apprenants.

Bien qu'il soit fictif, ce scénario illustre trois problèmes pouvant survenir dans les contextes d'apprentissage social informel, à savoir *le besoin d'être accompagné dans la recherche des pairs appropriés*, *la divulgation excessive des données personnelles* et *le besoin d'être accompagné dans la recherche de contenus pertinents.* Ceci étant dit, résoudre ces problèmes revient à améliorer les interactions entre apprenants afin de faciliter l'entraide et à trouver un compromis entre la protection de la vie privée et la divulgation de données personnelles. C'est ce à quoi nous tentons de répondre dans cette thèse.

Dans la section suivante, nous présentons les objectifs de cette recherche en réponse aux trois problèmes évoqués ci-haut.

1.3. Objectifs de recherche

Nos travaux de recherche visent à soutenir l'entraide dans l'apprentissage social informel et à préserver la vie privée en contextualisant la divulgation de données personnelles aux besoins d'apprentissage. Plus précisément, nous proposons de réaliser les trois objectifs suivants :

1. **Proposer un module de sélection des partenaires d'interaction appropriés :** notre premier objectif est de soutenir l'apprentissage social informel en proposant un module sélectionnant les pairs appropriés pour fournir l'aide, tout en tenant compte aussi bien des facteurs de compétence liés à l'apprentissage que des facteurs sociaux nécessaires pour préserver la vie privée comme *la confiance* et *la réputation*.
2. **Proposer un module de décision de divulgation des données :** notre deuxième objectif est de proposer un module qui permet de trouver un *compromis entre divulgation de données personnelles* et *protection de la vie privée* dans une situation d'interaction entre apprenants visant l'entraide et la réponse à un besoin d'apprentissage. Plus précisément, notre objectif est d'estimer les risques et les avantages de la divulgation pour proposer une meilleure décision de protection.
3. **Proposer un module d'analyse d'interactions :** finalement, notre troisième objectif est de proposer un module d'analyse d'interactions sociales entre apprenants dans le but, d'une part, d'aider l'apprenant à trouver les contenus pertinents, étant donné son *besoin d'apprentissage* et *son état émotionnel* et, d'autre part, de préserver sa vie privée en omettant tout feedback pouvant influencer négativement son apprentissage. Cela devrait appuyer le sentiment de présence sociale entre apprenants dans les contextes d'apprentissage informel.

Afin de répondre à ces objectifs, nous proposons un *cadre de vie privée*, que nous avons appelé « gestionnaire de vie privée», composé de trois modules associés aux objectifs évoqués ci-haut : le premier module, *Sélection des pairs*, se base sur des algorithmes de filtrage afin de sélectionner des pairs appropriés pour fournir l'aide. Le module proposé tient compte, dans le processus de sélection, de la compétence et de la réputation des pairs afin d'assurer une bonne réponse à la requête d'aide et une interaction préservant la vie privée.

Le deuxième module, *Décision de divulgation*, se charge d'estimer les risques de la divulgation en se basant sur *l'information mutuelle*. Pour contextualiser la divulgation au besoin de l'apprentissage, la décision de divulguer ou de retenir une donnée considère les

préférences de divulgation de l'apprenant en question (1), les pairs sélectionnés pour fournir l'aide (2), l'utilité de chaque donnée (3) et le risque potentiel de sa divulgation (4).

Enfin le dernier module, *Composition des feedbacks*, a pour rôle d'analyser les feedbacks des pairs en réponse à une requête d'aide en tenant compte du contenu de la requête elle-même et de l'état émotionnel de l'apprenant qui l'a émise. Ce **premier niveau** d'analyse se base sur des techniques *d'analyse des sentiments* pour omettre les feedbacks pouvant influencer négativement l'apprentissage. Le **deuxième niveau** d'analyse concerne la protection de la vie privée et a pour rôle de détecter et de supprimer toute divulgation non intentionnelle des données personnelles en utilisant des techniques d'analyse sémantique, plus précisément *Analyse Sémantique Latente* (ou *Latent Semantic Analysis* en anglais).

1.4. Organisation du document

Ce travail est organisé en *huit* chapitres. **Le premier chapitre** concerne l'interaction dans les situations d'apprentissage social informel et les risques inhérents en matière de vie privée. Nous nous interrogeons sur la pratique de divulgation de données personnelles en nous focalisant sur les activités d'aide et les interactions dans les environnements d'apprentissage informel sur lesquels porte principalement cette recherche.

Les approches théoriques et méthodologiques qui ont guidé ce travail sont décrites dans le second et le troisième chapitre. **Le second chapitre** est divisé sur deux parties. La *première* est consacrée au rôle de l'interaction dans l'accomplissement de l'entraide. L'interaction, dans ce qu'elle permet d'accéder à celle-ci, est vue à la fois comme un résultat de l'évolution des théories d'apprentissage et un besoin imposé par l'évolution technologique et sociale (Duplàa et Talaat, 2012). Nous montrons que le déploiement récent des apprentissages *informels* oblige à revoir la conceptualisation de l'interaction. Dans cette optique, interagir est devenu une stratégie d'auto-socio-construction des connaissances (Pélissier et Metz, 2010)

La seconde partie du deuxième chapitre s'intéresse à la question de divulgation de données lors des interactions et les risques inhérents à celle-ci. Nous expliquons dans un premier temps l'importance de considérer la vie privée dans les situations d'interactions et les activités d'entraide. Nous faisons état dans un second temps des enjeux méthodologiques liés à la protection de la vie privée dans ce type d'apprentissage, notamment la question de *paradoxe de vie privée*.

Le chapitre 3 est consacré à la présentation des problématiques étudiées dans cette thèse et les axes et méthodologie de recherche adoptés. Ce chapitre est l'occasion de faire un état de l'art des problématiques au centre des travaux portant sur les facteurs déterminants le paradoxe de vie privée dans les situations d'apprentissage social. Il présente une synthèse des limites de ces travaux pour positionner les contributions de cette thèse par rapport à la littérature. Ensuite, il fait état des travaux qui ont fortement inspiré notre démarche de recherche de compromis entre divulgation et protection de vie privée.
Finalement, il donne un aperçu de la solution que nous proposons incluant les axes de recherche que nous étudions dans cette thèse en réponse à la problématique de la protection de la vie privée dans les interactions entre apprenants.

Les **chapitres 4, 5** et **6** sont consacrés à **nos contributions**. **Le chapitre 4** est consacré à notre module de sélection des pairs pour fournir l'aide. **Le chapitre 5** présente notre module d'estimation des risques potentiels de la divulgation de données personnelles et de décision de protection de vie privée. **Le chapitre 6** introduit le rôle des *émotions* et de la *protection de la vie privée* dans l'analyse des interactions. Il présente le module composition qui classifie et analyse les feedbacks des pairs dans le but d'omettre les feedbacks négatifs et ceux divulguant des données personnelles. Ce chapitre présente également les résultats de *deux expérimentations* que nous avons menées pour évaluer la performance du module proposé.

Finalement, **le chapitre 7** présente une étude de cas ayant pour but d'examiner l'un des risques les plus répandus dans les interactions sociales entre apprenants : *la cyberintimidation*. Nous étudions dans ce chapitre les corrélations entre les variables de risque et de protection examinées dans cette recherche et la probabilité de risque de cyberintimidation. Pour cela, nous formulons un ensemble d'hypothèses et nous menons une étude empirique sur *Amazon Mechanical Turk* pour les valider.
Le chapitre se termine par une discussion des résultats de l'étude montrant la prévalence de la cyberintimidation et discutant le rôle des facteurs qui augmentent les risques de victimisation, plus particulièrement l'auto-divulgation.

En conclusion, **le chapitre 8** résume les contributions de cette thèse, les limites de nos travaux et les perspectives de nos recherches.

Chapitre 2 : Environnements d'apprentissage et vie privée

L'évolution permanente des besoins d'apprentissage vers plus d'efficacité, plus de flexibilité et plus de personnalisation a favorisé l'émergence de nouveaux outils pédagogiques et informatiques dont l'objectif est de rendre l'apprentissage accessible à tout le monde et adapté aux évolutions sociales et technologiques.

Les nouvelles technologies ont amené plusieurs avantages ainsi que des défis aussi bien pour les apprenants que pour les concepteurs et développeurs des environnements d'apprentissage en ligne (Duplàa et Talaat, 2012). Parmi ces défis, nous nous intéressons à ceux liés aux interactions entre apprenants dans les contextes de demande d'aide. Nous nous focalisons surtout sur les risques qui touchent la vie privée de l'apprenant lors de ses interactions avec ses co-apprenants ainsi que les solutions potentielles pour sa protection.

La première partie de ce chapitre est consacrée à la présentation des environnements d'apprentissage et leur évolution, tandis que la deuxième partie s'intéresse surtout aux atteintes à la vie privée, générées par cette évolution.

2.1. Environnements d'apprentissage en ligne

Nous présentons, dans cette section, l'évolution des théories d'apprentissage ainsi que les environnements virtuels d'apprentissage qui en résultent. Cette revue nous conduit à une distinction importante entre deux types d'environnements d'apprentissage en ligne : d'un côté les plateformes d'apprentissage formel et de l'autre ce que nous appellerons les environnements d'apprentissage « *non formel* ». Nous montrons les particularités de ces deux types d'environnements tout en mettant l'accent sur l'interaction comme moyen pour favoriser l'aide entre apprenants.

2.1.1. Apprentissage en ligne : théories et évolutions

Le paradigme de l'apprentissage évolue au fil des années et s'enrichit de nouveaux concepts et théories. L'objectif de ces dernières est d'expliquer le processus d'apprentissage en étudiant les différents facteurs qui peuvent l'influencer ainsi que leurs impacts (Hofer, 2001).

Théories d'apprentissage

Une majorité de théoriciens en éducation s'accordent pour regrouper les théories de l'apprentissage selon quatre courants : le *béhavioriste*, le *cognitiviste*, le *constructiviste* et le *socio-constructiviste* (John-Steiner et Mahn, 1996; Vygotsky, 1987). Bien que ce dernier courant ait été prolongé pour suivre les évolutions technologiques actuelles, le nouveau paradigme, dit *connectivisme*, n'a pas reçu autant d'attention de la part des chercheurs en éducation que les quatre courants susmentionnés (Skinner, 2011).

Le béhaviorisme est une théorie de l'apprentissage qui s'intéresse surtout à l'étude des comportements observables (Skinner, 2011). Cette théorie considère l'apprentissage comme une modification du comportement basée sur l'acquisition des connaissances par des entrainements successifs et enchainés (Borich et Tombari, 1997). De là sont issus les environnements de l'enseignement programmé et l'enseignement assisté par ordinateur (EAO) (Simonson *et al.*, 2011).

Miller et Bruner ont critiqué cette théorie en énonçant que l'apprentissage n'est pas limité à un enregistrement des connaissances, mais doit plutôt être envisagé comme nécessitant un traitement complexe de l'information reçue (Skinner, 2011). Basée sur le traitement et l'organisation des connaissances, une nouvelle théorie dite le cognitivisme (ou rationalisme) a vu le jour (Simonson *et al.*, 2011). La critique principale qui a été adressée au cognitivisme est que le traitement des connaissances seul n'est pas suffisant pour assurer l'apprentissage.

Contrairement aux behavioristes, les constructivistes croient que l'acquisition des connaissances ne se réalise pas par simple empilement mais passe par une construction ou reconstruction de conceptions mentales précédentes (O'loughlin, 1992). Aujourd'hui, le constructivisme apparait toujours prometteur du point de vue des technologies éducatives et apprentissage en ligne. Il favorise des outils donnant une grande autonomie à l'apprenant et une grande personnalisation lui permettant d'avancer à son rythme.

Une prolongation de l'approche constructiviste a été jugée nécessaire par Vygotsky (1987) qui a repris les principes de cette approche en y introduisant une dimension supplémentaire, celle des interactions, des échanges, et de co-construction des connaissances. Pour l'auteur, l'apprentissage est un processus interactif dans lequel les gens apprennent les uns des autres. Dans cette perspective, l'idée d'une construction sociale de l'intelligence est prolongée par l'idée d'une *auto-socio-construction* des connaissances par les apprenants.

Les principes de ces théories d'apprentissage ont été utilisés pour expliquer et soutenir l'apprentissage présentiel ainsi que celui à distance et en ligne. Afin de répondre aux besoins des apprenants, les environnements d'apprentissage en ligne ont subi des mutations continues tout en adoptant de nouvelles dimensions afin de faire évoluer l'apprentissage.

Évolution des environnements d'apprentissage en ligne

L'évolution des théories d'apprentissage est due en partie aux évolutions sociales et technologiques qui influencent grandement tous les aspects de l'homme et notamment son apprentissage (Duplàa et Talaat, 2012). Les concepteurs des environnements d'apprentissage en ligne ont vu dans cette évolution une opportunité pour pousser les limites et surmonter la distance en tant qu'obstacle éventuel pour l'apprentissage en ligne. Cela a contribué à mettre l'accent sur l'importance de la notion d'interaction dans les situations d'apprentissage (Foucher et Pothier, 2007). Plusieurs dispositifs d'apprentissage ont alors intégré des technologies d'interaction et de communication comme les Systèmes Tutoriels Intelligents et les environnements CSCL (*Computer Supported Collaborative Learning*).

Les objectifs principaux de l'interaction dans ces environnements sont, d'une part, de surmonter le problème d'isolement social dû à la distance entre apprenants et entre apprenants et tuteurs, et d'autre part, d'appliquer les principes des théories constructivistes et socioconstructivistes qui voyaient dans l'interaction un élément pertinent favorisant l'apprentissage.

Ces environnements d'apprentissage en ligne s'attachent à l'analyse des situations d'interaction et de collaboration entre les apprenants en utilisant des outils technologiques. L'une des principales critiques qui a été adressée à ces domaines porte justement sur le fait qu'ils ont mis l'accent uniquement sur les activités de collaboration, autrement dit les caractéristiques des activités en ignorant les autres aspects de l'interaction énoncés par l'approche socioconstructiviste telle que la dimension sociale dans l'apprentissage (Seedhouse, 1999).

C'est ce dernier point qui nous semble au cœur même de la perspective dans laquelle nous abordons la question de l'interaction entre apprenants dans les situations d'apprentissage en ligne à une prise en compte des dimensions contextuelles de celles-ci, notamment sociales et affectives.

Avec le développement du web 2.0, le déploiement récent de l'apprentissage social oblige à re-questionner les travaux sur les interactions entre apprenants. Dans ce cadre, l'action d'interagir ne vise plus seulement la production collective d'une connaissance ou l'échange dans un contexte d'une activité collaborative d'apprentissage (Pélissier et Metz, 2010). L'interaction est devenue un moyen pour partager les expériences, solliciter le soutien et obtenir de l'assistance des pairs (Duthoit *et al.*, 2011).

L'apparition des environnements informels d'apprentissage en ligne (c.-à-d. les espaces et les contextes non institutionnels d'apprentissage) tels que les forums de discussion, les réseaux sociaux d'apprentissage et les communautés virtuelles oblige alors à revoir la conceptualisation de l'interaction comme une stratégie d'apprentissage à un moyen *d'auto-socio-construction* des connaissances par les apprenants tel que conçu par Vygotsky (1987).

2.1.2. Interaction dans les environnements d'apprentissage

L'apprentissage est vu comme l'acquisition des connaissances grâce aux échanges entre l'apprenant et son environnement et la transmission de ces connaissances par l'interaction. L'interaction est donc vue comme une occasion pour favoriser le débat entre les apprenants (conflit sociocognitif), et acquérir et transmettre les connaissances (Doise et Mugny, 1981).

La notion d'interaction dans l'apprentissage fait l'objet de récents travaux scientifiques. Ce regain d'intérêt est vraisemblablement à associer à un changement technologique et social. En effet, les nouvelles technologies de communication offrent de nombreuses possibilités dans les échanges et interactions en ouvrant de nouvelles perspectives pour l'apprentissage en ligne. Cela a permis le développement des environnements et plateformes d'apprentissage informels centrés sur la participation des apprenants et leurs interactions pour construire les connaissances.

Les **environnements formels**, mêmes ceux basés sur des approches constructivistes et socioconstructivistes, tendent à considérer l'interaction comme une stratégie d'apprentissage permettant aux étudiants d'apprendre en réalisant des activités collaboratives, ou des stratégies d'évaluation en intégrant des outils d'évaluation entre pairs (*peer assessement* en anglais) (Liu et Carless, 2006). Tandis que dans **les environnements informels**, l'interaction est un moyen pour accéder à l'aide des pairs (voir tuteur s'il y en a) et d'auto-socio-construction de la connaissance et de l'apprentissage.

Une analyse des interactions dans ces derniers environnements ne peut pas faire l'impasse sur l'étude de particularités et caractéristiques de ces environnements, surtout qu'ils ont eu peu d'attention dans la littérature en tant qu'environnements d'apprentissage.

Environnements d'apprentissage informel

Dans la littérature, on distingue souvent l'apprentissage **informel** et **non formel** (Duthoit, 2014). Le premier type d'apprentissage, dit aussi implicite, signifie l'apprentissage *non intentionnel* découlant des activités de la vie quotidienne, à l'inverse de l'apprentissage explicite qui désigne, selon Lanchantin *et al.* (2012), l'apprentissage dans l'intention d'acquérir ou de compléter de nouvelles connaissances. Un exemple de ce dernier type est l'inscription sur un site pour apprendre une langue par exemple.

Une étude plus détaillée et classification de différents types d'apprentissages existants aujourd'hui faite par Bingham et Conner (2015), a abouti à distinguer cinq types d'apprentissage basés sur les interactions. Ces types sont illustrés dans la figure 1.

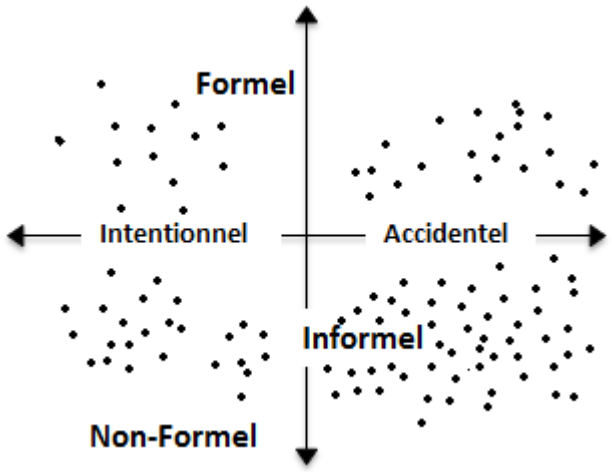


Figure 1 – Types d'apprentissage basés sur l'interaction

Si l'apprentissage a souvent lieu dans un cadre institutionnel et formel, on apprend aujourd'hui plus souvent d'une façon délibérée ou informelle. Les chercheurs en éducation, psychologie et sociologie sont d'ailleurs de plus en plus conscients de la source abondante et sous-étudiée que représente l'apprentissage non formel et informel. Les travaux récents s'intéressent à cet apprentissage, non seulement parce qu'y accéder devient de plus en plus facile mais aussi parce que l'apprentissage dans ces contextes implique une *déformalisation*,

construction et reconstruction des savoirs nécessaires pour les régulations individuelles et sociales (Volckrick et Deliège, 2001).

Dans ce même sens, étudier les environnements d'apprentissage informels, et plus particulièrement l'interaction dans ces derniers implique d'appréhender également ce qui entoure l'apprentissage, c'est-à-dire les différents éléments impliqués dans l'interaction, et l'apprentissage. Malgré l'absence des cadres théoriques acceptés par la majorité des chercheurs, certains travaux se sont intéressés à identifier les éléments influençant l'apprentissage dans ces environnements. Parmi ces travaux, Balsam et Tomie (2014) ont identifié principalement trois facteurs entourant l'apprentissage dans ces contextes informels : la *technologie*, *l'apprenant lui-même* et la *communauté*, tel que le montre la figure 2.

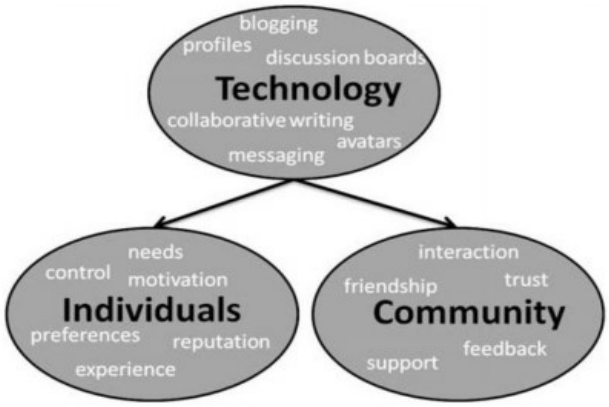


Figure 2 – Facteurs entourant l'apprentissage informel (Balsam et Tomie, 2014)

L'analyse de ces facteurs destinés à conceptualiser l'interaction dans ces contextes d'apprentissage implique d'interroger les cadres théoriques et méthodologiques supposant l'interaction comme une stratégie d'aide au sein d'une communauté.

Interaction et aide dans les environnements d'apprentissage informel

Selon Puustinen (2012), l'aide est vue comme le résultat d'une interaction ou un dialogue engageant un ou plusieurs acteurs aboutissant à une compréhension d'une connaissance ou un avancement du processus de réflexivité.

Le développement des technologies numériques a contribué à l'émergence de la notion d'aide dans les situations d'apprentissage (Duthoit, 2014). L'un des objectifs principaux de l'aide est, en effet, de soutenir l'apprenant et lui permettre plus d'autonomie dans sa démarche d'apprentissage. Dans cette perspective, notons alors l'émergence des réseaux, sites et forums

ouverts d'entraide pour les apprenants (Duthoit *et al.*, 2011). L'objectif de ces espaces informels est de proposer un environnement d'interaction et d'entraide, constitué d'un échange d'expériences, un soutien et surtout de demande d'aide entre pairs. Pour n'en citer qu'un, on a pu constater l'apparition des environnements s'intéressant à un domaine précis d'apprentissage et proposant des services destinés à faciliter le développement des compétences en langues, par exemple : Babel, Livemocha, etc. (voir figure 3).

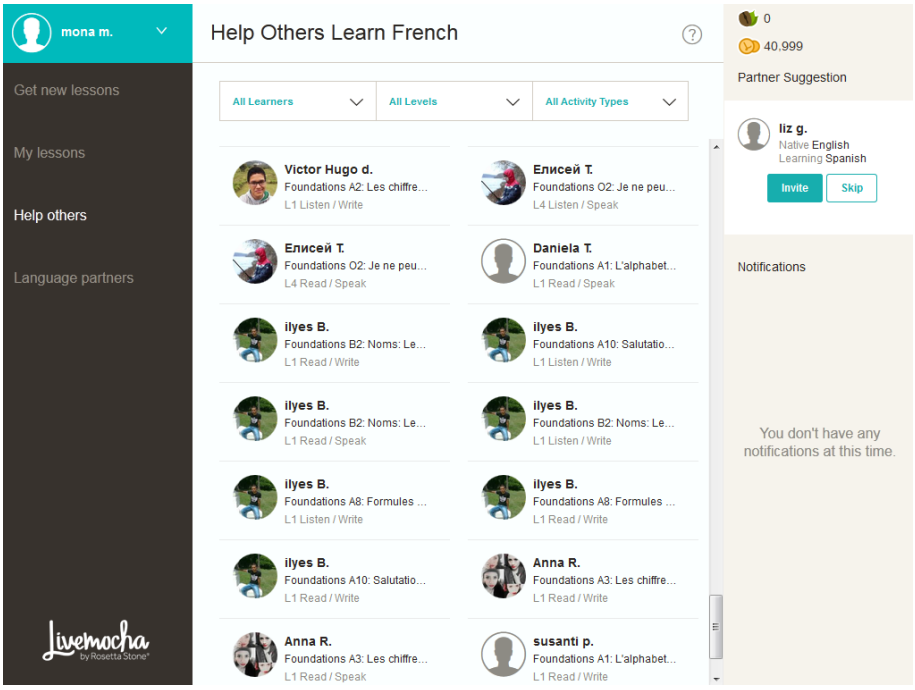


Figure 3 – Exemple d'activité d'aide entre apprenants sur Livemocha

Par ailleurs, la focalisation sur l'aide dans les situations d'apprentissage a fait l'objet de plusieurs travaux dans les sciences de l'éducation et de la psychologie (Karabenick et Newman, 2009). Ces travaux ont étudié les questions de la recherche d'aide (*help seeking*) ainsi que la demande d'aide (*help request*) d'un point de vue sociocognitif en analysant leurs influences principalement sur l'*autonomie*, *l'auto-efficacité* et *l'auto-régulation*. Ils ont, dans un premier temps, considéré la recherche d'aide comme la manifestation d'une faiblesse ou d'une dépendance, dans le sens où la demande ou la recherche aurait un coût cognitif (Suizzo, 2000).

Par la suite, ces recherches ont défini l'aide non plus comme un coût cognitif mais comme un mécanisme qui favorise l'apprentissage et l'acquisition de connaissances (Foucher et Pothier, 2007). Cette dernière position fait appel aux travaux de Zimmerman (1990) et les stratégies

d'auto-régulation dans les situations d'apprentissage (*self-regulated learning strategies*). Elle fait aussi appel à la théorie de l'auto-régulation de Piaget (Suizzo, 2000) montrant que la demande d'aide est également interdépendante du sentiment d'auto-efficacité. Ce sentiment est défini, selon Bandura (1986), comme le jugement de ses propres capacités à atteindre un certain objectif.

Dans ce cadre, Van der Meij (1990) propose deux phases au processus de recherche d'aide : la première est de se poser des questions et la seconde est de les poser aux autres. Tandis que, Karabenick et Newman (2009) distinguent plusieurs étapes dans un processus de recherche d'aide. Ces étapes comprennent (1) la détection d'un problème, (2) la détermination de la nécessité de l'aide, (3) la décision de demander de l'aide, (4) le choix du type approprié de l'aide, (5) l'identification d'une personne potentielle pour fournir l'aide, (6) la sollicitation de l'aide, (7) l'obtention de l'aide, et finalement (8) le traitement de l'aide reçue.

Les quatre dernières étapes - de l'identification au traitement de l'aide reçue - sont consistantes avec notre étude de l'interaction pour accéder à l'aide dans les environnements informels d'apprentissage. Nous étudierons principalement dans les prochaines sections ces quatre étapes. Parce que les comportements de recherche d'aide et les perceptions des apprenants sont étroitement liés, ils ont été généralement étudiés ensemble dans les environnements d'apprentissage.

Perceptions et comportements de recherche d'aide

Les perceptions ou les attitudes envers la recherche d'aide font référence aux risques perçus (ou coûts) et avantages de la recherche d'aide dans un contexte d'apprentissage (Ryan et Pintrich, 1997). Selon les auteurs, les perceptions et les attentes sont des facteurs cognitifs importants influençant les intentions de comportement des apprenants ainsi que leurs comportements réels. Plusieurs études dans des contextes d'apprentissage traditionnels ont montré que les perceptions que les apprenants avaient des avantages et des coûts ont influencé leurs comportements de recherche d'aide (Troncy *et al.*, 2011).

La perception des avantages de la recherche d'aide reflète la reconnaissance auprès des apprenants selon laquelle la demande d'aide est une stratégie utile qui favorise l'apprentissage (Ryan et Pintrich, 1997). Dans ce sens, des études antérieures ont montré que plus les apprenants déclarent percevoir les avantages de la recherche d'aide, plus ils y ont recours durant l'apprentissage (Troncy *et al.*, 2011).

En contrepartie, d'autres études ont identifié principalement deux inconvénients perçus de recherche d'aide dans les environnements d'apprentissage traditionnels : la diminution de l'estime de soi et la diminution de l'autonomie (Butler, 2007). Pour les apprenants, la recherche d'aide implique une diminution de l'estime de soi parce qu'ils la perçoivent comme un signe d'incompétence à résoudre un problème sans l'aide des autres (Skaalvik et Skaalvik, 2005). Ce type d'apprenants ne recherche généralement pas d'aide soit pour appuyer leurs impressions de compétence ou pour éviter les jugements négatifs des autres.

Des travaux dans des environnements d'apprentissage en ligne ont confirmé ces résultats en précisant que plus la perception de la diminution de l'estime de soi est grande, plus les apprenants évitent de demander de l'aide auprès de leurs co-apprenants (Troncy *et al.,* 2011).

La recherche d'aide peut également être évitée dans un contexte d'apprentissage pour une autre raison : les apprenants peuvent considérer la demande d'aide comme un comportement de dépendance envers les autres. Ils évitent alors de demander de l'aide pour préserver leur sentiment d'autonomie en réalisant les tâches par leurs propres moyens et sans l'aide des autres.

La recherche du « *feedback* » peut également être considérée comme une sorte de recherche d'aide quand les apprenants ont la possibilité de demander du feedback pour les aider à compléter une tâche d'apprentissage ou acquérir un savoir (Narciss et Huth, 2006). Selon les auteurs, les apprenants ont tendance à considérer le feedback comme un moyen utile pour développer la compréhension et la maîtrise des connaissances. En revanche, dans certains contextes d'apprentissage social ou collaboratif, les apprenants considèrent la demande de feedback comme un moyen pour révéler leurs incompétences et les exposer aux jugements de leurs pairs (Develotte, 2008).

Analyser les situations d'aide, et plus généralement l'interaction, dans ces contextes requiert de questionner les cadres théoriques et méthodologiques pour cerner les objets d'analyse.

2.1.3. Analyse des interactions

Selon la théorie socioconstructiviste, la connaissance est co-construite par l'interaction des participants dans un contexte social. La construction collaborative des connaissances résulte des échanges d'expériences et de partage des opinions entre les apprenants impliqués dans l'interaction. Une étude des différentes phases du processus de construction collaborative des connaissances, menée par De Wever *et al.* (2010), a révélé que les questions, les réponses, les

explications, les interprétations et les conflits sont des éléments de l'interaction qui facilitent la construction de la connaissance.

Dans une étude récente, Lin *et al.* (2013) ont examiné différentes taxonomies pour analyser et représenter les discussions entre apprenants dans un contexte informel d'apprentissage, et plus particulièrement dans une application sur Facebook, en termes de connaissances et processus cognitifs. Leur étude a révélé l'existence de différentes dimensions influençant la construction des connaissances dans ces contextes. Cette hypothèse a aussi été appuyée par une étude de Kasdali (2014) qui a démontré la marginalité des dimensions métacognitives, instrumentales et disciplinaires dans un contexte d'interaction entre apprenants dans les forums de discussion, bien que la littérature ait été prolifique sur ces dimensions. En contrepartie, les auteurs ont pu constater la prédominance de la dimension sociale et affective dans les contextes informels d'apprentissage. Lin *et al.* (2013) ont alors suggéré de considérer la contribution de différentes dimensions dans l'analyse des interactions. Un des modèles qui considère une combinaison des dimensions est le modèle de *Community of Inquiry* (ou COI). Proposée par Garrison *et al.* (1999), ce modèle s'appuie sur le principe selon lequel les interactions sociales entre apprenants créent une certaine forme de présence lorsque ces derniers sont engagés dans un processus de collaboration ou d'entraide à distance.

Bien que ce modèle ait été utilisé dans plusieurs travaux pour analyser les interactions dans des contextes d'apprentissage en ligne, une étude de Jézégou (2010), a montré qu'il ne mobilise pas suffisamment les théories de socioconstructivisme auxquelles il se réfère. Face à ce constat, l'auteure a tenté de consolider le modèle de COI en en proposant un nouveau basé sur trois dimensions tel qu'illustré dans la figure 4.

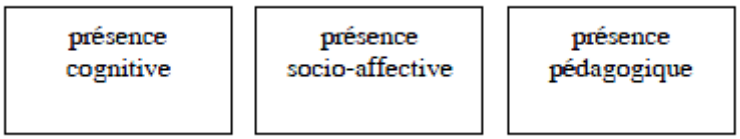


Figure 4 – Les trois dimensions de la présence (Jézégou, 2010)

La première dimension fait écho à la présence cognitive du modèle *community of inquiry* en s'appuyant sur la pratique d'enquête (ou practical inquiry) de Dewey (1938). La deuxième dimension, dite *présence socio-affective* est basée sur la théorie du conflit sociocognitif. Elle

inclut les aspects qui permettent de soutenir les interactions à distance entre apprenants lorsque ces derniers sont engagés dans une pratique d'enquête.

La troisième dimension, qualifiée de *présence pédagogique*, est basée aussi sur la théorie du conflit socio-affectif et les théories d'apprentissage à distance pour définir le rôle du tuteur ou l'instructeur dans les interactions sociales entre les apprenants.

D'une manière générale, l'interaction dans un contexte formel d'apprentissage diffère de celle dans un contexte informel par plusieurs éléments. Ce dernier contexte se caractérise par l'égalité des statuts des membres impliqués dans les interactions sociales, ainsi que par le fait qu'ils mènent conjointement des activités définies ensemble pour résoudre un problème partagé (Remesal et Colomina, 2013). De plus, les membres de la communauté s'y engagent activement et ont accès à des ressources partagées tout en assurant la réciprocité des informations, des soutiens et des services. Dans ce même contexte, l'engagement de l'individu dans les interactions sociales avec les autres membres, sa participation et sa contribution dans ces interactions témoignent indirectement de l'apprentissage réalisé. Ceci étant dit, c'est la présence sociale selon le modèle de COI ou la présence sociocognitive qui est plus présente dans les contextes informels d'apprentissage.

Nous nous focalisons donc dans la présente recherche sur la dimension de présence sociale ou socio-affective dans l'analyse des interactions entre apprenants.

2.1.4. Présence sociale, socio-affective et apprentissage informel

La théorie du pragmatisme souligne l'importance du climat socio-affectif dans lequel se déroulent les transactions lors de la pratique d'enquête. Elle insiste plus spécifiquement sur les aspects permettant de soutenir les interactions à distance entre les apprenants tels que le respect mutuel nécessaire à la confrontation des divers points de vue, à la négociation et à la régulation pour concevoir et mettre en œuvre des solutions pour résoudre des problèmes d'apprentissage (Shea et Bidjerano, 2009). Ces éléments constituent la dimension de la présence sociale et socio-affective telle que définie par Jézégou (2010).

Présence sociale et socio-affective

La présence dans les environnements virtuels fait référence aux interactions entre les apprenants lorsque que ces derniers, bien qu'éloignés géographiquement, se regroupent, spontanément ou pas, pour résoudre une situation problématique en collaborant ensemble à distance par des outils de communication synchrones ou asynchrones (Jézégou, 2010).

Se focalisant sur les aspects socio-affectifs des interactions, Dejean-Thircuir (2010) propose de cerner l'analyse des interactions en deux indicateurs principaux : le *dévoilement de soi* et la *gestion de conflits*.

Le dévoilement de soi, selon l'auteur, passe souvent en premier lieu par le dévoilement de son univers incluant certains traits de son caractère ou encore de ses émotions. Par exemple, le simple partage de ses émotions afin de justifier une confusion liée à une connaissance bien déterminée peut susciter une certaine empathie chez les membres de la communauté et contribuer ainsi à l'intensité socio-affective entre les membres manifestée dans leurs échanges.

Grosjean (2008), quant à elle, estime que la révélation d'aspects multiples de soi-même conduit les individus à construire une identité sociale et à se démarquer des autres en présentant leurs caractéristiques individuelles. Cette présentation de soi permet aux apprenants impliqués dans une situation d'apprentissage informel d'établir des connexions et échanger des expériences personnelles nécessaires pour leur apprentissage.

Au regard de l'ensemble de ces éléments, la présence socio-affective et sociale s'avère un élément fondamental pour le bon déroulement d'interactions entre apprenants, plus particulièrement dans un contexte informel d'apprentissage où le formateur ou l'instructeur est généralement absent.

Une étude de Mangenot et Nissen (2013) approfondit cette idée de l'importance de la dimension socio-affective dans l'apprentissage. Les résultats ont montré très clairement, de manière statistiquement significative, que les apprenants ayant bénéficié des feedbacks affectifs lors de leurs interactions avec les pairs (par feedback affectif nous désignons ici les interventions destinées à créer un climat relationnel propice à l'apprentissage, à favoriser l'entraide entre apprenants et à les soutenir) ont plus progressé que les autres dans leur apprentissage.

Enfin, l'intérêt que suscite le concept de présence socio-affective dans les contextes d'apprentissage informel est non seulement lié au soutien qu'offre cette dimension à la présence cognitive qui résulte des transactions en jeu entre les apprenants pour résoudre une situation problématique, mais également à l'engagement et la motivation socialement ancrés qu'ont les apprenants pour interagir ensemble autour de leurs objectifs communs.

Néanmoins, si le climat lié à la présence socio-affective est une condition propice à la construction de la connaissance, il n'est pas évident pour les apprenants, sans s'être rencontrés

physiquement, de créer à distance des relations symétriques et stables basées sur une empathie et une amabilité ressentie par chacun (Balsam et Tomie, 2014).

Cette situation est d'autant plus délicate que, dans les environnements d'apprentissage informel, les outils de communication intégrés aux plateformes permettent rarement de mettre en jeu le facteur émotionnel; ce dernier étant alors peu perceptible par des interlocuteurs distants. Or, il constitue un puissant vecteur d'affectivité dans l'interaction humaine. Ainsi, il convient de soutenir la présence socio-affective avec la dimension émotionnelle.

Émotions

De nombreux travaux nous amènent à constater que les émotions influencent fortement tout processus mental, notamment l'apprentissage. Pekrun et Linnenbrink-Garcia (2012) ont prouvé que, durant une séance d'apprentissage, un apprenant peut éprouver différentes émotions négatives ainsi que positives tels que l'ennui, l'anxiété, l'espoir, la joie, etc., ayant un grand impact sur ses performances. En revanche, des émotions positives peuvent, selon Isen (2001), faciliter la mémorisation et le raisonnement et favoriser le succès de l'apprentissage. D'autre part, Cleveland-Innes et Campbell (2012) ont démontré, lors d'une session d'apprentissage en ligne, que le rendement d'un apprenant est fortement influencé par certains états affectifs tels que la confusion, l'ennui, la frustration, etc.

O'Regan (2003), pour sa part, a étudié les émotions, négatives et positives des étudiants en ligne : la frustration à cause de la technologie ou le contenu mal structuré, l'anxiété face au temps à gérer, face à des consignes de travail peu claires, face au regard des pairs inconnus ou face aux feedback des autres. L'auteur a également étudié l'embarras ou la honte liés au caractère public et permanent des échanges publiés, l'enthousiasme dû à la nouveauté du mode d'apprentissage, la fierté ou la joie résultante de la réussite d'une tâche ou de la réception d'un feedback positif de l'enseignant et des pairs. L'auteur livre en conclusion de ses travaux un certain nombre de conseils pratiques destinés à éviter les émotions négatives, en affirmant que la question des émotions ne doit pas être écartée de la recherche sur l'apprentissage en ligne.

Lipman (2003) a évoqué la question des émotions dans les communautés d'apprentissage et a affirmé que la considération du facteur émotionnel dans un contexte social et collectif améliore le raisonnement et renforce la présence sociale. Cette présence a été définie dans le modèle de COI (Garrison *et al.*, 1999), présenté ci-haut, comme la mesure dans laquelle les

apprenants se sentent socialement et émotionnellement engagés dans la communauté et connectés aux autres membres. Ceux qui sont engagés dans l'apprentissage en ligne ou en communauté expérimentent les effets de l'émotion sur une base quotidienne, que ce soit en relation à l'apprentissage en ligne ou à leur rôle dans la communauté.

Les travaux sur l'apprentissage en ligne, et l'éducation en général, suggèrent que l'émotion est ni un objectif, ni un résultat de l'apprentissage. Elle est au cœur de la cognition et doit être considérée comme un élément nécessaire, au bon fonctionnement de la communauté, l'adaptation de l'apprenant à son rôle dans la communauté et son autorégulation (Artino *et al.*, 2010).

Enfin, selon Artino *et al.* (2010), sept des quinze indicateurs socio-affectifs identifiés lors des analyses des traces d'apprentissage en ligne sont des expressions émotionnelles. Ceci dit, l'étude de l'émotion comme un aspect fondamental de la présence sociale est nécessaire pour l'analyse des interactions sociales entre apprenants, et plus particulièrement dans un contexte informel d'apprentissage où la dimension affective a un grand impact sur l'expérience d'apprentissage.

2.1.5. Synthèse

Des environnements formels aux contextes d'apprentissage informels d'aujourd'hui, en passant par les communautés, le dénominateur commun est la pratique sociale du partage et de la construction de connaissances qui se développe avec l'évolution des technologies. Bien que l'espace d'interaction et d'entraide s'étende désormais à l'échelle globale, l'apprentissage qui s'y réalise demeure social, toujours *en tension* avec la dimension personnelle et collective et grandement affecté par la dimension socio-affective d'un côté et l'évolution continue des pratiques et de comportements en ligne de l'autre côté.

Cette **première partie du chapitre** a fait l'état de l'ensemble des cadres théoriques et méthodologiques qui nous semblent nécessaires pour appréhender l'aide dans des contextes d'apprentissage informels. Dans ces contextes, l'aide est interdépendante de l'espace d'interactions. De cet espace, émergent des situations d'entraide résultant des interactions entre apprenants faisant partie d'une communauté d'apprentissage et ayant un objectif commun. L'aide, en tant que processus cognitif, est liée au développement de compétences pour celui qui la reçoit mais elle est grandement affectée par des facteurs sociaux et psychologiques dont la perception des risques et des avantages. Il s'agit alors de mobiliser les

travaux qui portent sur cette vision de l'aide, ou l'interaction en général, en tant que compromis entre *avantages attendus* et *risques potentiels*.

2.2. Vie privée

La vie privée comme valeur essentielle à l'être humain s'est élaborée progressivement. Aujourd'hui encore, c'est bien souvent lorsqu'il y a un problème que cette préoccupation émerge. C'est d'une part la fragilité de la vie privée qui est remise en question et son insuffisante protection face à un nombre continuellement croissant de menaces. Mais c'est la pertinence de la définition de la vie privée qui est également source de préoccupation au regard de pratiques qui ne cessent d'évoluer, tant du point de vue des utilisateurs que du point de vue des technologies et institutions.

Dans cette deuxième partie de ce chapitre, nous nous intéresserons à cette notion de vie privée et nous mettrons l'accent sur les risques que posent les différentes activités d'apprentissage en ligne sur la vie privée des apprenants, et plus particulièrement l'interaction.

2.2.1. Définitions et propriétés

Le droit à la vie privée est un principe significativement ancien, il désigne le droit d'un individu d'avoir une protection complète de soi et de ses biens (Warren et Brandeis, 1890). Cependant, il est parfois nécessaire de le redéfinir afin qu'il soit conforme aux nouvelles menaces et exigences.

Nous discutons dans cette section les propriétés et les exigences de la protection de la vie privée, en passant par les différentes définitions de cette notion dans la littérature.

Définitions

La notion de vie privée semble être floue et par conséquent difficile à cerner (Solove, 2007). En effet, elle est considérée comme une traduction du terme *privacy* en anglais qui désigne *right of privacy* ou *privacy* dans le sens de protection. Intuitivement, ce concept éveille chez chacun de nous le droit à cacher un certain nombre de choses sur soi et donc relève nécessairement de notre droit à la protection de la vie privée.

Dans la littérature, certains auteurs ont proposé des définitions très laconiques dont on peut se demander si elles correspondent vraiment à cette vision intuitive de la vie privée.

Westin (1968) a défini le terme *privacy*, en adoptant un point de vue juridique, comme le droit d'un individu de contrôler quand, comment et pour quelle finalité une donnée à propos de lui-même est collectée. Selon cette définition la vie privée n'est donc qu'une question de gestion des informations se rapportant à une personne. De même, Muller (2006) définit la vie privée comme la possibilité de contrôler la collecte et la divulgation des données personnelles.

La définition qui semble être donc la plus adoptée de la vie privée est le droit d'une personne de contrôler l'accès aux renseignements qui la concernent et son droit de conserver son anonymat. Cela signifie que la personne décide des renseignements qui sont divulgués, à qui et à quelles fins. Partant de ce constat, certains auteurs posent des définitions plus générales. Ainsi, Basse (2003) propose une définition selon laquelle la vie privée peut signifier globalement : l'absence d'intrusion, le contrôle des informations nous concernant et l'absence de surveillance. En effet, la plupart des chercheurs considèrent que la vie privée est une ressource précieuse qui, si elle est perdue par des manœuvres intentionnelles ou par inadvertance, peut être rarement récupérée. C'est pourquoi il est essentiel de la protéger. Par conséquent, toutes les actions faisant intrusion dans l'intimité de la personne sont considérées comme portant atteinte à la vie privée, notamment la surveillance de ses activités, l'enregistrement ou le traitement d'informations le concernant, sa vie sentimentale, l'état de sa santé, etc.

Crépin *et al.* (2009) formalisent une définition bien plus générale et utilisent plutôt le terme de sphère privée pour désigner l'ensemble des informations, se rapportant à un individu, qu'il considère comme sensibles et donc dignes d'être protégées. Selon les auteurs, cette sphère encapsule toutes les informations qui concernent un individu et qu'il souhaite protéger. Par conséquent, elle doit être :

- personnelle : la personne est la seule propriétaire des informations qu'elle contient
- personnalisable : la personne décide des informations qu'elle contient
- dynamique : les informations peuvent être mises à jour
- dépendante du contexte : les informations qu'elle contient dépendent du temps, des activités de l'individu ou d'autres paramètres.

De ce fait, le droit à la vie privée d'un individu inclut le contrôle de la collecte, de l'utilisation et de la conservation de ses données personnelles, quelle que soit la représentation de ces données (Crépin *et al.*, 2009). Dans un contexte contemporain, ce droit a été intégré dans la plupart des textes légaux internationaux au cours des dernières décennies, et remis à jour au

fil de l'évolution des technologies et des menaces en proposant un ensemble des mesures techniques et un ensemble des propriétés à satisfaire pour assurer la protection de la vie privée de l'utilisateur et ses données personnelles représentées sous forme numérique et mises en jeu dans le cadre d'une application informatique.

Propriétés et critères communs

Les critères communs (*Common Criteria for Information Technology Security Evaluation)*[1] est un standard international pour la sécurité des systèmes informatiques. Ils définissent des classes de fonctionnalité pour satisfaire les différents besoins de sécurité de ces systèmes.

Pour la protection de la vie privée, une classe de fonctionnalité dite la classe *privacy* est consacrée. Cette classe décrit quatre propriétés principales qui sont :

- Anonymat (*anonymity*) : requiert que d'autres utilisateurs soient incapables de déterminer l'identité d'un utilisateur associée à une action
- Pseudonymie (*pseudonymity*) : impose qu'un ensemble d'utilisateurs soit incapable de déterminer l'identité d'un utilisateur associée à une action, mais que cet utilisateur soit tenu pour responsable de ses actions
- Non-chainabilité (*unlinkability*): exige que des utilisateurs soient incapables de déterminer si le même utilisateur a déclenché certaines actions dans le système
- Non-observabilité (*unobservability*) : consiste à ce que des utilisateurs ne puissent pas savoir si une action est en cours d'exécution.

Ces propriétés définissent ce que les autres peuvent collecter comme informations au sujet d'une communication et visent à protéger les données personnelles et la vie privée des utilisateurs en ligne. Toutefois, même si elles sont théoriquement nécessaires et suffisantes pour garantir la protection dans certains contextes, elles ne peuvent certes pas protéger contre toutes les menaces posées à la vie privée en ligne surtout que ces dernières sont de plus en plus croissantes.

2.2.2. Menaces en ligne

Les auditions ont permis de mesurer à quel point les facilités apportées par les nouvelles technologies pouvait entraîner les individus, par ignorance ou par indifférence, à mettre de

[1] www.commoncriteriaportal.org

côté la protection de leur vie privée (Smith *et al.*, 2011). Pour analyser ces menaces, il convient de distinguer les différentes étapes du cycle de vie des données personnelles mises en jeu dans des applications en ligne qui sont la collecte, l'utilisation et l'effacement (Le Métayer et Piolle, 2010).

Collecte des données personnelles

Avant de traiter les données personnelles, il faut les obtenir. Les risques à cette étape sont déjà nombreux : Le premier risque est la collecte d'informations à l'insu de la personne concernée, ou sans qu'elle en prenne vraiment conscience (exemple des caméras de surveillance) (Solove, 2007)**.** D'autre part, il arrive également que la collecte soit clairement annoncée, mais disproportionnée par rapport à l'objectif du traitement de la donnée (Deswarte et Gambs, 2010).

Le deuxième risque est l'utilisation secondaire par des tiers ou par les collecteurs de données eux-mêmes. En effet, pour avoir ces données, deux moyens sont possibles : d'une part, la divulgation délibérée contre rémunération des données personnelles par le collecteur et d'autre part, l'exploitation de failles de sécurité et de l'indifférence de la part du collecteur de données (Bélanger et Crossler, 2011).

Le troisième risque est lié aux progrès effectués en matière d'inférences de données et de techniques de *ré-identification* (Aïmeur *et al.*, 2013). De nombreuses études et expériences réelles ont montré comment des données apparemment anonymes pouvaient être analysées ou regroupées avec d'autres données disponibles pour retrouver les personnes concernées (Aïmeur *et al.*, 2013; Ohm, 2010; Sweeney, 2002) ce qui contredit le principe de la *non-chainabilité*.

Utilisation des données personnelles

Une fois collectées, les données doivent être utilisées suivant les finalités déclarées lors de la collecte. Cependant, il arrive d'utiliser les données à des fins non prévues, par exemple pour des besoins de marketing ou pour cibler des offres publicitaires (Solove, 2007). Ce risque est d'autant plus significatif que la personne ne dispose plus, après la collecte, d'aucun contrôle sur ses données ni moyen d'y accéder.

On retrouve ici aussi l'exploitation des failles de sécurité évoquées plus haut, surtout qu'on sait malheureusement que les mesures minimales de sécurité ne sont pas toujours mises en œuvre pour protéger les données lors de la collecte ou lors du traitement, ce qui permet à des

personnes non autorisées d'accéder à des données parfois très sensibles (comme informations médicales, bancaires, etc.) (Bélanger et Crossler, 2011).

D'un autre côté, les conséquences peuvent être graves en cas d'usurpation d'identité, c'est-à-dire qu'une personne Alice passe pour une autre personne Bob pour accéder à des données pour lesquelles seul Bob a les droits (données bancaires par exemple), ou pour réaliser une action malveillante dont Bob sera tenu responsable (Aïmeur *et al.*, 2013) .

Effacement des données personnelles

Cette étape est aussi une source de risques dans le sens où les données peuvent être conservées au-delà du temps nécessaire surtout que les ressources en mémoire augmentent de manière exponentielle, ce qui rend souvent plus facile de conserver les données que les effacer (Le Métayer et Piolle, 2010). Par ailleurs, certains systèmes ont également intérêt à conserver ces données le plus longtemps possible afin d'en tirer un maximum de bénéfice, c'est ainsi que les sites de commerce électronique conservent les données et l'historique de recherche de leurs clients pour comprendre leurs habitudes et leur proposer des produits susceptibles d'attirer leur attention (Turban *et al.*, 2015). Cela contredit, d'une part, un principe si intensément défendu aujourd'hui celui de droit à l'oubli et, d'autre part, aggrave les autres risques cités plus haut car plus longtemps une donnée est conservée, plus les risques s'accentuent (Smith *et al.*, 2011).

Ces menaces sont peut-être invisibles, mais leurs effets sont tout à fait tangibles particulièrement avec l'avènement du web 2.0 et les systèmes interconnectés, accessibles à l'échelle planétaire, rendant les individus plus vulnérables.

2.2.3. Nouvelles pratiques, nouvelles menaces

L'évolution technologique modifie la conception de la vie privée et les pratiques des internautes. Les nouvelles pratiques, dites de « socialisation numérique », illustrent le fait qu'il n'y a pas d'existence d'un sujet sans la relation à l'autre. L'une des fonctions principales de ces pratiques consiste à rechercher de l'interaction et de l'inter-reconnaissance : solliciter l'aide des autres et recevoir des feedbacks, se dévoiler, partager pour susciter en retour des commentaires, socialiser, référencer des blogs pour être référencé dans un réseau, etc. Dans les espaces relationnels tels que les réseaux sociaux et les communautés virtuelles, l'interaction et les réactions des autres semblent dès lors capitales pour mener à bien le processus de construction identitaire et de visibilité sociale (Tisseron, 2011).

Dans ce nouveau contexte, la conception de la vie privée a été bouleversée par un nouveau phénomène : l'*auto-divulgation*. L'objectif de l'auto-divulgation est d'obtenir une validation de la part d'autrui, en sollicitant sa reconnaissance ou son empathie (Casilli, 2013). Elle consiste en l'extériorisation de sa vie privée à des fins de validation de l'image de soi en utilisant les outils et plateformes du web social. Tisseron (2011) définit l'auto-divulgation comme le processus par lequel des fragments du soi intime sont proposés au regard d'autrui.

Ce phénomène a suscité de nombreuses interrogations. Des psychologues, des sociologues, des économistes, des juristes, tout comme les défenseurs des droits et libertés individuels et collectifs, s'attachent à saisir les ressorts et à évaluer les effets de telles pratiques. Le principal enjeu aujourd'hui est alors l'identification de ce qui est privé, qui dépend étroitement des normes et des perceptions de la vie privée à une époque donnée et dans une société donnée et pour un individu donné (Casilli, 2013). Ceci étant dit, la contextualisation des données s'avèrent nécessaires à leur protection comme l'a indiqué (Nissenbaum, 2009).

Même si de nombreux chercheurs considèrent la vie privée comme une question de contrôle des données (Whitley, 2009), force est de constater que toute action ou transaction du monde contemporain conduit souvent à une perte de ce contrôle puisqu'elle requiert de fournir toujours davantage de données personnelles (Hough, 2013).
À cette nouvelle réalité, s'ajoute le fait qu'Internet représente un nouvel environnement en ligne pour les comportements risqués et non éthiques (Latzko-Toth et Pastinelli, 2014), notamment en ce qui concerne le dévoilement de soi, la collecte des données, leur utilisation pour usurper l'identité d'un individu, le harceler ou l'intimider (Proulx, 2012).

Ceci devient d'autant plus fréquent avec l'émergence des plateformes d'interactions sociales en ligne qui mettent en contact des personnes qui ne se sont pas préalablement rencontrées en direct et peuvent rester plus ou moins durablement séparées physiquement les unes des autres, voire mutuellement inconnues bien qu'il arrive, pour ces derniers, d'interagir et de communiquer pour s'entraider ou collaborer sur une tâche.

Ces nouveaux comportements en ligne ont généré avec eux de nouveaux risques susceptibles d'engendrer de nouvelles conséquences quant à la vie privée. Il est ici principalement question des risques encourus par les individus lorsqu'ils divulguent des informations personnelles et que celles-ci sont exploitées par des inconnus. Les risques auxquels les individus s'exposent dans ce cas sont extrêmement variés. Contrairement aux informations qui peuvent être collectées à l'insu des internautes ou sans leur autorisation, les informations

divulguées et dévoilées volontairement lors des interactions sont d'autant plus difficiles à contrôler et à retracer.

Sans en faire une liste exhaustive, les risques sont de plus en plus élevés : certains relèvent de l'atteinte à la vie privée et du droit à l'image, alors que d'autres relèvent de la diffamation et de l'atteinte à la réputation, comme résumé par (Aïmeur *et al.*, 2013); Vallet (2012). Il s'agit, par exemple, de l'utilisation secondaire d'informations, de propos diffamatoires, porter préjudice à une personne ou de la divulgation d'informations sensibles. Il peut également être question de discriminations en raison de l'orientation sexuelle, de la race, de la religion, de la couleur et de l'origine ethnique (Vallet, 2012). Ces comportements destructeurs en ligne peuvent entraîner un éventail d'effets négatifs, tels qu'une faible estime de soi, l'anxiété, la colère, la dépression, l'absentéisme scolaire, la baisse de la performance scolaire et professionnelle, une tendance accrue à agresser d'autres personnes et le suicide des jeunes (von Marées et Petermann, 2012).

Bien que ces menaces à la vie privée et leurs conséquences fassent la réalité du web social d'aujourd'hui, elles ne sont pas nécessairement toutes présentes dans le contexte des environnements d'apprentissage informel qui nous intéressent dans cette recherche. Ces environnements qui incluent désormais les technologies du web social peuvent être touchés par les risques évoqués ci-haut, mais ils soulèvent aussi d'autres risques liés au contexte d'apprentissage en ligne.

2.2.4. Problématiques de vie privée dans le contexte d'apprentissage en ligne

Plusieurs travaux antérieurs ont étudié la question de la protection de la vie privée dans les contextes d'apprentissage en soulignant les risques qui se posent dans ces contextes. Anwar et Greer (2011) se sont intéressés surtout aux environnements d'apprentissage formel en ligne et ont relevé deux activités principales posant des risques à la vie privée, notamment l'évaluation et la personnalisation. Toutefois, ces deux activités sont généralement présentes dans tout contexte d'apprentissage mais ne sont pas les seules sources de risques dans ce contexte. En effet, jusque-là, les problèmes associés à la protection des données personnelles ont été étudiés dans le cadre d'une relation où un groupe d'agents (les institutions publiques ou les entreprises) détenant des données personnelles à propos d'un individu à l'occasion d'une transaction commerciale ou administrative pouvaient causer un préjudice à cet individu (Hage et Aïmeur, 2009).

Avec l'intégration des outils du web relationnel ou social dans le contexte éducatif, de nouvelles pratiques sont à considérer quant à la protection de la vie privée. Désormais, les données sont surtout divulguées par les individus eux-mêmes dans le cadre de leurs interactions et échanges avec leurs co-apprenants ou pairs. Dans ce contexte, plusieurs défis sont à relever si on veut profiter des avantages de l'interaction sociale comme favorable à l'apprentissage en minimisant les risques à la vie privée. En se basant sur les constatations de Anwar et Greer (2011) nous préconisons la nécessité de la protection de la vie privée dans les activités d'apprentissage suivantes : l'évaluation, la personnalisation et l'interaction.

Nous discuterons dans ce qui suit des problématiques et conséquences que posent ces trois activités d'apprentissage sur la vie privée de l'apprenant à savoir la sensibilité des données mises en jeu, le pouvoir d'inférences des algorithmes utilisés en ce qui concerne la personnalisation ainsi que l'auto-divulgation résultante de l'interaction.

Sensibilité des données

Dans les contextes d'apprentissage en ligne formel ou informel, l'apprenant est amené à dévoiler des informations de diverses natures : des données servant à l'identifier (nom, âge, etc.), d'autres concernent ses préférences d'apprentissage par exemple mais aussi des informations en lien avec son comportement et sa navigation lors de son utilisation du système (comme ses mouvements, ses expressions faciales, etc.).

De plus, on constate qu'il y a deux problèmes au sujet de la collecte : d'abord, on ne s'entend pas sur les informations nécessaires (à fournir) pour atteindre l'objectif de l'utilisation du système qui est dans ce cas-là l'apprentissage (Deswarte et Gambs, 2010). Deuxièmement, il est difficile sur le plan technique de séparer les informations légitimes de celles qui relèvent de la sphère privée (Feidakis *et al.*, 2011). Par exemple une webcam peut servir à reconnaitre les expressions faciales de l'apprenant mais elle enregistre aussi tout autre mouvement de l'apprenant.

Données massives et analytique des données

Si le *Big Data* représente une opportunité formidable pour la personnalisation dans les environnements d'apprentissage en ligne, il faut évaluer les implications de celui-ci du point de vue vie privée. En effet, la collecte et l'usage des données liées à la navigation des internautes peuvent être souvent plus révélatrices que des données (Tene et Polonetsky, 2012). La puissance de traitement dont disposent les plateformes et les algorithmes utilisés

aujourd'hui dans le cadre d'apprentissage en ligne permettent d'interpréter les comportements des utilisateurs ainsi que leurs préférences au point de prédire certaines de leurs actions (Crawford et Schultz, 2014).

Bien que l'objectif initial de leur utilisation soit certes de rendre l'expérience d'apprentissage en ligne plus pertinente, plusieurs autres inférences peuvent être faites en utilisant les données collectées. En effet, la «*datafication »* (c'est-à-dire la mise en données) s'est récemment intensifiée à cause de la collecte continue et indistincte (Crawford et Schultz, 2014). Les informations sont enregistrées en permanence, par les pratiques de navigation, pour un usage futur possible inconnu à priori et c'est justement cela qui est contradictoire par rapport aux critères communs de la protection de la vie privée (Tene et Polonetsky, 2012).

Selon Cointot et Eychenne (2014), cette mise en données des utilisateurs, relèvent deux actions trop risquées du point de vue de la vie privée : la *prédiction* et le *profilage*. En effet, la possibilité de prédiction apportée par les données massives devient principalement statistique basée sur des corrélations statistiques imperceptibles entre des phénomènes ou des utilisateurs. Cela pourrait avoir des avantages du point de vue personnalisation, mais il génère plusieurs problèmes vu qu'il ne permet plus la compréhension des raisons et causes de tel ou tel phénomène. En outre, l'avènement des données massives permet aussi un profilage précis des utilisateurs en accentuant l'homogénéisation de leurs pratiques et leurs profils (Cointot et Eychenne, 2014). Il faut noter que ce profilage peut entraîner l'identification d'un utilisateur, même si aucune donnée personnellement identifiable n'a fait l'objet de collecte, ce qui pose un risque à sa vie privée. Une autre préoccupation en matière de vie privée est liée à l'exactitude de l'information recueillie et à la validité des conclusions fondées sur ces renseignements.

Les apprenants, par ignorance des inférences que ces algorithmes d'analyse des données (Data analytics) puissent faire, cèdent certaines de leurs données personnelles en échange d'un droit d'accès à des services, ce qui rend le droit à la vie privée d'autant plus fragile. Même si l'identification d'un utilisateur n'est pas plus importante pour le collecteur des données que l'appartenance de cet utilisateur à un groupe précis, le nombre des données qu'il manie peut mettre fin au droit à la vie privée.

Auto-divulgation et exposition de soi

Malgré les précautions que beaucoup semblent prendre dans leurs échanges et interactions sociales en ligne, le succès des réseaux sociaux et des communautés virtuelles rend bien compte de la tendance à l'auto-divulgation et l'exposition de soi. Comme le souligne Granjon (2009), ces sites stimulent à l'évidence le consentement à divulguer des informations personnelles. Le concept derrière le web relationnel ou participatif est basé d'ailleurs sur la contribution de l'utilisateur à créer tout le contenu. S'inscrire sur un site, adhérer à une communauté virtuelle, solliciter l'aide des autres sur un forum ou répondre à des commentaires exigent une divulgation de données. Les conditions sont alors réunies pour que la résistance à la divulgation de données personnelles se relâche progressivement.

L'ensemble des attitudes décrites dans l'étude de (Granjon, 2009) confirme l'intérêt heuristique du concept de paradoxe de la vie privée exprimé à travers le décalage entre les déclarations et les pratiques des utilisateurs. Ce paradoxe pourrait être défini comme la contradiction entre, d'une part, une méfiance et une inquiétude bien réelle face à des menaces également bien réelles en matière de protection de sa vie privée, et, d'autre part, le désir de créer des liens sociaux en livrant volontairement des informations sur soi susceptibles de porter atteinte à sa vie privée.

S'il ne faut bien entendu surestimer la dimension rationnelle des comportements individuels, l'attention portée à la protection de la vie privée ne pèse pas lourd dans la balance face aux avantages relationnels que le web social semble procurer aux utilisateurs. Particulièrement dans le contexte d'apprentissage informel dont les objectifs de l'apprenant sont de créer des connexions et d'accéder à l'aide des autres, la divulgation de données ne semble pas être un obstacle.

Bien que la *récompense* offerte - l'accès à l'aide des autres- ne vaut pas les dangers majeurs que comportent la surexposition, il demeure que, dans les faits, les utilisateurs cèdent bien souvent sur leurs exigences en matière de vie privée. Selon Rochelandet (2010), il est bien difficile d'être confiant dans la capacité des individus à prendre les décisions conformes à leurs intérêts en matière de vie privée. Une fois qu'ils ont mis en ligne ces informations, les utilisateurs sont confrontés à un risque de perte de contrôle sur l'utilisation de ces données : d'une part, ces informations peuvent être vues ou lues par un nombre indéfini de personnes; d'autre part, elles peuvent être réutilisées à leur insu par d'autres utilisateurs ou institutions.

D’un autre côté, cette divulgation de données soulève plusieurs préoccupations en matière de vie privée. En effet, l'anonymat couplé à la confrontation d’opinions donne lieu à de nombreux débordements, regroupés sous l'appellation de comportements antisociaux. Il existe, dans les échanges en ligne, une omniprésence visible des comportements violents (Tierney et Subramanian, 2014). Allant de la moquerie excessive au harcèlement moral, ces débordements menacent l’apprentissage et la construction de la connaissance collective en ligne en faisant potentiellement courir nombre des conséquences négatives. Que deviennent les problèmes de la vie privée et comment les réguler lorsque la divulgation de données personnelles est le produit d’interactions sociales sur des plateformes numériques dont les services reposent sur l’exploitation de ces données ?

Dans la section suivante, nous présentons de nombreux outils qui ont été proposés pour protéger la vie privée et les données personnelles. Ces technologies, dites technologies de protection des données personnelles ou «*Privacy-Enhancing Technologies»*, peuvent être classées en plusieurs catégories dont la gestion des identités et l’authentification, le contrôle d’accès et l’autorisation, les communications et accès anonymes, la gestion des données personnelles, etc. (Deswarte et Gambs, 2010).

2.2.5. Protection de la vie privée : lois et outils

Plusieurs violations et attaques ont suscité des préoccupations croissantes pour la protection de la vie privée (Tierney et Subramanian, 2014). Cela a mené les défenseurs des libertés à proposer des lois ainsi que des solutions techniques pour protéger la vie privée des utilisateurs et leurs données personnelles.

Nous discutons dans cette section les principales lois et réglementations et surtout les solutions techniques qui visent à protéger la vie privée des utilisateurs.

Lois et réglementations

La vie privée est protégée au niveau international par l'article 12 de la déclaration universelle des droits de l'homme de 1948 : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation » (Pfitzmann et Hansen, 2010).

Plusieurs autres organismes ont comme mission principale de protéger la vie privée et les données personnelles des utilisateurs tels que le Commissariat à la protection de la vie privée

du Canada[2] (CPVP) et la Commission nationale de l'informatique et des libertés[3] (CNIL) en France. Les deux organismes évoquent les lignes directrices à suivre pour la protection de la vie privée et identifient plusieurs principes et critères de protection dont principalement le consentement, la minimisation de la collecte des données et la détermination des fins, etc.

De son côté, Ann Cavoukian, la commissaire à l'information et à la protection de la vie privée de l'Ontario, a proposé le principe de la vie privée par défaut (*Privacy by design)* énonçant que résoudre efficacement les questions relatives à la vie privée et les données personnelles, requiert de traiter le problème dès la création des informations à caractère personnel (Cavoukian, 2011).

Ces règlements ont été proposés pour protéger la vie privée des utilisateurs de la collecte, l'utilisation et la conservation illégales par des institutions ou applications informatiques. Cependant, l'auto-divulgation n'a pas reçu une attention égale dans le système juridique en raison de la nouveauté de ce concept et pratique de dévoilement de soi. Bien que la majorité des lois précisent le fait que la personne ait elle-même révélé des données n'autorise pas la redivulgation de certains de ces données en faisant référence au droit à l'oubli (Pfitzmann et Hansen, 2010).

Nous ne saurions trop mettre l'accent sur le fait que les lois et règlementations n'offrent aucune protection de la vie privée et que la capacité accrue des systèmes d'aujourd'hui pour recueillir, traiter et conserver les informations au sujet d'un utilisateur a exacerbé les craintes concernant la collecte, l'utilisation et la conservation des renseignements personnels. Il est donc très important de mettre en œuvre des solutions techniques qui garantissent la protection de la vie privée.

Solutions de protection

La nécessité de mettre en œuvre des solutions efficaces quant à la protection de la vie privée des utilisateurs en ligne est primordiale. Dans ce sens, le standard P3P [4] du World Wide Web Consortium a été proposé pour vérifier que les exigences de respect de la vie privée de l'utilisateur sont compatibles avec la politique de sécurité et de préservation de la vie privée proclamée par le service utilisé. Il s'agit d'un outil de communication des sites web sur leurs politiques de protection des données personnelles. Un document P3P contient des

[2] www.priv.gc.ca/
[3] www.cnil.fr/
[4] www.w3.org/P3P/

informations comme l'identité de l'entité collectant les données, la nature des données collectées, la justification de la collecte de données, etc. Par conséquent, son seul objectif est de résoudre le problème de l'information de l'utilisateur, il n'impose aucune politique et il ne permet pas de vérifier si une politique déclarée par un site est véritablement appliquée (Aïmeur *et al.*, 2016).

Un utilisateur n'a alors aucun moyen de savoir si ces politiques respectent telle loi ou telle directive et si elle est effectivement respectée. Cela implique qu'un outil comme P3P n'assure pas réellement la protection des données personnelles.

D'un autre côté, dans un contexte d'apprentissage en ligne, Aïmeur et Hage (2010) ont proposé un système d'e-learning préservant la vie privée en se focalisant sur la protection lors de l'authentification. Dans leurs travaux, ils ont utilisé une accréditation anonyme (*anonymous credential*) pour prouver qu'un apprenant ait certains droits sans dévoiler explicitement son identité. De ce fait, l'apprenant ne sera pas obligé de révéler son identité à chaque fois qu'il accède au système. D'ailleurs, dans le domaine du e-learning, la majorité des travaux ont proposé des techniques et outils pour assurer surtout l'intégrité et la confidentialité des données comme étant les deux clés de la protection de la vie privée de l'apprenant (Isabwe et Reichert, 2013). Ils se sont, donc, plus concentrés sur la mise en œuvre des mécanismes de contrôle d'accès pour restreindre l'accès aux données de l'apprenant.

Bien que ces solutions puissent assurer la protection de la vie privée de l'apprenant dans certains contextes, elles ne permettent pas de garantir un principe important de la protection de la vie privée celui de l'anonymat (Deswarte et Gambs, 2010). Dans ce sens, plusieurs méthodes ont été proposées comme *k*-anonymat (Sweeney, 2002), qui garantit qu'un individu ne puisse pas être distingué des autres dans un groupe d'au moins *k* personnes. D'autres travaux, comme ceux de Fung *et al.* (2010) et Ganti *et al.* (2008) ont proposé des techniques d'assainissement (*sanitizing* en anglais), qui consistent à remplacer des données sensibles par d'autres qui soient génériques (généralisation), ou de perturber certaines valeurs par des variations aléatoires, ou encore d'échanger des valeurs d'attributs entre différentes personnes (perturbation).

Les outils et techniques proposés dans le contexte des données relationnelles ne garantissent qu'une protection partielle, et ce pour deux raisons : les informations dans les systèmes d'aujourd'hui sont collectées continuellement et changent durant la session d'apprentissage

(1), et ces informations ne peuvent pas être séparées de l'identité de la personne dans la plupart de cas (2).

Dans le contexte d'analyse des données, peu de travaux se sont intéressés à proposer des techniques de protection de la vie privée des utilisateurs surtout que les risques dans ce contexte sont beaucoup plus nombreux à cause de la collecte continue et l'utilisation des algorithmes de prédiction et de profilage. La collecte concerne plusieurs types des données dont l'état psychologique et émotionnel. Dans ce contexte, Cornelius *et al.* (2008) ont proposé *Anonysense* pour rendre anonymes les données provenant de différents utilisateurs en se basant sur des réseaux Mix (Deswarte et Gambs, 2010) pour empêcher l'analyse de trafic (non observabilité). *PoolView* proposée par Ganti et *al.* (2008) est une architecture basée sur un schéma de perturbation qui ajoute du bruit aux données collectées. D'autres travaux comme ceux d'Ahmadi *et al.* (2010) ont introduit des techniques de perturbation ou transformation sur les données originales pour protéger les identités des utilisateurs.

Cependant, ces techniques peuvent préserver l'identité de l'utilisateur mais ne peuvent pas protéger les données en relation avec son comportement et sa navigation qui font l'objet de la collecte aussi. De plus, ils n'assurent pas le contrôle sur la divulgation de ces données. Ce principe est par contre, en quelque sorte présent dans le contexte des réseaux sociaux (Hélou *et al.*, 2012). Les concepteurs des réseaux sociaux en ligne ont pris conscience de ces risques et ont mis en place un système de contrôle des paramètres de confidentialité. Le but de ces outils de paramétrage est d'offrir aux utilisateurs les moyens de disposer d'un contrôle perçu, même s'ils encourageaient la divulgation, sur les données personnelles qu'ils mettent en ligne, en leur permettant de définir avec précision quelles seront les informations accessibles et par qui. En s'inspirant de ces travaux, plusieurs architectures offrent aux utilisateurs le contrôle sur leurs données personnelles telles que *virtual individual servers* proposée par (Cáceres *et al.*, 2009), *PrPl* proposée par Seong *et al.* (2010) qui est une architecture décentralisée avec un stockage des données personnelles (*Personal Cloud Butler*).

En ce qui concerne la divulgation des données par les utilisateurs eux-mêmes, certains travaux se sont surtout concentrés sur la quantification de la divulgation principalement sur les réseaux sociaux tels que les recherches de Liu et Terzi (2010) qui ont proposé une approche pour quantifier le risque d'un profil utilisateur en fonction des paramètres de confidentialité. D'autres auteurs ont fourni des recommandations aux utilisateurs dans le but de minimiser les risques en surveillant leurs comportements de divulgation (Hélou *et al.*, 2012).

Ces techniques sont bien évidemment insuffisantes dans le cas des interactions en ligne car elles s'appuient sur les paramètres du profil de l'utilisateur pour évaluer le risque. Toutefois, la divulgation des données personnelles dans les interactions sociales, que ce soit dans un contexte d'apprentissage ou non, se fait beaucoup plus dans les échanges textuels entre les apprenants.

L'absence des technologies de protection pertinentes et suffisantes de la vie privée dans ces contextes est notamment due à l'absence des travaux qui ont abordé cette question de la protection contre la divulgation de données personnelles d'une part et d'autre part à l'évolution des pratiques, comportements des utilisateurs et par conséquent des risques courus. Par ailleurs, une protection de la vie privée est nécessaire dans un contexte d'apprentissage pour garantir un environnement favorable aux apprenants pour évoluer et apprendre sans être privé d'un niveau essentiel de personnalisation et d'interaction pour maintenir leur motivation et engagement sur les tâches d'apprentissage.

2.2.6. Conclusion

Bien qu'il soit difficile de cerner toutes les problématiques de la vie privée, nous avons essayé, dans ce chapitre, de préciser les principaux risques liés à la divulgation dans les contextes d'apprentissage ainsi que les solutions qui ont été proposées pour sa préservation.

Nous croyons que garantir à l'apprenant la liberté d'évoluer dans un milieu favorable à l'apprentissage et à la construction de la connaissance et l'intelligence collective exige d'abord de faire bénéficier les utilisateurs d'une bonne information sur les risques et sur les techniques adéquates de protection pour assurer leur autonomie. La protection de la vie privée des utilisateurs inclut non seulement la préservation de leurs données personnelles une fois recueillies mais aussi leur fournir un contrôle et une souveraineté à la fois dans leur apprentissage et leur protection. Un défi à relever ici réside dans ce que les chercheurs qualifient de paradoxe de la vie privée. En effet, même si les utilisateurs sont conscients des différents risques liés à la divulgation, leur comportement ne reflète pas souvent leurs préoccupations.

Dans cette perspective, nous supposons que toute solution de protection concernera un compromis (ou trade-off) entre la divulgation d'une part et la protection de la vie privée d'autre part.

Nous discuterons plus en détail, dans le chapitre suivant, le problème de la protection de la vie privée dans les environnements d'apprentissage social informel ainsi que la solution que nous proposons pour y répondre.

Chapitre 3 : Problématiques de recherche

Les premiers environnements d'apprentissage offraient des fonctions de personnalisation visant à adapter l'apprentissage aux caractéristiques de l'apprenant (Sleeman et Brown, 1982). Dans ce contexte, la personnalisation dépendait surtout de la représentation de connaissances dans un modèle d'apprenant. Toutefois, dès l'apparition des réseaux sociaux, des interactions en ligne et de l'apprentissage social, il est devenu indispensable de représenter aussi le contexte dans lequel l'apprenant évolue.

Bien que les fonctionnalités visées aujourd'hui par les systèmes d'apprentissage soient bien différentes, l'objectif était toujours de soutenir les apprenants en leur offrant de nouveaux outils favorisant leur apprentissage. Dans cette perspective, Vassileva (2008) a confirmé que soutenir l'apprentissage d'aujourd'hui requiert la mise en œuvre des outils considérant le contexte social de l'apprentissage. Pour cela, l'auteure a identifié trois objectifs principaux pour les environnements d'apprentissage social : (a) *accompagner l'apprenant dans sa mise en relation avec les partenaires d'interaction appropriés* (b) *accompagner l'apprenant dans sa recherche du contenu pertinent* et (c) *l'encourager et le motiver dans son apprentissage*.

Pour atteindre ces objectifs, les chercheurs se sont appuyés sur des travaux menés dans différents domaines pour identifier et recommander des ressources d'apprentissage pertinentes (Vuorikari *et al.*, 2009), motiver les apprenants lors des sessions d'apprentissage (Derbali et Frasson, 2012) et modéliser la présence humaine en considérant les partenaires d'interaction (Nowakowski *et al.*, 2014).

Cependant, la vie privée est un facteur qui a reçu peu d'attention de la part des chercheurs malgré qu'il soit un élément indispensable dans un contexte social d'apprentissage. Les premiers travaux soutenant l'apprentissage social ont surtout exploré des éléments de la présence sociale en étudiant les bénéfices d'intégrer les outils d'interaction entre apprenants dans les environnements d'apprentissage et d'adapter l'apprentissage aux caractéristiques des réseaux sociaux. Le défi est alors de proposer des services de façon à ce que les interactions entre apprenants tiennent compte de la nécessité de protéger la vie privée sans affecter la structure et l'organisation de l'apprentissage social.

Dans cette recherche, nous nous intéressons principalement aux deux premiers objectifs parmi les trois établis par Vassileva (2008). Nous allons détailler dans ce chapitre les problématiques de vie privée dans les fonctionnalités associées à ces deux objectifs ainsi que la solution que nous proposons pour protéger la vie privée des apprenants.

3.1. Paradoxe de vie privée

La question de la protection de la vie privée n'est pas nouvelle dans le contexte d'apprentissage, mais la nécessité de la considérer devient plus urgente dès lors que les environnements d'apprentissage incluent des outils d'interaction en s'inspirant de la théorie socioconstructiviste (Lowenthal *et al.*, 2009). La protection de la vie privée d'un apprenant dans une interaction sociale en ligne veut dire aussi bien se protéger contre les potentielles intrusions de ses co-apprenants, que gérer les flux d'informations qu'il envoie lui-même vers eux. En effet, beaucoup d'apprenants croient que la divulgation de données personnelles lors des interactions sur les plateformes d'apprentissage en ligne est sans risque et qu'ils sont encouragés à partager plus de renseignements personnels afin de renforcer leur présence sociale et maximiser leurs opportunités d'apprentissage en interagissant avec des co-apprenants de même langue, âge, objectifs d'apprentissage, etc.

Néanmoins, une récente étude de Taddicken (2014) a révélé que dans les interactions sociales en ligne, tout le monde partage des données personnelles, et pourtant tout le monde exprime un souci et une préoccupation de sa vie privée. En effet, cela fait plusieurs années que les chercheurs affirment qu'il existe une grande divergence entre les préoccupations en matière de vie privée et les comportements réels des utilisateurs en ligne, faisant référence à ce qu'ils appellent le paradoxe de la vie privée. Ce paradoxe désigne la contradiction entre la conscience des menaces réelles de la divulgation des données personnelles et la tendance des utilisateurs à divulguer souvent leurs données.

Christofides *et al.* (2009) ont confirmé, à leur tour, l'existence de cette dichotomie suite à une expérience qu'ils ont menée pour évaluer l'influence des bénéfices attendus par les utilisateurs et les risques de divulgation sur leurs intentions de partager des données personnelles. Les auteurs ont conclu que les utilisateurs partagent activement des renseignements personnels en dépit de leurs préoccupations, car ils ne tiennent pas compte uniquement les risques mais aussi les bénéfices de la divulgation. Ils ajoutent que la perception du risque élevé est une

motivation insuffisante auprès des utilisateurs pour opter pour la protection, malgré la connaissance des stratégies de protection.

D'un autre côté, certains chercheurs ont associé ce paradoxe à la différence de sensibilité des données. En effet, il existe plusieurs types de données personnelles et les utilisateurs leur attribuent des valeurs différentes selon leur sensibilité et les risques potentiels de leur divulgation (Mothersbaugh *et al.*, 2011). Les informations tels que l'âge, l'origine, la religion, l'état de santé ou l'historique de navigation sont différentes les unes des autres et donc leur divulgation entraine des risques différents à savoir sociaux, psychologiques (par exemple l'intimidation et le harcèlement) et financiers (par exemple l'usurpation d'identité). Par conséquent, il parait absurde, selon Mothersbaugh *et al.* (2011), de comparer les préoccupations des utilisateurs et leurs comportements sans tenir compte de leurs perceptions de sensibilité des données. D'autres chercheurs dont Morando *et al.* (2014) expliquent ce paradoxe par l'influence du contexte de l'interaction sur le comportement de divulgation. Les auteurs ont indiqué que le contexte influence non seulement les comportements mais aussi les perceptions des utilisateurs.

Dans un contexte d'apprentissage, il a été démontré que les perceptions et les attentes sont des facteurs cognitifs importants influençant les intentions de comportement des apprenants ainsi que leurs comportements réels. Cette hypothèse a été appuyée par plusieurs expériences dont celle de Tsai et *al.* (2011) qui ont étudié le comportement de divulgation des étudiants versus leurs intentions collectées quelques semaines plutôt. Les auteurs ont expliqué la divergence entre le comportement réel et l'intention par le fait que l'étude ait eu lieu dans un environnement familier et visiblement protégé (salle de cours) pour les étudiants.

Partant du principe que l'interaction est un moyen pour accéder à l'aide des co-apprenants, les perceptions que les apprenants avaient des avantages et des risques ont influencé leurs comportements, et plus particulièrement la demande d'aide (Troncy *et al.*, 2011). Deux types de comportements ont été alors identifiés selon les perceptions. Plus les apprenants ont déclaré percevoir les avantages de la demande d'aide, plus ils en ont eu recours durant l'apprentissage (Troncy *et al.*, 2011). En contrepartie, plus les apprenants ont déclaré percevoir les risques de la demande d'aide (diminution de l'estime de soi et jugements négatifs des autres), plus ils l'ont évitée durant leur apprentissage (Butler, 2007).

Les travaux susmentionnés soutiennent tous l'hypothèse de l'existence de paradoxe entre les préoccupations des utilisateurs eu égard à la vie privée et leurs comportements de divulgation

en ligne, mais leurs interprétations ne fournissent pas réellement d'explications concernant l'évaluation et l'influence des facteurs risques et avantages sur la décision de divulgation. Dans cette perspective, Miltgen et Peyrat-Guillard (2014) suggèrent alors de donner aux utilisateurs le contrôle sur la décision de divulgation ou la protection de la vie privée dépendamment de leurs préférences et de leurs perceptions eu égard aux facteurs de risques et avantages de la divulgation. Néanmoins, Young et Quan-Haase (2013) ont révélé que la décision de la protection de vie privée est grandement affectée par le manque d'informations et la rationalité limitée des utilisateurs.

S'il ne faut pas bien entendu surestimer la dimension rationnelle des comportements des utilisateurs, les pratiques montrent que l'attention portée à la protection de la vie privée ne pèse pas lourd dans la balance face aux avantages que la divulgation semble procurer aux utilisateurs. Les chercheurs ont établi que les avantages de divulgation des données personnelles sont associés à trois besoins fondamentaux : le *besoin de divertissement*, le *besoin de relations sociales* et le *besoin de la construction de l'identité* (Miltgen et Peyrat-Guillard, 2014). Particulièrement dans le contexte d'apprentissage informel, dont l'objectif de l'apprenant est d'accéder à l'aide des autres afin de résoudre un problème lié à son apprentissage ou compléter la compréhension d'un savoir, la divulgation des données ne semble pas être un obstacle.

Bien qu'on puisse s'étonner du caractère dérisoire de la récompense offerte - l'accès à l'aide des autres-en contrepartie d'une divulgation qui peut entrainer une atteinte à la vie privée, il demeure que, dans les faits, les utilisateurs cèdent bien souvent sur leurs exigences en matière de vie privée. Selon Rochelandet (2010), il est bien difficile d'être confiant dans la capacité des individus à prendre les décisions conformes à leurs intérêts en matière de vie privée. En effet, la plupart des utilisateurs n'ont pas la capacité de calculer les risques et les bénéfices de la divulgation et n'ont surtout pas accès aux informations nécessaires pour prendre une décision pertinente sur le compromis divulgation et vie privée. Selon Acquisti *et al.* (2015), les individus prennent généralement une décision rapide basée sur une vision incomplète des risques et des avantages. Selon Kokolakis (2015), la rationalité limitée des utilisateurs en termes de calcul des bénéfices et risques de divulgation ainsi que l'absence des outils et solutions permettant leur évaluation favorisent la divulgation des données plutôt que leur protection.

Par ailleurs, Taddicken (2014) ajoute que la décision de protection ou de divulgation dépend d'autres facteurs, dont principalement l'influence sociale. Cette variable désigne la réciprocité du comportement de divulgation chez les utilisateurs (*you tell me and I tell you*). Ces derniers se prêtent volontiers à la divulgation de leurs informations personnelles sous la pression du groupe et la crainte d'être socialement isolés s'ils ne s'engagent pas dans le même comportement que leurs pairs. Ceci étant dit, l'utilisateur demeure libre de décider de divulguer ses données personnelles même si cette liberté est parfois sous contrainte.

Bien que le paradoxe de la vie privée ait été abordé par plusieurs chercheurs dans plusieurs disciplines (sociologie, psychologie et informatique), aucun modèle théorique n'a été proposé pour appuyer le compromis entre la préservation de vie privée et la divulgation, et aider ainsi les utilisateurs dans leurs décisions. D'ailleurs, les travaux qui ont étudié ce paradoxe l'ont abordé en isolant le comportement de divulgation de l'utilisateur du contexte d'interaction.

Une considération de ces facteurs s'avère nécessaire afin de trouver un équilibre entre ces deux notions visiblement contradictoires : la **divulgation des données personnelles** imposée par l'évolution sociale et technologique et la **protection de la vie privée** mise d'autant plus en danger dans le contexte social actuel. L'enjeu principal est donc de trouver un moyen pour soutenir l'apprentissage, situé dans les interactions sociales en ligne, tel que recommandé par Vassileva (2008) tout en considérant la protection de la vie privée des apprenants, plus particulièrement des risques de l'auto-divulgation de leurs données personnelles.

3.2. Problématiques

S'il est devenu fréquent de porter atteindre à la vie privée dans les interactions sociales en ligne, cela veut dire que l'atteinte provient aujourd'hui surtout de cet aspect social tel que suggéré par Steeves (2009). Selon l'auteure, cela n'est pas le simple résultat d'une mauvaise application d'une politique de protection de la vie privée, mais plutôt le résultat d'une mauvaise définition de la vie privée, incompatible avec les risques émergents aujourd'hui. En effet, on transforme la violation de la vie privée aujourd'hui en un problème quelque peu aléatoire et causé de façon imprévisible par des personnes difficiles à retracer (Hasebrink *et al.*, 2011).

Dans cette optique, Steeves (2009) indique que la protection de la vie privée doit être étendue pour tenir compte du contexte social. D'autres chercheurs se sont penchés sur la proposition des solutions visant à réguler les comportements des utilisateurs afin de protéger leur vie

privée. Dans ce sens, encourager simplement la non-divulgation des données personnelles et l'abandon des environnements sociaux constitue une solution inefficace parce qu'elle sous-estime la valeur de ces environnements dans la vie sociale d'aujourd'hui et plus particulièrement pour l'apprentissage informel.

Il ne semble pas raisonnable donc de simplement se retirer des environnements d'interaction sociale qui peuvent fournir de grandes opportunités pour soutenir l'apprentissage. Il ne semble pas possible également de retenir toute divulgation des données parce que dans le contexte de connectivité sociale d'aujourd'hui, la protection de la vie privée de chaque individu ne peut pas se réaliser dans l'isolement et sans considérer le contexte.

Ceci étant dit, du point de vue de la vie privée, soutenir l'apprentissage social revient à trouver un compromis entre la protection de la vie privée et la divulgation des données personnelles dans les contextes d'interaction sociale, plus particulièrement ceux informels. Cela implique de résoudre principalement trois problématiques illustrées dans les points suivants :

1. **la sélection des partenaires d'interaction appropriés :** Du point de vue de l'apprentissage, sélectionner des partenaires appropriés signifie mettre en œuvre des techniques pour aider un apprenant à trouver des pairs ou des partenaires *ayant les compétences nécessaires* pour fournir l'aide à l'apprenant en question dans le contexte précis de la demande d'aide.

   Cependant, on peut constater aujourd'hui que les environnements d'apprentissage social informel se basent uniquement sur la similarité entre les profils d'apprenants (même langue, même objectifs d'apprentissage, etc.) pour proposer des pairs (par exemple les réseaux sociaux d'apprentissage des langues). Sinon, ils ne fournissent aucun outil pour aider les apprenants à trouver des partenaires (par exemple dans les forums de discussion).

   La première option a l'avantage de réduire la charge cognitive de l'apprenant imposée par la recherche des partenaires d'interaction mais ne garantit pas de sélectionner des partenaires qui peuvent répondre aux besoins d'apprentissage quand ils surgissent. En revanche, la deuxième option a l'avantage de maintenir l'aspect spontané de l'apprentissage informel mais elle soulève autant de défis du point de vue de la protection de vie privée. En effet, il n'est plus suffisant dans le contexte actuel centré sur l'interaction et la divulgation des données personnelles de considérer uniquement

des variables liées à l'apprentissage dans la sélection des pairs. Il est nécessaire de considérer des variables sociales relatives essentiellement aux personnes impliquées dans l'interaction telles que la confiance et la réputation qui visent à garantir un climat favorable à l'interaction et à l'apprentissage.

2. **L'estimation des risques de la divulgation des données et le compromis entre la divulgation et la protection de vie privée :** On est passé d'une conceptualisation de la vie privée comme un noyau des données sensibles à protéger des intrus à une nouvelle vision centrée sur la divulgation de ces données et la négociation de la vie privée dans un contexte façonné par les interactions sociales. Dans ce nouveau contexte, trouver un compromis entre la divulgation et la protection requiert l'évaluation des risques et des avantages de cette divulgation pour proposer une meilleure méthode de protection. Toutefois, ces deux facteurs sont difficiles à observer et à évaluer parce qu'ils reflètent des besoins et des préoccupations principalement psychologiques. En plus, les utilisateurs ont une vision incomplète des risques, ce qui entraine généralement la divulgation des données lorsqu'ils doivent effectuer un calcul entre une perte sous-estimée de la vie privée et un gain potentiel de la divulgation. Par ailleurs, contrairement aux informations qui peuvent être publiées par des organismes, les informations divulguées et dévoilées volontairement par la personne elle-même lors des interactions sont d'autant plus difficiles à contrôler et à retracer (Hough, 2013). Dans les faits, il est très difficile d'empêcher les autres (individus ou institutions) d'exploiter des informations sensibles que l'individu lui-même a fait circuler ou dévoiler. Il est encore plus difficile d'évaluer les risques encourus par l'auto-divulgation.

   Or, la vie privée est un *concept individuel* et *contextuel*, selon Nissenbaum (2009), elle devrait être mesurée séparément pour chaque individu dans un contexte bien déterminé. Trouver un compromis repose alors sur la mise en œuvre d'un processus de contextualisation de la protection de vie privée visant à adapter la divulgation des données aux besoins de l'apprentissage.

3. **la recherche de contenus pertinents dans les interactions :** Les interactions sociales dans les contextes d'apprentissage informel peuvent entrainer la désorientation de l'apprenant et augmenter sa confusion. En effet, dès que l'espace d'informations accessibles par navigation devient important, l'apprenant peut perdre des repères et n'arrive pas à discerner les informations pertinentes. Pour cela, il convient, dans le

contexte d'apprentissage social, d'accompagner l'apprenant dans sa recherche de contenus pertinents. Par contenus ici, nous désignons les feedbacks donnés par les pairs suite à une demande d'aide. Ces feedbacks peuvent être *positifs* visant la collaboration et la construction de la connaissance comme ils peuvent être *négatifs* omettant toute opportunité d'apprentissage. Si on conçoit les comportements négatifs et intrusifs (extorsion, chantage, usurpation d'identité, cyberintimidation) comme une atteinte à la vie privée dans le contexte actuel, on se représente les interactions sociales comme des moyens qui exploitent les renseignements personnels pour les raisons les plus viles. Dans ce cas-là, les conséquences sont généralement aussi graves sur le plan d'apprentissage que sur le plan de la vie privée. Rappelons ici la triste histoire d'Amanda Todd. Une jeune canadienne qui s'est suicidée suite à une cyberintimidation.

Ceci dit, il est nécessaire de trouver un moyen pour évaluer et analyser automatiquement les interactions entre apprenants pour deux raisons : garantir un espace interactionnel favorable à l'apprentissage et préservant la vie privée (1) et aider l'apprenant dans la recherche du contenu pertinent (2).

Après avoir décrit brièvement les problématiques que nous envisageons d'aborder dans cette thèse, nous discuterons dans la section suivante la solution que nous proposons pour résoudre ces problématiques et assurer une protection de la vie privée, des risques de l'auto-divulgation surtout, dans un contexte d'interaction sociale en ligne.

3.3. Gestionnaire de vie privée : une solution en trois axes

La pertinence de cette recherche est issue de la réflexion de Vassileva (2008) qui pose l'apprentissage social comme la base de l'apprentissage futur et l'apprentissage tout au long de la vie. A celui-ci s'ajoute le bouleversement provoqué par les technologies les plus récentes, telles que le *mobile learning* et les MOOCs (*Massive Open Online Course*), qui ont bousculé la conception même de l'apprentissage (Sharples *et al.*, 2015).

Pour ces différentes raisons, les interactions sociales entre apprenants constituent une pertinence et une spécificité en tant qu'objets d'étude scientifique, surtout depuis que l'apprentissage social en ligne, et plus spécifiquement l'informel, est passé d'un statut de occasionnel à celui de plus répandu et plus recherché (Simonson *et al.*, 2011).

Avant de décrire la solution que nous proposons pour remédier aux défis posés en matière de vie privée dans les contextes d'apprentissage informel, nous commençons par présenter les cadres théoriques sur lesquels nous nous sommes basés pour proposer notre solution.

3.3.1. Cadres et fondements théoriques

Les travaux relatifs à l'apprentissage social font état d'une diversité d'influences théoriques sur les origines de ce type d'apprentissage et son évolution. Certains auteurs l'attribuent au principe de coopération entre élèves de Jan Amos Comenius (Alava, 2010). Comenius recommandait l'enseignement mutuel afin d'aider les nouveaux apprenants, car, entre pairs on est moins timide et l'on n'a pas honte d'expliquer des choses et de poser des questions (Falchikov et Blythman, 2001). Pour désigner ce type d'interactions entre pairs, les chercheurs ont d'ailleurs eu recours à différentes appellations (Duthoit, 2014). On l'a désigné alors de travail de groupe, d'aide mutuelle, d'apprentissage collaboratif, d'apprentissage coopératif, de tutorat entre pairs, d'apprentissage social, bien que ces différentes appellations renvoient parfois à des modalités d'interactions différentes et à des fondements théoriques très différents.

Selon Johnson *et al.* (2000), les fondements théoriques derrière ce type d'apprentissage seraient les théories de l'interdépendance sociale (Deutsch, 1980), du développement cognitif (Suizzo, 2000) et principalement celles de l'apprentissage social (Bandura, 1986). La théorie de l'interdépendance sociale considère que l'interdépendance entre les apprenants faisant partie d'un même groupe ou communauté, peut être positive, négative ou inexistante. Mettre en place une situation coopérative revient à promouvoir les échanges entre les personnes, à les faire collaborer. La même théorie de l'interdépendance sociale postule par ailleurs que, par nature, les relations sociales présentent un caractère conflictuel. La résolution des conflits prend alors des formes distinctes selon la situation d'interaction (Deutsch, 1980). Une situation coopérative autorise une résolution saine et constructive eu égard aux conflits interindividuels. Une situation compétitive est à l'origine d'une résolution malsaine et négative de ces mêmes conflits.

S'appuyant sur ces théories, il est judicieux d'estimer que l'apprentissage social et plus spécifiquement informel, en raison de ses caractéristiques (degré élevé d'autonomie des étudiants et flexibilité) n'inclut pas nécessairement d'indépendance. En effet, il peut y avoir diverses formes de collaboration entre pairs, tout comme des activités d'apprentissage en

groupe qui ne correspondent pas nécessairement aux définitions susmentionnées. Dans ce sens, Poellhuber *et al.* (2008) ont avancé que la collaboration entre pairs, découlant de simples échanges non structurés, constitue une première forme de collaboration où il n'y a pas nécessairement interdépendance menant à l'atteinte d'un but commun, mais il y a des interactions. Aussi évidentes qu'elles soient, ces interactions ne sont pas moins importantes pour l'apprentissage et l'auto-socio-construction de la connaissance, mais requièrent l'instauration d'un espace favorisant la coopération plutôt que la compétition.

La présente recherche a donc pour objectif d'améliorer les interactions et l'entraide entre apprenants dans le contexte d'apprentissage social informel. Le principal défi étant de conserver la flexibilité, l'aspect spontané et les avantages de ce type d'apprentissage, tout en y associant les aspects positifs de l'interaction et du soutien social entre pairs. À cette fin, nous nous sommes appuyés sur la théorie de la liberté coopérative élaborée par Paulsen (2008). Selon cette théorie, de nombreux étudiants souhaitent pouvoir concilier les avantages de l'apprentissage en ligne (émancipation des contraintes liées au temps et à l'espace, et choix du rythme d'apprentissage) avec les avantages de l'apprentissage social (accès à l'aide et au soutien des autres, collaborer pour poursuivre un but d'apprentissage) et bien évidemment la liberté de choisir le type de média, de contenu et les modalités d'accès à ces contenus.

Selon Paulsen (2008), il est possible d'encourager la collaboration à court terme entre apprenants en leur laissant le choix du moment et de la durée d'interaction et de les amener à travailler ensemble et à s'entraider. Cela est possible en mettant en œuvre des outils favorisant les interactions entre pairs et le développement d'un sentiment de présence sociale susceptibles d'influencer positivement leur apprentissage.

En nous appuyant sur cette théorie de la **liberté coopérative**, nous avons fait en sorte que les étudiants inscrits dans un cours sur une plateforme d'apprentissage puissent avoir le choix de suivre un cours à leur rythme (synchrone ou asynchrone), de s'engager ou non, dans une démarche de socialisation à l'intérieur de la communauté d'apprentissage. L'étudiant inscrit dans un cours disposait de toutes les ressources nécessaires pour apprendre d'une façon autonome et demander le soutien approprié pour entrer en relation de façon informelle avec les autres étudiants présents dans le même cours.

Nous lui laissons en outre la pleine liberté quant à ses interactions (quand demander l'aide) tout en l'encourageant à échanger avec ses pairs pour avoir l'aide quand il en a besoin. Nous avons mis en place aussi une approche d'engagement entre les différents membres en

instaurant un mécanisme d'interaction dynamique basé sur l'évaluation des feedbacks échangés et la confiance entre apprenants pour préserver la vie privée et favoriser les échanges positifs.

Nous sommes partis de la prémisse de base qu'à compter du moment où un étudiant rejoint un environnement d'apprentissage social informel, il en deviendrait éventuellement un membre actif, encouragé à s'engager davantage dans sa communauté en offrant l'aide aux autres selon ses compétences et à solliciter l'aide de ses pairs lorsqu'il en a besoin.

3.3.2. Solution proposée

À la lumière des cadres et théories susmentionnés, nous proposons **un cadre,** que nous avons appelé **gestionnaire de vie privée**, visant à protéger la vie privée d'un apprenant lors de ses interactions avec ses pairs en (1) *recommandant des pairs appropriés pour fournir l'aide nécessaire*, (2) *adaptant la divulgation des données personnelles aux besoins d'apprentissage* et (3) *analysant les feedbacks fournis par les pairs* en vue de supprimer tout feedback affectant négativement l'apprentissage. Le cadre proposé est composé de **trois modules** correspondant aux trois problématiques de notre recherche évoquées ci-haut : *sélection des pairs*, *décision de divulgation* et *composition des feedbacks*.

Comme illustré dans la figure 5, ces **trois modules** contiennent **six sous-modules** : *Filtrage* est responsable de la sélection des pairs. L'*évaluateur de confiance*, le deuxième sous-module, a pour rôle d'évaluer le niveau de confiance des pairs sélectionnés pour fournir l'aide. Tandis que le sous-module d'*anonymisation* se charge d'*anonymiser* les données des apprenants, et que l'*estimateur de risques* évalue le risque de la divulgation des données de l'apprenant. Le sous-module *divulgation* décide de la quantité des données à dévoiler à chaque pair sélectionné. Enfin, les sous-modules de *composition des feedbacks* se chargent d'analyser les interactions des apprenants pour supprimer les feedbacks négatifs qui pourraient gêner l'apprentissage.

Ce cadre a pour objectif principal de soutenir l'interaction et l'entraide entre apprenants dans les contextes d'apprentissage social informel tout en préservant leur vie privée principalement des risques de l'auto-divulgation des données personnelles. Il permet également de résoudre le paradoxe de vie privée en contextualisant la protection de vie privée et en adaptant la divulgation des données personnelles aux besoins d'apprentissage.

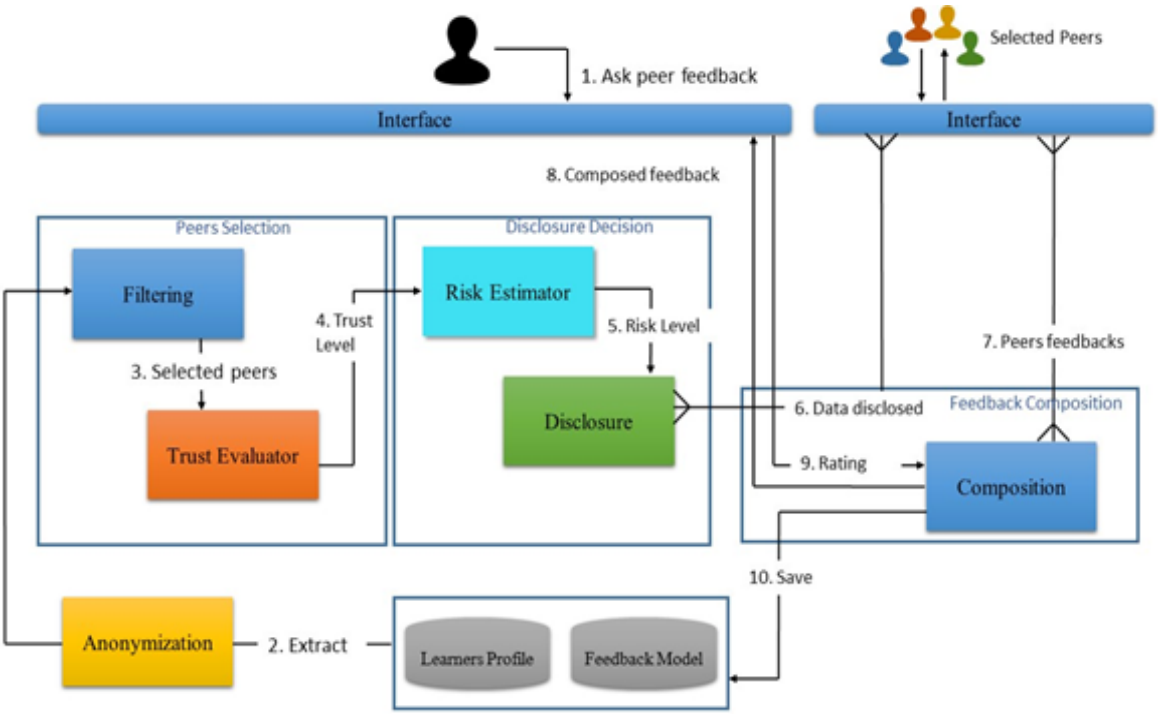


Figure 5 – Architecture générale du cadre proposé

Pour illustrer l'apport du **gestionnaire de vie privée**, reprenons l'exemple de l'apprenant Bob (voir section 1.2 page 2). La mise en œuvre du cadre proposé dans cette recherche dans un environnement d'apprentissage social informel permettra à Bob d'avoir l'aide de ses pairs plus facilement et plus rapidement. En effet, il n'a plus à chercher lui-même des pairs ayant la compétence et l'agréabilité pour fournir l'aide sans l'intimider ou le ridiculiser. Il n'a qu'à spécifier quelques informations concernant sa requête et le module *Sélection des pairs* (chapitre 4) se chargera de trouver les pairs appropriés pour l'aider.

De ce fait, Bob pourrait dès lors se concentrer sur le but principal de son interaction avec les autres qui est l'apprentissage plutôt que de gérer les éléments de ses interactions (à qui demander l'aide, comment, etc.).

Si Bob souhaite avoir des feedbacks personnalisés de la part de ses pairs sans trop divulguer des informations à propos de lui-même, il n'a qu'à spécifier ses préférences de divulgation au moment de l'écriture de sa requête. Le module *Décision de divulgation* (chapitre 5) procèdera à estimer les risques potentiels et à adapter la divulgation au contexte d'apprentissage. Cela permet de résoudre le dilemme de paradoxe de vie privée, vu que l'apprenant n'a plus à prendre la décision entre la divulgation des données et la protection de sa vie privée. Cela

permet également d'éviter l'auto-divulgation excessive et de s'engager dans une interaction risquée (avec des pairs abusifs par exemple).

Rappelons que notre apprenant Bob hésite à demander l'aide de peur de recevoir des feedbacks négatifs de ses pairs. Pour pallier ce problème, le module *Composition des feedbacks* (chapitre 6) analyse et classifie les feedbacks avant de les envoyer à Bob. De fait, tout feedback négatif (intimidant, ridiculisant, etc.) pouvant affecter négativement l'apprentissage et l'état émotionnel de l'apprenant est supprimé. Cette analyse des feedbacks est indispensable dans les contextes d'apprentissage informel parce que la nature des interactions influence en profondeur les apprentissages qui en découlent : des interactions négatives omettent toute opportunité d'entraide et d'apprentissage, tandis que des interactions positives maintiennent des apprenants motivés, engagés et coopératifs.

Nous nous sommes penchés sur le choix d'une application et d'un environnement qui, tout en permettant le réseautage social et la gestion du contenu, étaient assez flexibles en matière de communication, de partage et de collaboration entre les apprenants. L'objectif étant de trouver un environnement qui, tout en offrant une base de fonctionnalités, pouvait être adapté, modifié et étendu pour intégrer le cadre proposé dans cette recherche comme un module supplémentaire ayant pour rôle de gérer la protection de la vie privée. À cet égard, de nombreux logiciels sociaux à code ouvert peuvent être utilisés (par exemple ELGG), mais nous avons choisi de mettre en œuvre les différents modules de notre gestionnaire de vie privée de façon ad hoc.

3.4. Conclusion

En mettant à profit le potentiel qu'offrent les interactions sociales en ligne, la présente recherche vise à favoriser la collaboration et l'entraide entre apprenants, tout en préservant leur vie privée afin de créer un environnement favorisant l'apprentissage.

Comme nous le verrons plus en détail dans les prochains chapitres, cette recherche vise à développer, chez les apprenants, un sentiment de présence sociale, à proposer des outils permettant d'adapter l'apprentissage dans les environnements informels au contexte éducatif ainsi qu'à mettre en relief le potentiel pédagogique des outils utilisés dans ces environnements et leur capacité à favoriser la collaboration et l'entraide entre apprenants.

Les chapitres suivants seront consacrés à nos contributions. Le chapitre 4 décrit le module de sélection des pairs pour fournir l'aide. Le chapitre 5 présente le module responsable de

l’estimation des risques potentiels de divulgation des données personnelles et de prise décision de protection de la vie privée. Le chapitre 6 présente une architecture d’analyse automatique des interactions entre apprenants soutenant la présence sociale et préservant la vie privée.

Chapitre 4 : Sélection des pairs

Les apprenants ont généralement recours aux environnements informels pour chercher l'aide dans leur apprentissage. Ils utilisent alors les forums de discussion ou la messagerie instantanée pour chercher des réponses ou poser des requêtes. Néanmoins, plusieurs requêtes restent sans réponses : il peut arriver qu'aucun des co-apprenants ne remarque qu'une question a été posée, et dans d'autres cas ils ne se sentent pas obligés d'y répondre. En plus, plusieurs apprenants hésitent de chercher l'aide de peur d'être reconnus ou ridiculisés. C'est pour cela que, la mise en œuvre d'un module de **sélection des pairs** dans les environnements d'apprentissage informel aidera les apprenants à trouver des co-apprenants appropriés pour répondre au besoin d'apprentissage. La sélection des pairs considère non seulement *des données d'apprentissage*, comme **la compétence du pair**, mais aussi *des données sociales*, telles que **la confiance** et **la réputation**, pour garantir une interaction favorisant l'apprentissage et préservant la vie privée.

Dans les sections suivantes, nous soulignons le rôle de la confiance et de la réputation dans les interactions sociales et dans la sélection des pairs. Ensuite, nous présentons brièvement les principales techniques de recommandation avant de détailler le module de sélection des pairs que nous proposons dans cette thèse.

4.1. Interaction sociale, confiance et réputation

Dans les contextes d'apprentissage social, la confiance possède plusieurs facettes : *cognitive*, *émotionnelle* (ou *affective)*, *psychologique* et *comportementale* (Alloing et Pierre, 2012).
La facette cognitive de la confiance se réfère principalement à la confiance dans la compétence de l'autre (Qureshi et Evans, 2013). Dans les faits, cela dépend de l'enregistrement des interactions passées avec la même personne. Par exemple, quand on lit des commentaires positifs et pertinents donnés par un utilisateur en réponse à une requête dans un forum de discussion, on estime que le résultat de l'interaction avec cet utilisateur sera positif. Cet exemple rappelle également la notion de *réputation*, nécessaire pour maintenir la confiance (Taddei et Contena, 2013). La réputation est associée à l'aspect comportemental de la confiance et désigne dans le contexte d'interaction sociale en ligne, l'image que les autres individus se font d'une personne.

Si l'aspect cognitif et comportemental de la confiance sont associés à la compétence et la réputation respectivement, l'aspect psychologique concerne le caractère d'un individu et sa personnalité. En effet, cet aspect est très important dans les interactions sociales parce qu'il permet de savoir si un nouvel apprenant (sans historique d'interactions) a tendance à avoir des réactions négatives ou agressives, à être abusif ou agréable et digne de confiance (Taddei et Contena, 2013). Cet aspect psychologique de la confiance dans les co-apprenants peut être évalué en se basant sur le *modèle de Big Five* ou *Five Factor Model* (Bernaud, 2008). Cet inventaire de personnalité est composé de cinq facteurs descriptifs de la personnalité d'un individu : *extraversion*, *névrosisme*, *ouverture* à *l'expérience*, *agréabilité* et *conscienciosité* (Bernaud, 2008). L'utilisation de cet inventaire permet de *reproduire un profil psychologique* d'un individu et de *prédire plusieurs comportements* par exemple si un apprenant est digne de confiance donc il est approprié pour fournir de l'aide à ses pairs.

Ceci étant dit, la confiance, composée de ces différents aspects, est l'un des éléments clés à considérer dans notre module de sélection des pairs. Avant d'entrer dans les détails de ce module, nous donnons un aperçu des travaux de sélection et de recommandation des pairs.

4.2. Systèmes de recommandation et apprentissage en ligne

Un système de recommandation est une forme spécifique de filtrage d'informations visant à présenter les éléments d'information (par exemple objets ou personnes) susceptibles d'intéresser un utilisateur (Jiang *et al.*, 2012). En guise d'exemple, les systèmes de recommandation les plus connus sont *Netflix* pour la recommandation de films et *Amazon* pour l'achat en ligne.

Dans un contexte d'apprentissage en ligne, un système de recommandation doit aider les apprenants à découvrir des activités et des ressources d'apprentissage pertinentes (matériel didactique ou collaborateurs) qui correspondent à leurs profils, au bon moment, dans le bon contexte afin de les garder engagés et motivés pour compléter leurs activités d'apprentissage efficacement (Manouselis *et al.*, 2012). C'est ce dernier point qui distingue les systèmes de recommandations des domaines comme le e-commerce de l'apprentissage en ligne. Dans cette optique, Nowakowski *et al.* (2014) ont proposé un système de recommandation pour suggérer à un apprenant des pairs avec qui il peut interagir pour collaborer dans une activité d'apprentissage. Le système proposé s'est uniquement basé sur un ensemble de critères d'apprentissage pour recommander des partenaires d'apprentissage sans considérer les

dimensions sociales dans les relations entre apprenants telles que la confiance, la réputation, etc. Or, une évolution logique des systèmes de recommandation est d'exploiter les possibilités offertes par le web 2.0 en particulier sa dimension sociale. Dans ce sens, Fazeli *et al.* (2012) ont proposé un système de recommandation basé sur la confiance pour aider les enseignants à trouver de nouvelles ressources en leur recommandant des collaborateurs dans un réseau social. Le problème dans ce système est qu'il est difficile de calculer la valeur de la confiance de nouveaux utilisateurs. Pour cela, les auteurs ont utilisé dans leurs systèmes des algorithmes de parcours de graphes et plusieurs techniques de recommandation afin de pallier aux limites de l'utilisation d'une seule technique.

Systèmes de recommandation

Quatre principales techniques de recommandation sont généralement distinguées dans la littérature : le *filtrage basé sur le contenu*, le *filtrage collaboratif basé sur la mémoire* ou sur un *modèle* ainsi que les *techniques hybrides* combinant plusieurs approches de filtrage dans le but de pallier les inconvénients de chacune (Renaud-Deputter *et al.,* 2013). Plusieurs possibilités d'hybridation sont présentées dans (Burke, 2002) dont la *pondération* (une combinaison linéaire des scores de chaque technique de recommandation), la *commutation* (il s'agit de définir les critères de commutation et de choisir une technique selon la situation) et la *cascade* (une technique qui raffine les résultats produits par une autre).

L'utilisation des techniques de recommandation révèle plusieurs difficultés affectant la qualité de recommandations. Parmi ces difficultés, nous citons principalement le problème de *démarrage à froid* qui se produit lorsqu'il n'y a pas assez de données au départ pour générer des recommandations pertinentes. Par exemple, dans un contexte d'apprentissage social, pour un apprenant nouvellement inscrit sans historique d'interactions avec ses pairs, les recommandations sont généralement aléatoires. Un autre problème des systèmes de recommandation réside dans les *données dispersées* ou *manquantes*. Ce problème se produit lorsqu'on doit recommander à un apprenant, ayant un historique limité d'interactions, un co-apprenant parmi des milliers voire des millions d'apprenants inscrits dans l'environnement d'apprentissage. Dans ce cas-ci, les recommandations sont généralement très mauvaises car trop de données sont manquantes ou dispersées (Renaud-Deputter *et al.*, 2013).

Pour résoudre ces problèmes, la plupart des environnements d'apprentissage en ligne intègrent des approches hybrides pour recommander des ressources (Hage et Aïmeur, 2009), en plus des algorithmes de parcours de graphes destinés à construire un réseau de confiance

entre utilisateurs (des contacts, amis d'un ami, etc.) (Fazeli *et al.*, 2012). Ce réseau a permis de calculer les scores de confiance des utilisateurs servant à compléter les données manquantes dans la matrice de filtrage. Bien que cela ait pu résoudre le problème de manque de données, il n'a pas permis d'éviter le problème de démarrage à froid.

Le module que nous proposons dans cette recherche se situe dans les techniques **hybrides** combinant un *filtrage basé sur le contenu* avec *un filtrage collaboratif* en **cascade**. Dans ce cas, le filtrage basé sur le contenu est appliqué en premier pour pallier le problème de démarrage à froid. Par la suite, le filtrage collaboratif raffine les résultats obtenus dans la première étape tout en réduisant l'espace de calcul pour résoudre le problème de manque de données. Les détails de la sélection des pairs seront présentés dans la section suivante.

4.3. Le module de sélection des pairs

Dans cette section, nous présentons le module de sélection des pairs que nous proposons dans cette recherche. Le module proposé doit accompagner l'apprenant dans sa recherche d'aide et garantir la protection de sa vie privée en sélectionnant des pairs compétents et appropriés.

4.3.1. Exigences d'un module de sélection des pairs

Nous avons défini les exigences suivantes auxquelles notre module de sélection des pairs doit répondre :

1. **Soutien synchrone ou asynchrone :** La question du temps est très importante dans le contexte d'apprentissage en ligne. D'une part, le soutien devrait être fourni assez rapidement pour que l'apprenant ayant besoin d'aide puisse continuer son apprentissage et surmonter ses émotions de confusion ou de frustration dues à la difficulté ou à l'ambiguïté rencontrée durant l'apprentissage. D'autre part, les pairs sélectionnés pour fournir l'aide doivent être en mesure de préparer une réponse réfléchie pour aider l'apprenant en difficulté.
2. **Équilibre de la charge cognitive entre apprenants :** Tout apprenant a une compétence dans un domaine bien précis dans lequel il pourra fournir de l'aide. Ce principe est généralement très présent dans les contextes d'apprentissage non formel où un apprenant peut jouer le rôle d'un tuteur et d'un « *tutoré* ». Ceci dit tout apprenant peut être sélectionné pour fournir de l'aide ce qui permet d'équilibrer la charge cognitive due à la réponse aux requêtes des co-apprenants. Cela veut dire que

le module ne doit pas sélectionner toujours les mêmes apprenants pour fournir l'aide, même s'ils fournissent des feedbacks pertinents.

3. **Compétence et confiance des pairs :** Le module proposé devrait être en mesure de sélectionner des pairs suffisamment compétents pour répondre au besoin de l'apprenant qui a fait la requête. La compétence signifie ici que des pairs sélectionnés sont censés être en mesure de répondre à la requête, sur la base de leur compétence et leur historique d'aide. En outre, les pairs sélectionnés doivent être crédibles, dignes de confiance (« *trustworthy* ») et agréables. Cela permettra de garantir une interaction favorisant l'entre-aide entre apprenants et préservant la vie privée (sans intimidation ou critiques agressives, etc.).

En se basant sur ces considérations, nous proposons un module offrant un soutien synchrone aux apprenants ayant besoin de l'aide de leurs pairs dans des situations d'apprentissage social informel. Les objectifs de ce module sont d'une part de soutenir la coopération entre apprenants en sélectionnant des pairs appropriés pour fournir l'aide et d'autre part de garantir un espace interactionnel préservant la vie privée.

4.3.2. Architecture

L'idée est alors de *filtrer* les apprenants afin de trouver ceux qui ont la *compétence* pour répondre à la requête formulée. Un filtrage basé sur le contenu est une bonne option mais n'est pas suffisant. En effet, un pair peut avoir les *connaissances nécessaires* pour répondre à la requête, étant inscrit dans le même cours avec un niveau supérieur par exemple, mais les feedbacks qu'il a fournis dans le passé étaient *inacceptables*. Par exemple, il se peut qu'il donne le plus souvent des feedbacks *négatifs* ou *intimidants* (tonalité ironique ou sarcastique, mots à valeur négative, critiques agressives, etc.).

Ainsi, un **deuxième filtrage** en cascade est nécessaire pour s'assurer de ne sélectionner que les pairs qui ont donné des feedbacks pertinents et acceptables dans le passé. Pour ce faire, plusieurs options se présentent : *la première* est de filtrer les pairs disponibles pour fournir l'aide en se basant uniquement sur leur historique d'aide. Un pair qui a fourni des feedbacks pertinents dans le passé a un score de *réputation élevé* et donc peut être sélectionné pour aider l'apprenant ayant besoin d'aide. Néanmoins, de cette façon, les mêmes pairs vont toujours être sélectionnés pour répondre aux requêtes de l'apprenant en question. Cela non seulement *augmente la charge cognitive* du pair (puisqu'il va toujours être sélectionné pour aider les autres), mais il peut aussi *poser un risque en matière de vie privée*. En effet, un pair qui

répond aux requêtes d'un même apprenant finirait par le *reconnaitre* même s'ils interagissent *anonymement* si cet apprenant *divulgue des données personnelles* permettant de *reconstruire son identité réelle*. Ainsi, il est possible qu'un pair puisse collecter dans chaque interaction avec le même apprenant plus de données et finisse par le *ré-identifier*. Cela rendrait l'apprenant plus vulnérable au vol d'identité, à la cyberagression ou cyberintimidation. C'est pour cette raison que nous exigeons de considérer la *confiance* et la *réputation* dans la sélection des pairs.

La deuxième option du filtrage repose sur l'idée que les apprenants sont *différents* et tendent à *évaluer différemment* les interventions et feedbacks de leurs pairs. En effet, un même feedback donné par un pair peut être évalué comme pertinent par un apprenant et peu pertinent ou non pertinent par un autre. Ceci étant dit, trouver des pairs appropriés pour aider un apprenant revient à trouver les pairs qui ont été évalués comme appropriés par les apprenants similaires à l'apprenant en question. Cette deuxième option est plus souhaitable dans notre contexte : elle permet de sélectionner des pairs appropriés et qui ont donné des feedbacks positifs dans le passé. Cette option peut être mise en œuvre à l'aide de la technique de *filtrage collaboratif*.

Pour récapituler, nous proposons un module de sélection des pairs en utilisant un filtrage basé sur le contenu et un filtrage collaboratif en cascade, tel qu'illustré dans la figure 6. Cela a pour avantage que si le premier filtrage génère peu de recommandations, la deuxième technique ne sera plus utilisée.

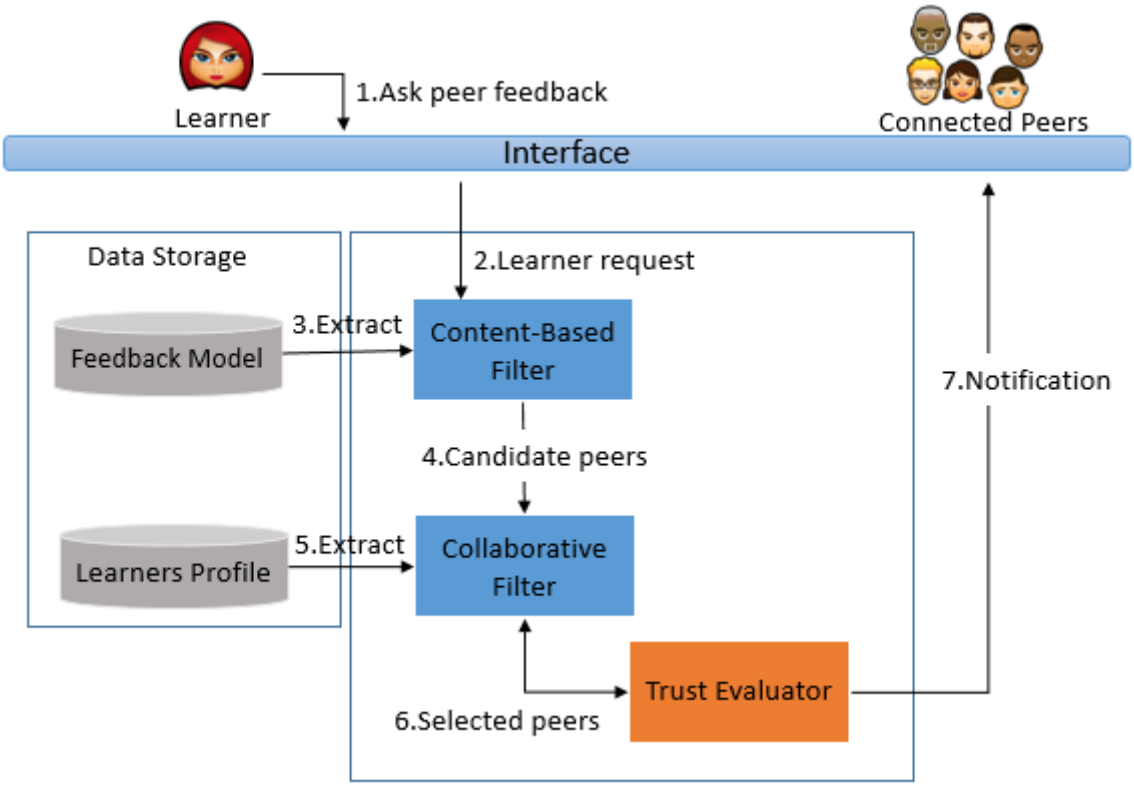


Figure 6 – Architecture du module proposé

Le filtrage basé sur le contenu est appliqué, en premier lieu, produisant un ensemble de candidats potentiels. Dans cette étape du filtrage, il s'agit d'extraire les pairs qui ont répondu à des requêtes similaires à la requête courante parmi celles formulées au passé et stockées dans le **modèle de feedback** (« Feedback Model » dans la figure 6). Puis, le filtrage collaboratif raffine cette liste en vue de retenir les pairs jugés appropriés par les apprenants similaires à l'apprenant ayant besoin d'aide. Dans cette deuxième étape du filtrage, il s'agit de trouver le **voisinage de l'apprenant** en question en se basant sur *ses évaluations des feedbacks reçus* dans le passé. Afin de retenir les co-apprenants les plus similaires, nous nous basons sur **le score de similarité** ainsi que **le score de confiance** calculé par le sous-module *Évaluateur de confiance* (« Trust Evaluator »).

Il est important de noter que dans de nombreux systèmes de recommandation, l'apprenant reçoit en recommandation une liste de contacts ou de co-apprenants avec qui il peut interagir (Manouselis *et al.*, 2012). Dans notre travail, l'apprenant ayant besoin d'aide reçoit en réponse à sa requête un ensemble de feedbacks fournis par les pairs sélectionnés. Nous avons choisi de fournir en recommandation des feedbacks plutôt qu'une liste des pairs à l'apprenant pour deux raisons : *aider l'apprenant à trouver une réponse rapidement à sa requête* en

sollicitant plusieurs pairs en même temps (1), *minimiser la distraction de l'apprenant de son objectif d'apprentissage* (il peut se laisser facilement distraire par l'interaction avec ses pairs) (2).

Les trois sous-modules de *filtrage basé sur le contenu*, *filtrage collaboratif* et é*valuateur de confiance* (figure 6) seront détaillés dans les sections suivantes. Avant cela, nous parlerons des données d'apprenants mises en jeu dans le module sélection des pairs et stockées dans le profil d'apprenant.

4.3.3. Profil apprenant

Dans un contexte d'apprentissage, le profil d'apprenant regroupe toutes les *informations démographiques* (l'âge, le sexe, le pays, le statut personnel, etc.), les *informations d'apprentissage* (le cours suivi, le niveau d'étude, etc.) et les *données d'interactions* tels que les feedbacks reçus et donnés ainsi que les notes attribuées aux feedbacks reçus.

L'*élicitation* de ces notes se fait d'une manière réactive suite à la réception des feedbacks fournis par les pairs sélectionnés. En effet, quand un apprenant reçoit des feedbacks de la part de pairs sélectionnés en réponse à sa requête d'aide, on lui demande d'évaluer chaque feedback reçu en attribuant une note parmi {1,2,3,4,5}. Les évaluations des feedbacks reçus permettent de *pouvoir modéliser l'apprenant* et d*'apprendre ses préférences de feedbacks pour pouvoir adapter les sélections à ses besoins*.

Nous avons choisi d'utiliser des notes (dites aussi *votes* ou *ratings*) pour l'évaluation parce qu'elles sont faciles à traiter : une note *élevée* signifie que l'apprenant trouve le feedback du pair *pertinent* et qu'il répond bien à son besoin d'apprentissage, tandis qu'une note *faible* signifie que l'apprenant trouve le feedback *non pertinent*.

Tel que mentionné plus haut, le profil d'apprenant comprend également des données démographiques et des données concernant l'apprentissage. Ces données, renseignées par l'apprenant lui-même lors de son inscription dans l'environnement d'apprentissage pour suivre un cours donné ou demander l'aide de ses co-apprenants, sont utilisées pour générer les sélections lorsqu'il s'agit de nouveaux apprenants (n'ayant pas d'historique de feedbacks reçus ou donnés). Ainsi, le module de sélection des pairs peut exploiter les similitudes entre apprenants, par exemple les apprenants suivant le même cours et ayant la même langue, afin de sélectionner des pairs pour fournir l'aide.

Notons aussi qu'en formulant sa requête, un apprenant doit spécifier un ensemble d'attributs liés à la requête courante tels que le cours associé, le niveau (débutant, intermédiaire, etc.), la langue, etc. Ces attributs vont être également utilisés dans l'étape de filtrage basé sur le contenu afin d'extraire les apprenants qui ont répondu à des requêtes similaires (voir table 1).

Table 1– Exemple de données du profil apprenant

Niveau	Débutant
Langue	Français
Style d'apprentissage	Visuel
Cours	Anglais
Score de confiance	0.1
Disponible	oui

Après avoir présenté la typologie des données exploitées en entrée par le module de sélection des pairs, dans les sections suivantes il est question de décrire les trois sous-modules de sélection.

4.3.4. Filtrage basé sur le contenu

Il s'agit de comparer la nouvelle requête (pour laquelle le module doit sélectionner des pairs) aux requêtes répondues précédemment par les apprenants en ligne. Étant donné que le soutien est synchrone seuls les *apprenants connectés* au moment de la requête sont considérés dans la sélection. Le filtrage basé sur le contenu dans notre contexte repose sur l'hypothèse que *les apprenants qui peuvent répondre à la requête courante sont ceux qui ont déjà répondu à des requêtes similaires*.

Calculer les similarités entre requêtes revient à calculer le degré de « ressemblance » entre les vecteurs des requêtes précédentes et la requête courante en se basant sur les attributs de filtrage comme le *cours associé*, le *niveau*, la *langue*, etc. (Voir figure 7).

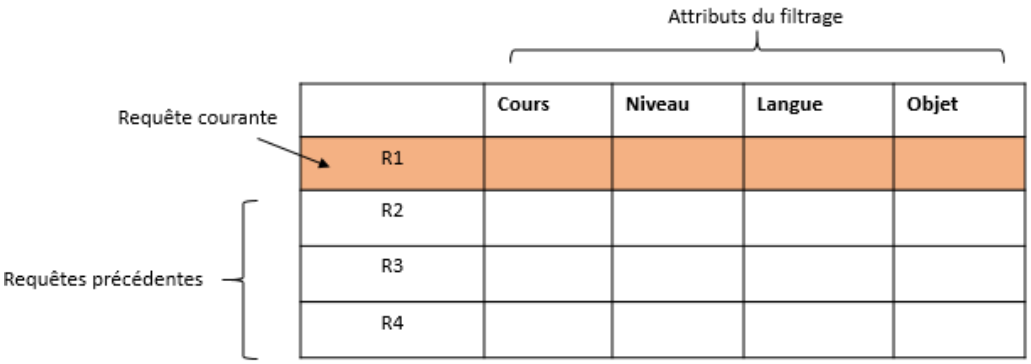


Figure 7 – Exemple de matrice de filtrage basé sur le contenu

L'élément clé de cette étape est alors la fonction qui calcule la similarité entre les deux vecteurs (requête courante, requêtes précédentes). La plupart de mesures de similarité entre vecteurs de caractéristiques peuvent être utilisées (Celma *et al.*, 2005). Nous avons utilisé la mesure de cosinus parce qu'elle est généralement efficace même quand l'espace dimensionnel devient relativement grand. La formule de cosinus utilisée est la suivante :

$$\boldsymbol{Sim}\,(\boldsymbol{X},\boldsymbol{Y}) = \cos(\theta) = \frac{X.Y}{\|X\|\|Y\|} = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\sum_{i=1}^{n}(x_i)^2}\sqrt{\sum_{i=1}^{n}(y_i)^2}}$$

Avec X et Y deux vecteurs à n dimensions représentant respectivement la requête courante et une requête précédente.

De ce fait, parmi les pairs connectés, seuls ceux qui ont posé ou répondu à des requêtes similaires seront retenus. Dans un contexte d'apprentissage social informel, un apprenant peut jouer le rôle d'un *tuteur* (s'il répond aux requêtes de ses pairs) et d'un *tutoré* (quand il demande l'aide de ses pairs). Ceci dit, un apprenant qui a déjà fait une requête similaire à la requête courante doit être sélectionné pour aider ses pairs; cela rappelle le principe de **transfert de la connaissance** qui est l'élément clé de l'interaction sociale dans l'apprentissage social informel.

Nous avons choisi d'appliquer un filtrage basé sur le contenu en premier pour pallier le problème de démarrage à froid. Ce problème se traduit par l'inscription d'un nouvel apprenant ayant besoin d'aide. Dans l'absence d'historique d'évaluations, le module de sélection ne peut pas extraire la liste des apprenants similaires à ce nouvel apprenant et donc le filtrage collaboratif ne peut pas être appliqué.

Par ailleurs, le filtrage basé sur le contenu ne peut être le seul filtre à appliquer dans le module de sélection des pairs parce qu'il va toujours faire des recommandations similaires et identiques. Or, dans un contexte très dynamique tel que les contextes d'apprentissage social informel où des milliers d'apprenants s'inscrivent et se retirent de l'environnement d'apprentissage, l'apprenant a intérêt à interagir avec tous les co-apprenants qui peuvent l'aider à poursuivre son apprentissage en répondant à ses requêtes et partageant leurs expériences personnelles. C'est pour cette raison que le filtrage collaboratif, deuxième filtre, est appliqué dans la sélection des pairs.

4.3.5. Filtrage collaboratif basé sur la mémoire

Le résultat du filtrage basé sur le contenu est une liste des pairs potentiels représentant les co-apprenants en ligne qui ont déjà posé ou répondu à des requêtes similaires à la requête courante. Le premier filtrage permet alors de sélectionner **la liste des pairs potentiels** ayant la **compétence** (ou les connaissances nécessaires) pour répondre à la requête.

Cette liste est essentielle pour le filtrage collaboratif qui repose sur l'hypothèse suivante : *les pairs les plus appropriés pour répondre à la requête d'un apprenant sont ceux qui ont été jugées comme appropriées par les apprenants similaires à l'apprenant courant.*

La similarité dans ce deuxième filtrage concerne les évaluations des feedbacks fournis par les pairs sélectionnés. Le filtrage consiste donc à déterminer les co-apprenants qui ont tendance à donner des notes similaires aux mêmes pairs sélectionnés que l'apprenant cible (qui a formulé la requête courante), ce qui revient à évaluer les similitudes entre les évaluations (les notes) données aux apprenants connectés (et sélectionnés par le filtrage basé sur le contenu).

La figure 8 explique d'une manière simplifiée la matrice *Apprenants* x *Apprenants connectés* qui sert à **trouver les apprenants similaires** à l'apprenant cible (*phase du calcul de voisinage*) afin de **prédire** les évaluations que ce dernier donnerait aux pairs potentiels à sélectionner parmi les apprenants connectés (*phase de prédiction*).

L'évaluation d'un apprenant à un pair (parmi les apprenants connectés) est illustré dans la figure ci-dessous par la note d'un apprenant A_i à un pair potentiel a_j (parmi les apprenants connectés). Étant donné qu'un pair peut être sélectionné plusieurs fois pour fournir des feedbacks en réponse aux requêtes d'un même apprenant, nous considérons la note donnée par un apprenant A_i à un pair sélectionné a_j comme **la moyenne de toutes les notes** données

aux feedbacks fournis par ce pair (sans dépasser un seuil de sélection de 10 d'un pair pour un même apprenant afin de minimiser les risques de ré-identification).

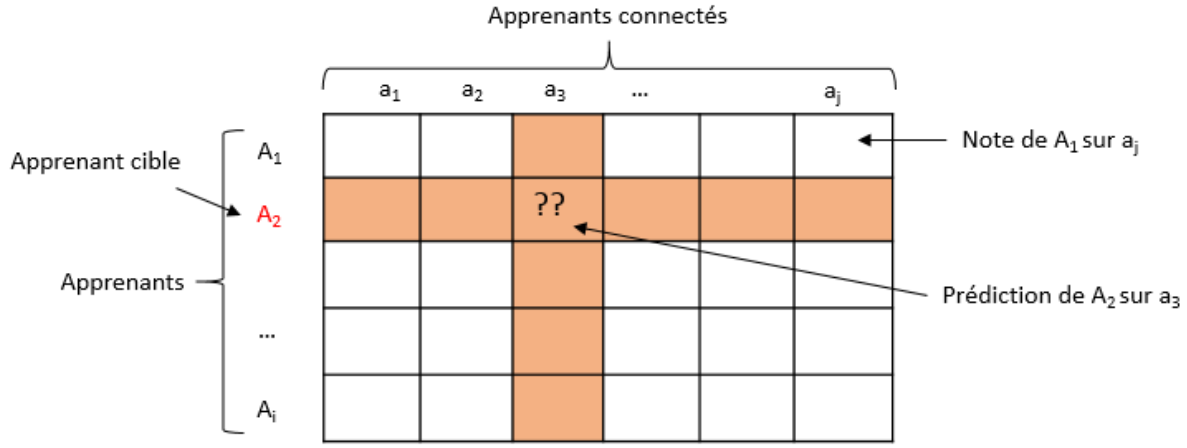


Figure 8 – Matrice Apprenants x Apprenants connectés

Ce filtrage collaboratif, dit **basé sur la mémoire**, repose sur les évaluations du voisinage pour prédire les évaluations de l'apprenant cible. Il comprend alors deux phases : *phase du calcul de voisinage* et *phase de prédiction*.

Phase du calcul du voisinage : Il s'agit de trouver les apprenants (connectés ou non), qui sont les plus similaires en termes d'évaluations des feedbacks donnés par les apprenants connectés en utilisant une mesure de similarité. La mesure la plus populaire, et qui est la plus satisfaisante dans notre contexte pour calculer les similarités entre les évaluations d'apprenants, est le *coefficient de corrélation de Pearson*. La similarité entre deux apprenants A et B est alors calculée en utilisant la formule suivante (Naak *et al.*, 2009) :

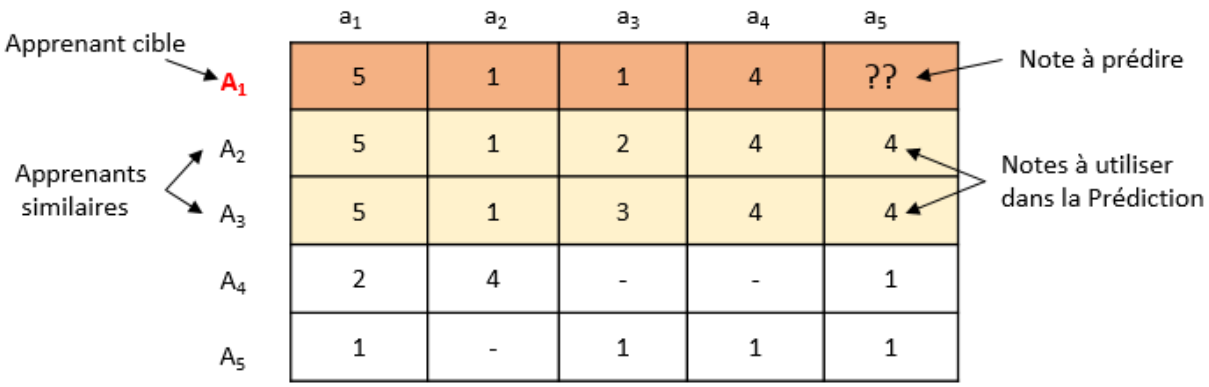
$$\boldsymbol{Simil}\,(\boldsymbol{A},\boldsymbol{B}) = \frac{\sum_j \left(v_{A,j} - \overline{v_A}\right)\left(v_{B,j} - \overline{v_B}\right)}{\sqrt{\sum_j (v_{A,j} - \overline{v_A})^2 (v_{B,j} - \overline{v_B})^2}}$$

j : nombre d'apprenants ayant été évalués par A et B

$v_{A,j}$: note de A pour l'apprenant j

$\overline{v_A}$: moyenne des notes de A

Pour mieux illustrer, prenons l'exemple de la figure 9 qui présente les notes données par 5 apprenants (dont l'apprenant cible) à leurs pairs (potentiellement sélectionnés pour répondre à la requête courante).



	a_1	a_2	a_3	a_4	a_5
A_1	5	1	1	4	??
A_2	5	1	2	4	4
A_3	5	1	3	4	4
A_4	2	4	-	-	1
A_5	1	-	1	1	1

Figure 9 – Exemple de filtrage collaboratif

En guise d'exemple de calcul des similarités par le coefficient de Pearson entre les deux apprenants A_1 et A_2 illustrés dans la figure 9, notée Simil (A_1, A_2), nous retrouvons :

$$\boldsymbol{Simil}\ (A_1, A_2) = \frac{\sum_j \left(v_{A_1,j} - \overline{v_{A_1}}\right)\left(v_{A_2,j} - \overline{v_{A_2}}\right)}{\sqrt{\sum_j (v_{A_1,j} - \overline{v_{A_1}})^2 (v_{A_2,j} - \overline{v_{A_2}})^2}}$$

$$= \frac{(5-2.75)(5-3.2) + (1-2.75)(1-3.2) + (1-2.75)(2-3.2) + (4-2.75)(4-3.2)}{\sqrt{(5-2.75)^2(5-3.2)^2 + (1-2.75)^2(1-3.2)^2 + (1-2.75)^2(2-3.2)^2 + (4-2.75)^2(4-3.2)^2}}$$

$$= 0.97$$

A partir de cet exemple, nous considérons que A_1 et A_2 sont très similaires dans les évaluations des pairs potentiels. Ainsi, les notes de A_2 seront considérées dans le calcul de prédictions pour A_1.

Cette phase de calcul de voisinage permet de générer une matrice de similarité des évaluations Apprenants x Apprenants connectés. Les voisins retenus peuvent ainsi être intégrés dans la phase suivante de calcul des prédictions.

Phase de prédiction : Une fois que les apprenants qui constituent le voisinage de l'apprenant cible sont définis, la prédiction de la valeur que l'apprenant *A* donnerait à un pair potentiel *j*, notée $P_{A,j}$, est calculée à l'aide de **la somme pondérée des notes** des voisins de *A* pour le pair potentiel *j* (Candillier *et al.*, 2009). Cette méthode considère uniquement les voisins de *A* ayant déjà évalué des feedbacks donnés par le pair *j* en réponse à leurs requêtes d'aide comme suit :

$$\boldsymbol{P_{A,j}} = \frac{\sum_{i=1}^{n} sim(A,i) * v_{i,j}}{\sum_{i=1}^{n} sim(A,i)}$$

n : nombre d'apprenants dans le voisinage de A, ayant déjà évalués le pair potentiel j

$v_{i,j}$: note de l'apprenant i pour le pair j

$sim(A,i)$: similarité entre l'apprenant cible A et l'apprenant i

Pour illustrer, reprenons l'exemple de la figure 9. Supposons que A_2 et A_3 sont les voisins retenus pour la phase de prédiction avec des scores de similarité de 0.97 et 0.88 respectivement. Afin de prédire la note que donnerait l'apprenant A_1 au pair potentiel a_5, les notes de A_2 et A_3 seront utilisées comme suit :

$$\boldsymbol{P}_{A_1,a_5} = \frac{0.97*4+0.88*4}{0.97+0.88} = 4$$

De cet exemple, nous pourrions considérer a_5 comme pair approprié pour fournir l'aide à l'apprenant A_1.

Notons que pour simplifier nous avons considéré un nombre réduit d'apprenants dans cet exemple de calcul. Néanmoins, dans les faits le nombre d'apprenants similaires à considérer dans le processus de sélection des pairs est un facteur crucial pour le calcul des prédictions. Bien que ce facteur affecte grandement la qualité du filtrage, il n'y a pas une méthode claire pour spécifier le nombre précis d'apprenants à considérer dans le calcul des prédictions. Ainsi, quand le nombre d'apprenants similaires devient grand, nous avons choisi de retenir les 20 plus proches voisins pour la phase de prédiction. En effet, diminuer le nombre de voisins peut affecter la qualité des prédictions et l'augmenter accroit le temps de calcul sans améliorer la qualité. Pour ce faire, nous considérons dans cette recherche non seulement le score de similarité mais aussi le score de confiance d'apprenants similaires à l'apprenant cible. Nous présumons que la similarité entre les deux apprenants dans les évaluations est une condition nécessaire mais insuffisante. Il faut que l'apprenant similaire soit *crédible* et *digne de confiance* pour considérer ses évaluations comme pertinentes et les intégrer dans la prédiction. Pour cela, nous retenons les 20 apprenants ayant les scores de similarité et les scores de confiance les plus élevés. Le score de confiance est calculé par le sous-module évaluateur de confiance.

4.3.6. Evaluateur de confiance

Etant donné que le but du filtrage est de sélectionner des pairs appropriés, un pair ayant tendance à être *désagréable* et *abusif* dans ses feedbacks est considéré comme *inapproprié* et *indigne de confiance* et ne doit donc pas être sélectionné pour fournir l'aide. Tel que mentionné au début du chapitre, nous considérons dans cette recherche la confiance comme une variable reflétant **l'aspect psychologique** de l'apprenant (nous désignons sa *personnalité*) et **son comportement réel** (nous désignons sa *réputation*).

Pour cela, nous avons défini un **score de personnalité,** noté T_p, permettant de recueillir des informations sur un apprenant et de prédire ses réactions dans ses interactions avec ses co-apprenants. Pour ce faire, nous avons utilisé un **test de personnalité** dit *Modèle de Big Five* (McCrae et Costa, 1999). En effet, lors de son inscription dans l'environnement d'apprentissage tout apprenant remplit un inventaire de 20 questions mesurant cinq traits principaux de la personnalité. Dans le contexte d'interactions sociales entre apprenants, nous nous intéressons principalement à deux traits de Big Five : *agréabilité* et *conscienciosité.* En effet, un apprenant ayant un score élevé d'agréabilité et de conscienciosité peut être décrit comme un individu qui accorde de l'importance au fait d'aider les autres et aux règles sociales et qui est en mesure de se tenir à la tâche qui lui est assignée tout en étant agréable et responsable. En revanche, un apprenant ayant un score faible dans ces deux traits de personnalité est considéré comme irresponsable, désagréable et ayant tendance à ne pas valoriser l'aide des autres. Ainsi, seuls les scores obtenus en réponse aux questions de ces deux traits sont considérés dans le calcul de score de personnalité d'un apprenant. Ce dernier score, correspondant au premier aspect de la confiance, est alors la moyenne des scores d'agréabilité et de conscienciosité ramenée à une échelle de [0,1]. Ce score est calculé une seule fois au moment de l'inscription, vu que la personnalité est stable en règle générale.

Comme la confiance est dynamique, sa valeur initiale reflétée par le score de personnalité est mise à jour en considérant un deuxième score, correspondant au deuxième aspect de la confiance, qui est **le score de réputation**. Ce score, noté T_r, est calculé sur la base des notes attribuées par un apprenant en réponse aux feedbacks fournis par les pairs sélectionnés pour fournir l'aide. De cette façon, les pairs qui ont fourni des feedbacks pertinents auront des scores de réputation plus élevés et ceux qui n'ont pas fourni de bons feedbacks auront de scores moins élevés. Le score de réputation correspond alors à la moyenne des notes attribuées à un pair en réponse à ses feedbacks.

Le score de confiance T d'un apprenant est une valeur dans l'intervalle [0 ,1] calculée comme suit :

$$T = T_p * T_r$$

En guise d'exemple, supposons qu'un apprenant Bob a eu un score d'agréabilité et de conscienciosité de 8 et 12 respectivement. Bob a été sélectionné 5 fois pour fournir des feedbacks à ses co-apprenants et a reçu des notes de {1,3,3,2,2}.

- Le score de personnalité de Bob est alors T_p= (8+12)/2 = 10. Ramené à [0,1] cela donne T_p= 0.625
- Le score de réputation de Bob est alors : T_r = (1+3+3+2+2)/5 = 2.2.

Une fois les deux scores de personnalité et de réputation calculés, le score de confiance de Bob, ramené à [0 ,1] devient :

T= 0.275

La mise à jour de la valeur de la confiance est alors faite à chaque fois qu'un apprenant est sélectionné pour fournir un feedback à un pair et que ce dernier a attribué une note au feedback fourni. Tel que mentionné plus haut, dans le module de sélection des pairs, le score de confiance permet de décider des voisins à retenir pour le calcul des prédictions dans le module de filtrage collaboratif. Pour déterminer si notre choix de considérer ce score dans le filtrage collaboratif permet d'améliorer la sélection des pairs, nous avons mené des tests pour évaluer l'effet de ce choix sur les prédictions.

Avant cela, nous présentons un aperçu de l'implémentation de trois fonctionnalités principales du module de sélection des pairs qui sont : la demande d'aide, la sélection des pairs et la réponse à une requête.

4.4. Implémentation du prototype

Afin d'évaluer le fonctionnement du module proposé, nous avons développé un prototype d'une plateforme d'e-learning qui implémente les 3 fonctionnalités décrites ci-dessus. Le prototype a été développé en utilisant les langages et outils suivants : PHP, JavaScript, AJAX, et MySQL. Plus précisément, la plateforme propose des leçons d'anglais langue seconde et comprend 4 niveaux. Un ensemble d'apprenants a été simulé pour tester les fonctionnalités implémentées.

Au moment de l'inscription, chaque apprenant est invité à remplir un formulaire d'inscription en précisant ses données démographiques, ses objectifs d'apprentissage, et ses qualifications (les domaines dans lesquels il peut fournir de l'aide à ses co-apprenants). Ensuite, il est invité à remplir l'inventaire de personnalité qui sert à calculer le score de personnalité.

Après avoir créé son profil, l'apprenant peut alors accéder aux leçons. Il peut utiliser les ressources d'apprentissage fournies par la plateforme ou tester les fonctionnalités implémentées (demander l'aide des pairs, répondre à une requête d'un co-apprenant si une notification de sélection a été reçue et évaluer un feedback d'un co-apprenant en attribuant une note parmi {1,2,3,4,5}). Quand un apprenant demande l'aide de ses pairs, il doit écrire une requête en spécifiant certains attributs permettant de décrire la requête dont *le cours et le niveau associés* ainsi que *les données personnelles qu'il veut divulguer aux pairs sélectionnés*, tel qu'illustré dans la figure 10, pour leur permettre de donner un feedback personnalisé.

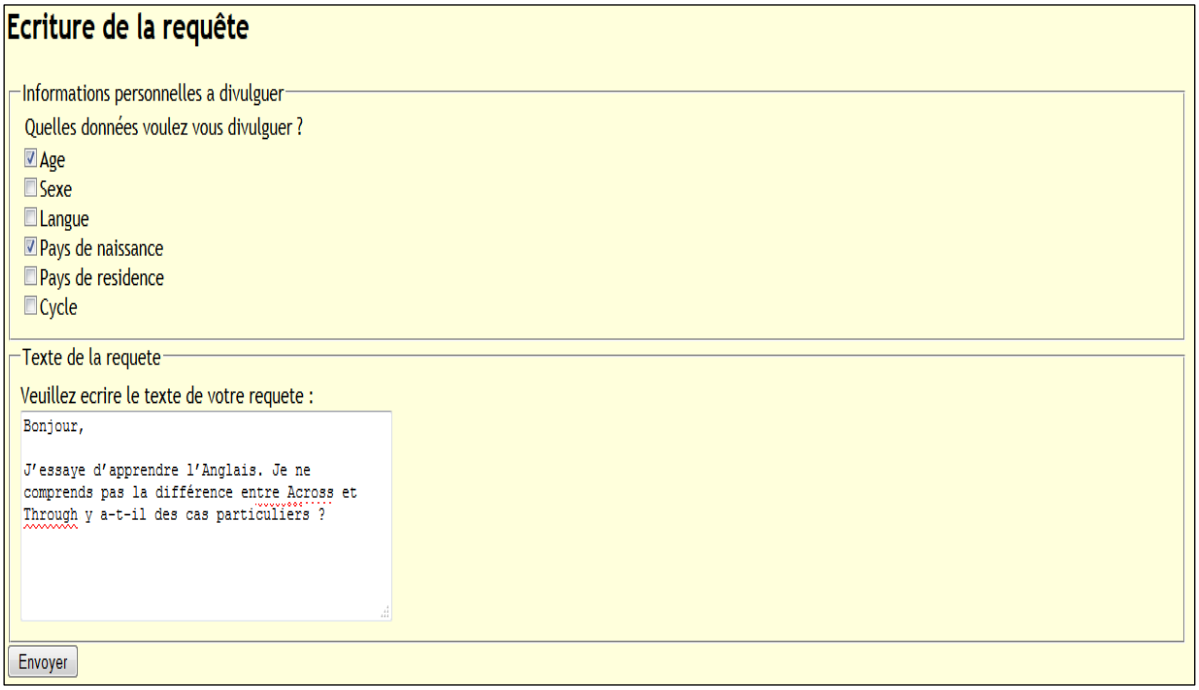


Figure 10 – Interface d'écriture d'une requête

Lorsqu'une requête est lancée, le module de sélection des pairs filtre les apprenants. La première sélection est basée sur les caractéristiques de la requête et vise à extraire des pairs qui ont posé ou répondu à des requêtes similaires. Ensuite, un filtrage collaboratif est appliqué afin d'extraire les pairs les plus appropriés pour fournir l'aide parmi ceux retenus par le premier filtrage. Enfin, les pairs sélectionnés pour fournir l'aide reçoivent une notification

pour approuver la sélection et reçoivent la requête pour y répondre, comme illustré dans la figure 11.

Figure 11 – Interface de réponse à une requête

Apres avoir implémenté notre prototype, il convient d'évaluer le bon fonctionnement du processus de sélection des pairs et s'assurer que les pairs sélectionnés sont des partenaires appropriés. Pour cela, nous avons mené une série de tests que nous présentons dans la prochaine section.

4.5. Tests et validation

De nombreuses mesures d'évaluation ont été proposées dans la littérature pour évaluer la performance des systèmes de recommandation telles que la *précision de la prédiction*, le *rappel*, la *couverture de l'algorithme*, le *temps d'exécution*, et la *vitesse de prédiction* (Shani et Gunawardana, 2011). Cependant, évaluer l'efficacité de ces systèmes est loin d'être trivial. En effet, une évaluation réelle des systèmes de recommandation est particulièrement difficile dans le domaine d'apprentissage et exige que de véritables apprenants utilisent le système pour une longue période de temps sous des conditions réelles (Erdt *et al.*, 2015). Déployer et maintenir un tel système est très coûteux car il nécessite des ressources suffisantes pour son

bon fonctionnement tel qu'une grande capacité de calcul, un soutien aux utilisateurs, etc. Pour des tests réels, il est presque impossible d'avoir de nombreuses variantes des systèmes de recommandation dans la littérature.

Pour pallier ce problème, nous avons créé un jeu de données synthétiques et l'avons utilisé pour évaluer les sélections des pairs. Le jeu de données a été construit en deux étapes. Tout d'abord, nous avons créé un ensemble de 20 apprenants. Puis, nous avons supposé que chaque apprenant a évalué 10 de ses co-apprenants en leur attribuant des notes aléatoires dans l'ensemble {1,2,3,4,5}. La figure 12 illustre l'exemple de deux apprenants a_1 et a_2 ayant évalués chacun un ensemble de co-apprenants différent.

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}	a_{20}
a_1	-	2	-	3	-	1	1	5	-	-	-	5	4	2	1	1	-	-	-	-
a_2	1	-	4	-	-	1	-	-	2	2	3	-	-	-	3	-	5	-	3	3

Figure 12 – Exemple des notes attribuées par deux apprenants initiaux

Ensuite, nous avons augmenté le jeu de données initial en ajoutant 10 apprenants supplémentaires pour chaque apprenant parmi les 20 premiers. Cela veut dire que le jeu de données résultant est composé de 220 apprenants (20 apprenants initiaux + 200 apprenants supplémentaires). Afin de créer des corrélations entre les notes attribuées par un apprenant initial et celles attribuées par les 10 apprenants supplémentaires associés, nous avons supposé que ces derniers ont évalué le même ensemble de co-apprenants en se basant sur les notes de l'apprenant initial.

Pour mieux illustrer notre propos, prenons l'exemple de la figure 13. Considérons que R est l'ensemble des notes attribuées par un apprenant a_1 (parmi les 20 initiaux) à un ensemble de 10 de ses co-apprenants. L'ensemble des notes d'un apprenant supplémentaire b_1 (parmi les 10 apprenants ajoutés à a_1) au même ensemble de co-apprenants est R + des valeurs aléatoires dans {-1, 0,1}. Ainsi, les notes de b_1 sont égales aux notes de $a_1 \pm 1$, ce qui permet de créer une corrélation entre les évaluations données par un apprenant initial et celles données par les 10 apprenants supplémentaires associés.

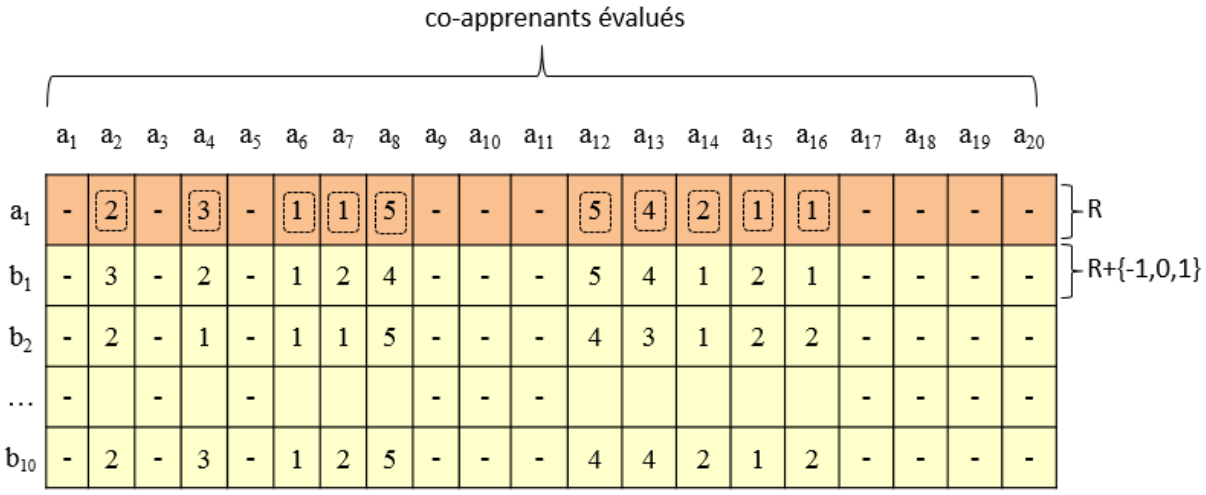


Figure 13 – Attribution des notes par les apprenants supplémentaires de a_1 (b_1,…, b_{10})

Afin d'évaluer la performance du module proposé, nous l'avons comparé à la performance de l'algorithme de filtrage collaboratif classique, noté **CF**. Nous avons également implémenté deux versions de notre module de sélection des pairs : **STV1** et **STV2**. Les deux versions sont basées sur un filtrage basé sur le contenu suivi d'un filtrage collaboratif basé sur la mémoire. La seule différence entre les deux versions est dans le fait que STV1 considère uniquement le score similarité pour générer les prédictions alors que STV2 utilise le score de similarité ainsi que le score de confiance. Cela revient à intégrer dans la version STV1 les évaluations des 20 apprenants les plus similaires, tandis que la version STV2 considère les évaluations des apprenants les plus similaires et les plus crédibles.

Pour comparer la fiabilité de ces trois approches (CF, STV1 et STV2), nous avons utilisé l'approche de validation croisée et plus spécifiquement la méthode de *leave-one-out* (Moore, 2001). Dans les faits, nous sélectionnons de façon aléatoire deux apprenants : un premier apprenant qui a demandé l'aide et un autre apprenant qui a été sélectionné pour fournir l'aide (pair sélectionné). Ensuite, nous supposons que le nouvel apprenant n'a pas encore évalué le feedback donné par le pair sélectionné, et nous tentons de prédire la note attribuée. Enfin, nous comparons les notes prédites avec les notes réelles (enregistrées dans la base de données) afin d'évaluer la précision de la prédiction.

Pour ce faire, nous utilisons la mesure statistique la plus utilisée pour l'évaluation des systèmes de recommandations qui est *l'Erreur Absolue Moyenne* (Mean Absolute Error ou MAE en anglais) (Moore, 2001). La MAE mesure la différence moyenne entre la prédiction et la valeur réelle d'une note. Elle est calculée comme suit :

$$\boldsymbol{MAE} = \frac{1}{n}\sum_{i=1}^{n} |f_i - y_i|$$

n est le nombre de prédictions, f_i est la prédiction i et y_i est la valeur réelle.

Après avoir présenté les trois versions implémentées et le jeu de données utilisé dans les tests, il est question dans la section suivante de présenter et de discuter les résultats obtenus.

4.6. Résultats

Un ensemble de test composé de 100 paires différentes de (apprenant, tuteur) a été choisi au hasard. La MAE calcule, pour chaque paire, la moyenne d'erreur absolue entre les notes prédites et les notes enregistrées dans notre ensemble de données de départ. La moyenne des MAE sur les 100 différentes itérations a été utilisée pour comparer les trois versions implémentées de FC, STV1 et STV2.

La figure 13 met en évidence le meilleur cas, le pire cas et la moyenne sur les 100 itérations : MAE minimale (MAE MIN), MAE maximale (MAE MAX) et MAE moyenne (MAE MOY) respectivement.

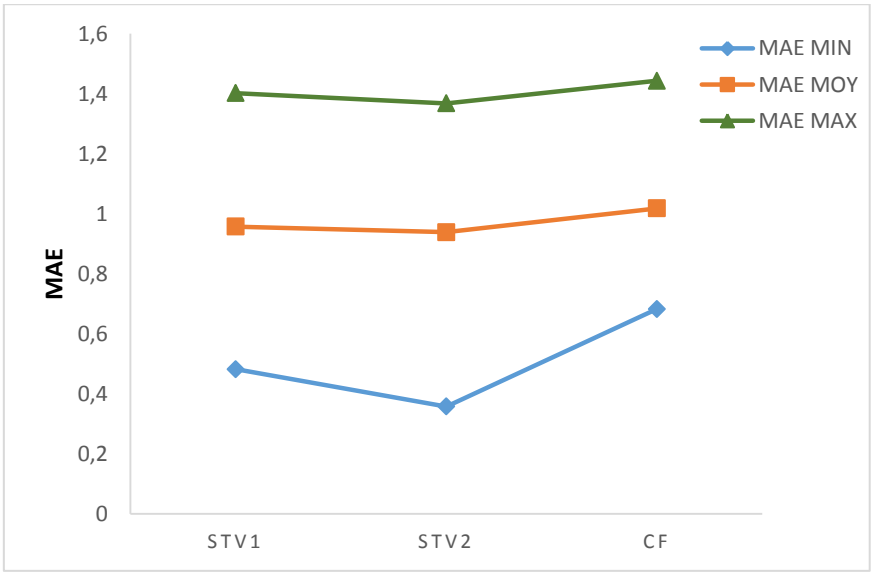


Figure 14 – Résultat de comparaison de MAE

Comme illustré dans la figure 13, l'approche la moins performante est l'approche du filtrage collaboratif classique CF. Plus précisément, l'erreur est la plus élevée dans les 3 cas (meilleur, pire et moyenne). Une explication plausible à ces valeurs élevées est due au problème de la

rareté ou du manque des données. En effet, le calcul de voisinage se fait sur la base de tous les apprenants, ce qui produit une similarité entre un apprenant et son voisinage qui n'est pas suffisamment rapprochée. Cela affecte les prédictions et engendre une différence élevée entre les notes prédites et celles enregistrées. Cela souligne le rôle du filtrage basé sur le contenu dans le module de sélection des pairs. L'impact du filtrage basé sur le contenu peut être déduit des résultats de STV1 qui implémente en cascade un filtrage basé sur le contenu suivi d'un filtrage collaboratif. STV1 produit de meilleures performances par rapport à CF parce que le premier filtrage (basé sur le contenu) réduit l'espace de calcul de voisinage, ce qui diminue le problème de la similarité non rapprochée. Néanmoins, STV2 a de meilleures performances par rapport à STV1 parce que cette dernière considère uniquement le score de similarité pour le calcul de prédictions. En revanche, STV2 intègre le score de similarité ainsi que le score de confiance. La différence entre les deux versions est que les dégâts possibles causés par des apprenants frauduleux (qui tentent de pervertir le système en assignant des notes toujours faibles pour tous les feedbacks reçus) sont limités, vu que le score de confiance est évalué avant d'intégrer les évaluations de ces apprenants. En outre, STV2 permet de sélectionner des co-apprenants n'ayant pas nécessairement une grande similarité avec l'apprenant cible mais ils sont très crédibles et leurs évaluations pourraient être très utiles.

La conclusion est que la méthode hybride STV1 cause une légère baisse de précision par rapport à STV2 mais toutes les deux sont meilleures que le filtrage collaboratif classique CF. Par ailleurs, nous pouvons constater que STV2 a une MAE MAX élevée par rapport à l'échelle de notes que nous avons utilisée. Pour mieux interpréter les valeurs de MAE et comprendre les raisons derrière l'erreur plus au moins élevée, il est important de considérer l'échelle sur laquelle les évaluations ont été effectuées et les données utilisées pour les tests. En effet, un MAE de 1 signifie que les prédictions, en moyenne, différaient par 1 de la valeur réelle. Une telle différence a plus d'impact sur une échelle de 1 à 5 qu'une différence de 1 sur une échelle de 1 à 20. Autrement dit, nous comparons la MAE, à l'échelle pour évaluer son impact réel; c'est-à-dire un MAE de 1 sur une échelle de 5 représente 20% alors que sur une échelle de 20, ne représente que 5% et par conséquent un impact plus faible sur la précision. La figure 14 illustre la MAE MOY des approches évaluées sur une échelle de 5.

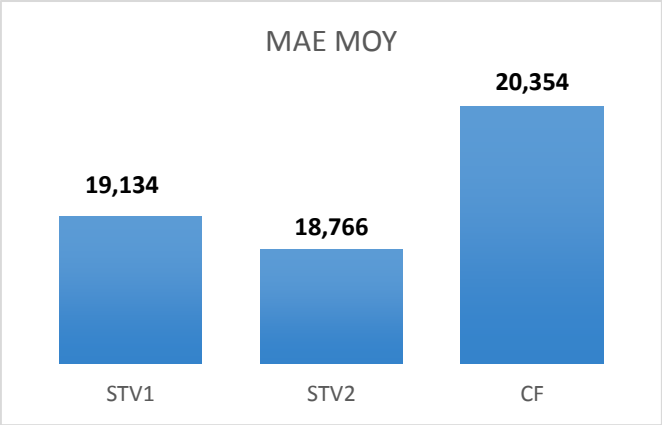


Figure 15 – Interprétation de MAE MOY

Bien que les résultats soient encourageants et la précision de STV2 est plus élevée par rapport aux deux autres approches testées, un MAE de 0,9 sur une échelle de 1 à 5 est à améliorer selon la littérature sur les systèmes de recommandation. Néanmoins, nous pensons que cette valeur de MAE est essentiellement due au fait que l'ensemble de données est généré aléatoirement. En effet, nous croyons que la valeur du MAE aurait été moins élevée si les tests avaient été faits sur un ensemble de données réelles.

4.7. Conclusion

Dans ce chapitre, nous avons présenté le premier module du notre gestionnaire de vie privée. Le module de sélection des pairs a pour rôle d'aider les apprenants à trouver des pairs tout en veillant à sélectionner les plus compétents et les plus crédibles pour fournir l'aide. L'avantage de la mise en œuvre d'un tel module dans les environnements d'apprentissage social informel est qu'il permet de réduire la charge cognitive de l'apprenant imposée par la recherche d'aide plutôt que par l'apprentissage en soi. Il permet aussi de préserver la vie privée de l'apprenant ayant besoin d'aide vu que le score de confiance des pairs est considéré dans le processus de sélection.

Selon les exigences énoncées au début du chapitre (voir section 4.3.1), le module proposé dans cette recherche offre un soutien synchrone aux apprenants tout en sélectionnant des pairs compétents et appropriés pour fournir l'aide et en équilibrant la charge cognitive entre ces derniers. Pour cela, nous avons défini un score d'aide dans la sélection permettant d'éviter que les mêmes pairs soient toujours sélectionnés pour répondre aux requêtes.

Les résultats du test sont encourageants et montrent le rôle de chaque sous-module dans la sélection. Toutefois, le processus de sélection des pairs peut être amélioré afin de diminuer

l’erreur des prédictions. En effet, le contenu de la requête (c.à.d. le texte) peut être considéré dans le filtrage basé sur le contenu pour sélectionner uniquement les pairs capables d’y répondre en utilisant une technique d’analyse sémantique telle que LSA. De plus, un filtrage collaboratif basé sur l’item peut être implémenté pour extraire, de modèle de feedback, des feedbacks enregistrés qui ont été donnés en réponse à des requêtes similaires au lieu de solliciter à chaque fois de nouveaux pairs. Cela permet de réutiliser le contenu enregistré et de fournir à l’apprenant des feedbacks qui ont été déjà évalués et donc pertinents.

Notons que sélectionner les pairs appropriés n’est que la première étape de gestionnaire de vie privée. Il convient de s’assurer, dans la deuxième étape, que l’interaction avec les pairs sélectionnés, incluant souvent une divulgation des données personnelles ne pose pas des risques en matière de vie privée. Cela fera l’objet du chapitre suivant.

Chapitre 5 : Décision de divulgation de données

La divulgation de données personnelles est associée à des bénéfices ou besoins psychologiques, sociaux et informationnels (Pérez-Ávilas *et al.*, 2011). Ainsi, un apprenant divulgue ses données dans le but de construire une identité sociale, de créer de nouvelles connexions ou d'accéder à l'aide de ses pairs.

Malgré les préoccupations en matière de vie privée, la satisfaction de ces besoins l'emporte souvent sur les risques potentiels de la divulgation de données personnelles. Kokolakis (2015) l'a expliqué par la *rationalité limitée* des utilisateurs en termes de calcul des bénéfices et risques de la divulgation ainsi que l'absence d'outils pour leur évaluation. La capacité d'**estimer automatiquement** la divulgation de données personnelles et de prendre des décisions en matière de vie privée fournit une méthode potentiellement utile pour les utilisateurs, leur permettant d'éliminer et de réduire la disparité entre les préoccupations relatives à la vie privée et les comportements d'auto-divulgation. Pour cela, nous proposons un module de prise de décision quant à la divulgation de données personnelles dans des situations d'interactions sociales entre apprenants. L'objectif de ce module est d'aider l'apprenant à protéger sa vie privée en adaptant la divulgation de ses données personnelles au contexte de ses interactions et au besoin de son apprentissage.

5.1. Divulgation de données : décision et facteurs

Plusieurs travaux se sont intéressés à étudier les facteurs expliquant le paradoxe de vie privée (Jiang *et al.,* 2012), d'autres se sont focalisés sur la proposition de solutions permettant de réduire cette disparité entre préoccupations en matière de vie privée et comportements de divulgation. Dans cette section, nous examinons certains de ces travaux en soulignant les principaux facteurs qui influencent la prise de décision de divulgation/protection de vie privée et les solutions proposées.

5.1.1. Prise de décision de divulgation/protection de vie privée

La majorité des travaux qui ont étudié la prise de décision en matière de vie privée ont trouvé dans les réseaux sociaux le milieu où le paradoxe de vie privée se manifeste le plus (Knijnenburg *et al.*, 2013). Bien que les motivations de la divulgation de données personnelles sur les réseaux sociaux et les contextes d'apprentissage social, auxquels nous

nous intéressons dans cette recherche, soient différentes, la décision de l'utilisateur et, sans doute, les facteurs qui influencent cette décision restent les mêmes : dans les deux cas, les utilisateurs tentent de trouver un compromis entre les avantages de l'interaction sociale, et les risques potentiels en matière de vie privée. En faisant ce compromis, les utilisateurs décident généralement de divulguer ou de retenir une partie de leurs renseignements personnels avec un sous-ensemble de leurs contacts (Dong *et al.*, 2015). Ce processus de décision et de compromis, est désigné par « *privacy calculus* » (Kokolakis, 2015).

5.1.2. Facteurs influençant la décision de divulgation

Plusieurs facteurs ont un grand rôle dans la décision de divulgation des données personnelles. En effet, selon Acquisti *et al.* (2015), la plupart des individus prennent souvent des décisions en se basant sur des informations incomplètes. Ils sont désorientés par les interfaces pour spécifier leurs préférences de confidentialité (Dong *et al.*, 2015) et trouvent qu'il est difficile et pénible d'ajuster ses préférences en fonction du contexte d'utilisation (Felt et Evans, 2008). À cela s'ajoutent des facteurs *psychologiques* influençant les décisions de divulgation/protection de vie privée. Nous citons principalement la *confiance dans l'autre*, la *sensibilité de l'information divulguée* et l'*objectif de sa divulgation* (Solove, 2007).

La **confiance entre les apprenants** demeure l'un des facteurs contextuels les plus importants dans la détermination de la tendance à la divulgation de données (Dong *et al.*, 2015). D'ailleurs, il a été pris en compte dans la majorité des réseaux sociaux qui ont mis en œuvre des catégories de contacts sous formes de cercles ou de groupes; par exemple famille, amis proches, amis ou connaissances sur Facebook. En ce qui concerne **la sensibilité de l'information**, Knijnenburg *et al.* (2013) ont démontré que le comportement de divulgation est *multi-dimensionnel*, ce qui veut dire que les individus ont tendances à évaluer différemment la sensibilité d'une donnée en se basant sur le contexte de la divulgation. Enfin, le troisième facteur, l'**objectif de divulgation** joue un rôle important dans la détermination de la décision de divulguer ou retenir une donnée (Nissenbaum, 2009). Ce facteur désigne la *pertinence* ou l'*utilité* de la divulgation d'une donnée ou plus, souvent liée à un scénario ou un objectif d'utilisation.

Certains de ces facteurs ont été intégrés dans les travaux proposant des solutions au paradoxe de vie privée. Afin de souligner la différence entre le module de décision de divulgation que

nous proposons dans cette recherche et ces travaux, nous présentons dans la prochaine section un bref aperçu de travaux similaires.

5.1.3. Paradoxe de vie privée : solutions

Afin de résoudre le paradoxe de vie privée, certains travaux ont proposé des solutions pour prédire et configurer la divulgation en évitant ainsi à l'utilisateur de prendre la décision. Citons, par exemple, (Dong *et al.*, 2015) et (Na, 2015) qui ont trouvé qu'il est possible de prédire le comportement des utilisateurs en se basant sur un ensemble de leurs comportements antérieurs de divulgation. De même, Fang et LeFevre (2010) ont proposé un outil capable de configurer automatiquement les paramètres de divulgation des utilisateurs en se basant sur un modèle d'apprentissage machine et en considérant uniquement des préférences de divulgation. Ces travaux avaient comme objectifs d'apprendre le comportement de divulgation de l'utilisateur afin de faciliter la prise de décision de divulgation pour celui-ci; plutôt que de prévenir les risques et protéger la vie privée.

En revanche, d'autres travaux ont proposé de résoudre le paradoxe de vie privée en quantifiant les risques de divulgation des données. Dans ce sens, Sweeney (2002) a proposé l'approche *k*-anonymat permettant d'évaluer le risque moyen de la divulgation d'une table. De même, une autre approche de quantification dite *one symbol information* a été proposée par (Bezzi, 2010) permettant de quantifier le risque individuel de la divulgation d'un enregistrement dans une table. Ces deux dernières approches ont été surtout utilisées dans un contexte de Contrôle Statistique de la Révélation (CSR) dont le but est de divulguer des données à des fins statistiques.

Dans cette recherche, nous considérons le risque comme un facteur contextuel nécessaire pour la prise de décision de divulgation mais il n'est pas l'unique facteur influençant la divulgation. Pour cela, nous proposons un module de prise de décision intégrant les facteurs évoqués ci-haut à savoir la sensibilité de l'information divulguée et son utilité. Le module proposé permet aux apprenants de contextualiser la divulgation de leurs données aux besoins de leur apprentissage. Les détails à propos de ce module seront fournis dans la prochaine section.

5.2. Module de décision de divulgation proposé

La décision de divulgation/ protection de vie privée est affectée par les principaux facteurs psychologiques, sociaux et contextuels suivants :

- le risque de la divulgation
- la confiance dans les co-apprenants
- la tendance à la divulgation
- la sensibilité des informations divulguées
- la pertinence ou l'utilité des données divulguées

Nous proposons de combiner ces facteurs dans le module *Décision de divulgation* permettant d'aider les apprenants à gérer la divulgation de leurs données personnelles et à contextualiser la protection de leur vie privée.

Une contribution de ce module est alors de *prévenir* les divulgations involontaires et les *regrets* associés en quantifiant les risques potentiels avant la divulgation même. Ainsi, un apprenant est alerté quand il est sur le point de divulguer des données qui semblent être très sensibles avec des co-apprenants ayant de faibles scores de confiance. **Une autre contribution** est d'*analyser*, *estimer* et *intégrer* les différents facteurs déterminant la décision de divulgation de données dans un environnement d'apprentissage social dans un module de prise de décision.

Dans les sections suivantes, nous analysons le rôle de chaque facteur dans la décision de divulgation/protection de vie privée. Ensuite, nous proposons des mesures pour les évaluer et les intégrer dans le module Décision de divulgation.

5.2.1. Aperçu général du module décision

La particularité des contextes d'apprentissage social est que l'interaction entre apprenants, source principale de divulgation de données personnelles, est nécessaire pour garantir leur motivation et leur engagement dans l'apprentissage. De même, la protection de la vie privée est indispensable pour instaurer un environnement favorisant la coopération et l'entraide. L'idée est alors de proposer une solution considérant à la fois les besoins de divulgation et les contraintes de protection de vie privée. Pour ce faire, nous proposons de collecter les préférences de divulgation de l'apprenant et de vérifier que la divulgation de celles-ci ne pose pas un risque sur sa vie privée. En cas de risque, des facteurs contextuels telles que la confiance dans les co-apprenants et l'utilité des données divulguées sont considérés pour prendre les meilleures décisions de divulgation.

Le module de décision, illustré dans la figure 16, comprend trois sous-modules :

- **Anonymisation** : vise à protéger l'identité de l'apprenant qui demande l'aide de ses co-apprenants en *anonymisant* ses préférences de divulgation
- **Estimation du risque** : a pour rôle d'estimer les risques potentiels de divulgation de données
- **Décision de divulgation** : considère le risque estimé afin de décider de la quantité des données à divulguer aux co-apprenants (pairs sélectionnés pour fournir l'aide).

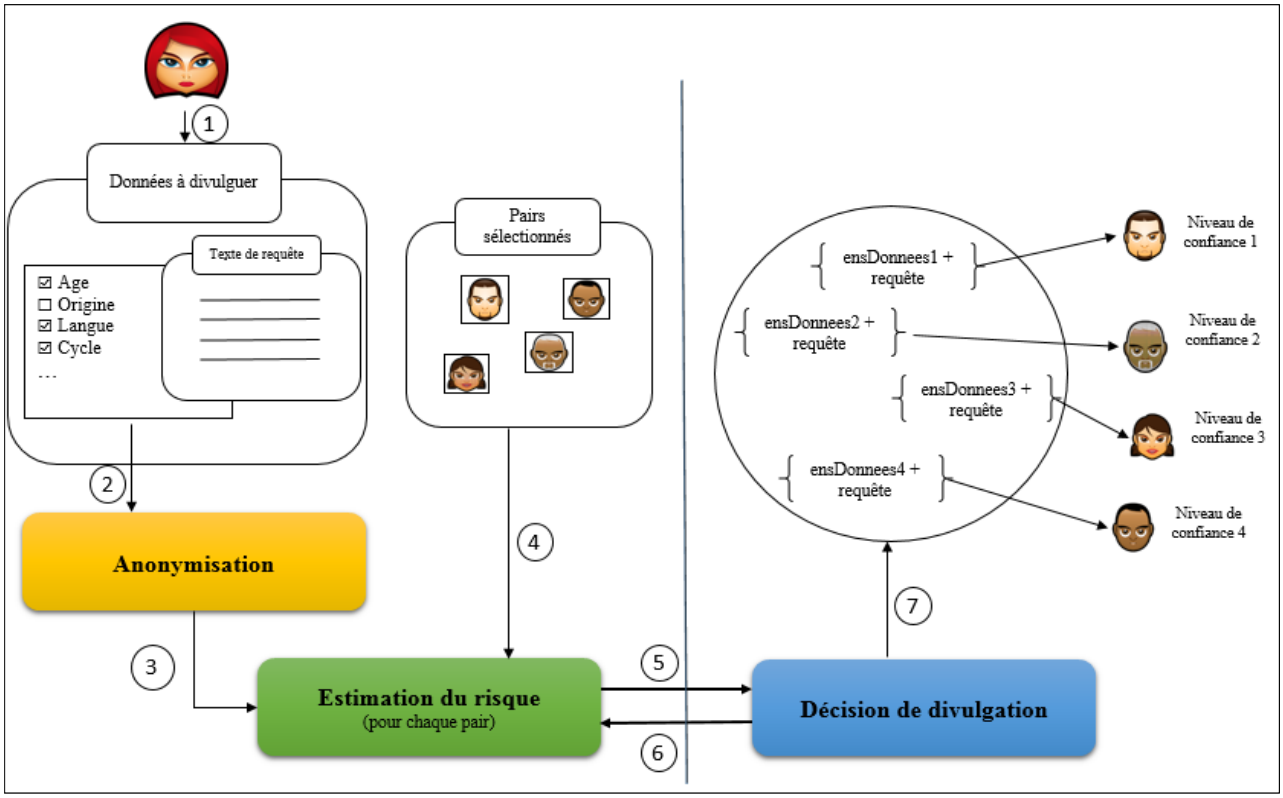


Figure 16 – Aperçu général du module décision de divulgation proposé

Nous détaillons, dans les sections suivantes, ces étapes avec les méthodes utilisées. Avant cela, il convient de définir le modèle d'attaquant afin de comprendre les risques potentiels de divulgation et de proposer une méthode appropriée pour les estimer.

5.2.2. Modèle d'attaquant

Nous nous intéressons dans cette recherche à **deux risques** en particulier dans les contextes d'interactions sociales entre apprenants : **la divulgation des attributs** (*Attribute disclosure*) et **la divulgation de l'identité** (*Identity disclosure*) (Hough, 2013). Ce dernier se produit

lorsque les informations personnelles révélées par un individu permettent à un tiers de le ré-identifier. La divulgation d'attributs peut se produire lorsque des informations confidentielles sont révélées de manière exacte ou peuvent faire l'objet d'une estimation proche de la valeur exacte. En effet, suite à une divulgation, des individus identifiés peuvent être sujets d'usurpation d'identité, de harcèlement, etc.

Pour illustrer cela, supposons que lors d'une interaction entre deux apprenants Bob et John, on a divulgué que l'âge de Bob est de 10 ans supérieur à l'âge moyen des canadiens (sans dévoiler l'âge exacte de Bob). Admettons que John ait essayé de trouver l'âge exact de Bob et ait eu accès à une base de données publique (dans ce cas-ci la source externe) révélant l'âge moyen des canadiens. Par conséquent, John pourrait inférer l'âge de Bob malgré qu'il ne l'ait pas divulgué explicitement.

Cet exemple, inspiré de la vision de (Dwork, 2006), montre que cela devient presque impossible dans le contexte actuel du monde connecté et avec la multiplication des sources d'informations en ligne de parler d'une **protection absolue**. Pour ces raisons, la plupart des travaux sur la protection de la vie privée considère une notion moins stricte et plus pratique en supposant que l'attaquant a une connaissance limitée provenant de sources externes.

Dans notre contexte d'interactions entre apprenants, le pair sélectionné pour fournir l'aide est considéré comme pouvant être *l'adversaire ou l'attaquant*. En effet, ce dernier peut essayer de ré-identifier l'apprenant ayant besoin d'aide en se basant sur ses données divulguées. Du point de vue apprentissage, plus de divulgation est utile pour fournir une aide personnalisée tandis que, du point de vue vie privée, un minimum d'informations sur l'apprenant devrait être divulgué afin de minimiser l'exposition aux risques.

Pour modéliser les connaissances externes de l'attaquant, nous considérons le pire scenario où la source de données externes dont dispose le co-apprenant coïncide avec l'ensemble de données brutes que l'apprenant a choisi de divulguer. La procédure de ré-identification consiste donc à estimer la probabilité de lier l'ensemble des données divulguées (les données observées par le co-apprenant) à l'ensemble des données originales de l'apprenant qui a fait la demande d'aide (avant leur anonymisation).

Afin de pouvoir estimer ce risque de ré-identification, nous commençons par spécifier la méthode d'anonymisation des données divulguées.

5.2.3. Anonymisation des données

C'est la **première étape** du module Décision de divulgation. Afin d'expliquer l'approche d'anonymisation utilisée dans cette étape, notons d'abord que du point de vue vie privée, les données d'un utilisateur peuvent être classifiées en 4 groupes :

- Les identificateurs explicites (*Explicit identifiers*) : regroupe les attributs permettant d'identifier directement une personne comme son nom, son numéro de téléphone, son courriel, etc.
- Les quasi-identificateurs (*Quasi-identifiers*) : regroupe les attributs permettant d'obtenir des informations précises sur une personne sans pouvoir la reconnaître directement comme âge, origine, etc.
- Les attributs sensibles (*Sensitive attributes*) : regroupe les informations sensibles sur une personne comme son état de santé, ses informations bancaires, etc.
- Les attributs non-sensibles (*Non-sensitive attributes*) : regroupe l'ensemble des autres attributs

L'anonymisation consiste à *retirer les identificateurs explicites* afin de protéger l'identité de l'apprenant en question. Toutefois, le retrait des identificateurs explicites ne peut garantir à lui seul la protection de la vie privée. En effet, la combinaison d'autres données peut permettre de ré-identifier l'individu concerné. Sweeney (2002) l'a mis en évidence en croisant une base de données médicale *pseudonymisée* et une liste électorale. Tel qu'illustré dans la figure 17, le croisement a été effectué non pas sur des champs explicitement identifiables, mais sur un ensemble de 3 attributs : *code postal*, *date de naissance* et *sexe*.

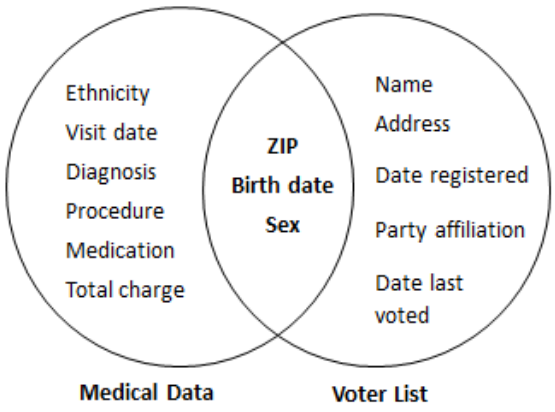


Figure 17 – Croisement de deux bases de données par Sweeney (2002)

La méthode *k*-anonymat permet de protéger contre ce type d'attaque, appelée *record linkage*. Elle tient compte d'une organisation des données en une table M composée de différents attributs classifiés selon les quatre groupes susmentionnés.

Le principe de *k*-anonymat consiste à transformer la table M de manière à ce qu'un individu ne puisse pas être distingué des autres dans un groupe d'au moins *k* personnes. On dit alors qu'une table M est *k*-anonyme par rapport à un groupe de quasi-identificateur QID si et seulement si, pour tout enregistrement *r* dans M, il existe au moins $(k - 1)$ autres enregistrements dans M qui ne peuvent être distingués de *r* par rapport à QID.

La transformation de la table originale M en une table anonyme M' est faite en appliquant une série d'opérations de généralisation et suppression (Fung *et al.*, 2010). Pour illustrer notre propos, prenons l'exemple de la table 2 non anonyme et sa version *anonymisée* par généralisation et suppression dans la table 3. Nous pouvons constater que la généralisation des valeurs numériques d'un attribut par des intervalles (p. ex., [15 − 20] pour âge) et des valeurs catégoriques par un ensemble (p. ex., {Canada, Mexique} a été remplacé par Amérique).

La table 3 est alors *2-anonyme* par rapport au QID = {Age, Origine}.

Table 2 – Exemple de table d'apprenants non anonyme

Nom	**Age**	**Origine**	**Cycle**	**Sport pratiqué**
Bob	18	Canadienne	Maitrise	Hockey
John	18	Mexicaine	Maitrise	Basketball
Alice	25	Italienne	Doctorat	Volleyball
Mark	27	Française	Doctorat	Football
Mikael	16	Brésilienne	Bac	Volleyball
Nadia	32	Marocaine	Doctorat	Soccer
Eliane	31	Gabonaise	Maitrise	Athlétisme

Table 3 – Table anonymisée par généralisation et suppression

Nom	**Age**	**Origine**	**Cycle**	**Sport pratiqué**
***	[15-20]	Amérique	Maitrise	Hockey
***			Maitrise	Basketball
***			Bac	Volleyball
***	[25-30]	Europe	Doctorat	Volleyball
***			Doctorat	Football
***	[30-35]	Afrique	Doctorat	Soccer
***			Maitrise	Athlétisme

Nous avons choisi *k*-anonymat parce que notre objectif est de protéger l'identité de l'apprenant ayant besoin d'aide. Cependant, la méthode fournit une évaluation du risque

moyen mesuré sur toute la table. Nous cherchons également à estimer le risque de divulguer un ensemble de données relatives à un seul apprenant. Cela revient à estimer le risque individuel de la divulgation. Pour ce faire, en plus de *k*-anonymat, nous utilisons la méthode d'*information spécifique* proposée par Bezzi (2010) pour estimer le risque individuel de la divulgation.

5.2.4. Estimation du risque

C'est la **deuxième étape** du module Décision de divulgation - voir figure 16. Comme la vie privée est un concept individuel, elle devrait être mesurée séparément pour chaque individu. Cela revient, dans notre contexte, à estimer le risque apporté par la divulgation de chaque donnée dans le risque total de la divulgation de l'ensemble de données à divulguer choisi par un apprenant. Pour illustrer cela, supposons qu'un apprenant ait choisi de divulguer l'ensemble de données suivant : {âge= [20-25], origine=Chine, pays actuel= Pérou}. Nous cherchons alors à estimer le risque occasionné par la divulgation de chacune de ces données par rapport au risque total de divulgation de cet ensemble.

En utilisant l'approche d'*information spécifique,* nous pouvons, d'une part, vérifier si l'ensemble de données à divulguer ne pose pas un risque, et d'autre part, estimer le risque apporté par la divulgation de chaque donnée par rapport au risque total de la divulgation d'un ensemble de données.

Avant d'expliquer comment nous l'avons adaptée et utilisée dans cette recherche, nous présentons d'abord un petit aperçu sur cette méthode, basée sur l'information mutuelle, et sa relation avec la méthode d'anonymisation *k*-anonymat utilisée pour anonymiser les données divulguées.

Information spécifique et information mutuelle

L'i*nformation mutuelle* est une fonction mathématique dont le but est de quantifier **l'information moyenne** ou le gain d'informations sur une variable aléatoire *X* en observant une autre variable aléatoire *Y*. Shannon (1948) n'a pas fourni d'indications sur la quantité d'information apportée par un seul symbole. Ainsi, afin de mesurer l'information du risque apportée par un seul symbole (une donnée dans notre cas), nous utilisons une décomposition de l'information mutuelle dite information spécifique (ou *one symbol specific information)* (Bezzi, 2013).

Pour mieux expliquer, considérons deux variables aléatoires *X* et *Y* à valeurs dans $\{x_1, x_2, \dots, x_n\}$ et $\{y_1, y_2, \dots, y_m\}$ telle que $p_i = P[X = x_i] \ \forall \ i \ \in [1, n]$, avec p_i la probabilité d'obtenir une valeur x_i et telle que $q_j = P[Y = y_j] \ \forall \ j \ \in [1, m]$, avec q_j la probabilité d'obtenir une valeur y_j.

Notons par ${p^*}_{ij}$ la probabilité conjointe entre *X* et *Y* et ${p^{**}}_{i|j}$ la probabilité conditionnelle *X* sachant *Y*. L'information mutuelle peut être décomposée pour quantifier la contribution d'une seule information dans l'information moyenne selon (Bezzi, 2010) comme suit :

$$I(X;Y) = H(X) - H(X|Y)$$

$$= H(Y) - H(Y|X)$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} {p^*}_{ij} \log\left(\frac{{p^{**}}_{i|j}}{p_i}\right)$$

Cette quantité mesure l'incertitude entre la connaissance à priori de *X*, définie par l'entropie *H(X)*, et la connaissance de *X* étant donné *Y,* notée par *H(X|Y)*. Dans un contexte de vie privée, l'entropie sert à mesurer et à estimer l'incertitude sur une variable aléatoire *X* (par exemple les valeurs spécifiques des *quasi-identificateurs* dans la table originale) en observant une autre variable aléatoire *Y* (par exemple les *quasi-identificateurs* anonymes divulgués). La mesure de l'incertitude entre les deux variables permet d'évaluer l'information apportée par les *quasi-identificateurs* anonymes par rapport aux données déjà connues par l'attaquant qui correspondent dans notre cas aux données brutes (nous modélisons le pire scénario).

Pour illustrer ce propos, reprenons les tables 2 et 3. Supposons qu'un attaquant Mark cherche à ré-identifier un apprenant ayant besoin d'aide. Mark veut s'assurer que cet apprenant est bien Bob, en se basant sur ses connaissances à propos de ce dernier : {âge=18, origine= Canada}. Supposons maintenant qu'on ait divulgué à Mark les données suivantes à propos de l'apprenant ayant besoin d'aide : {âge= [20-25], origine= Amérique}. Nous cherchons alors à estimer la différence d'incertitude entre la connaissance de Mark par rapport aux données de Bob {âge=18, origine= Canada} (dans cet exemple modélisant le pire scénario), et sa connaissance en observant l'ensemble de données divulguées à propos de l'apprenant ayant besoin d'aide {âge= [20-25], pays= Amérique}. Autrement dit, il s'agit d'estimer l'incertitude

entre le fait que les données divulguées à Mark sont celles de Bob et le fait que ces données divulguées appartiennent peut être à un autre apprenant par exemple Mikael (voir table 3).

Comme l'anonymisation peut généralement être représentée comme une fonction de X à $\widetilde{X}$, nous définissons l'ensemble de connaissances de l'attaquant $X = \{x_1, x_2 \dots, x_n\}$ et l'ensemble des données anonymes divulguées $\widetilde{X} = \{\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_m\}$.

Le gain d'informations de l'attaquant en observant les données divulguées peut donc être quantifié comme suit :

$$I(X\,;\,\widetilde{X}) = \sum_{i=1}^{n}\sum_{j=1}^{m} p(X = x_i \cap \tilde{X} = \tilde{x}_j)\, log\left(\frac{p(X = x_i \mid \tilde{X} = \tilde{x}_j)}{\sum_{j=1}^{m} p(X = x_i \cap \tilde{X} = \tilde{x}_j)}\right)$$

Nous supposons que toute observation d'une donnée ne diminue pas les connaissances que l'attaquant a sur l'apprenant. Pour estimer le risque de la divulgation des données anonymisées (en utilisant k-anonymat), il convient de trouver une relation entre k-anonymat et l'information spécifique.

***k*-anonymat et information spécifique**

Comme nous utilisons la méthode de généralisation et suppression pour l'anonymisation, nous pouvons admettre que chaque groupe $\tilde{x}$ de QID de la table anonyme correspond à un certain nombre N d'enregistrements x de X. Par conséquent, la probabilité de ré-identifier un enregistrement x étant donné $\tilde{x}$ peut s'écrire comme suit :

$$p(x|\tilde{x}) = \frac{1}{N}$$

Nous pouvons alors définir un indicateur du risque en se basant sur *k*-anonymat comme suit :

$$I(X\,;\,\widetilde{X}) \leq \log_2\left(\frac{N}{k}\right)$$

Afin d'estimer le risque de divulgation d'identité d'un apprenant, nous quantifions le risque sur l'ensemble de données à divulguer et nous le comparons à ce seuil maximal du risque, noté S_{max}, servant comme indicateur du risque. En pratique, définir des seuils (ou bornes) de risque est une méthode pour réduire le risque de ré-identification. Dans ce dernier cas, on veut, que l'estimation de la probabilité de ré-identification maximale soit bornée par S_{max}.

Reste à dire que le risque est un facteur, certes important, mais n'est pas le seul à considérer quant à la prise de décision de divulgation. Nous présentons dans la section suivante le module de décision de divulgation ainsi que les autres facteurs impliqués.

5.2.5. Décision de divulgation

C'est la **troisième étape** dans le processus de décision de protection de vie privée (figure 16). Dans cette étape, il s'agit de décider des données à divulguer aux pairs sélectionnés étant donné le risque calculé dans l'étape *Estimation du risque*.

Supposons que le risque est bien plus élevé que le seuil maximal S_{max}; quelle décision doit-on prendre ? La **première option** est de ne pas divulguer les données. Or, le but ultime des environnements d'apprentissage est de personnaliser et d'adapter l'apprentissage aux caractéristiques de l'apprenant. Dans l'absence de données à propos de l'apprenant ayant demandé l'aide, un même feedback peut être donné à tout apprenant sans aucune considération de ses caractéristiques. Pour illustrer notre propos, prenons l'exemple de deux apprenants *Eliane et Mikael* inscrits dans un environnement d'apprentissage social d'Anglais seconde langue :

Apprenant 1 : < *Eliane, 45, Gabonaise, Doctorat, Niveau 3*>

Apprenant 2 : < *Mikael, 16, Brésilienne, Secondaire, Niveau 1*>

Les deux apprenants ne partagent visiblement aucune caractéristique que ce soit sur le plan démographique (âge, genre, origine) ou le plan d'apprentissage (niveau 3 et niveau 1), en suivant la première option, aucune personnalisation ne peut être faite. Ceci étant dit, la divulgation d'informations est nécessaire dans un contexte d'apprentissage mais c'est surtout le choix de la donnée qu'il faut révéler ou cacher qui pose problème.

La **deuxième option** est alors de divulguer les données que l'apprenant a sélectionnées même si cela peut compromettre sa vie privée. Dans ce cas-là, nous ignorons un principe important dans l'apprentissage en ligne qui consiste à garantir aux apprenants d'interagir dans un environnement *préservant* la vie privée.

Une meilleure solution serait alors de pouvoir concilier les deux options en proposant une solution tenant compte de tous ces facteurs ; d'une part la *confiance* indispensable dans le contexte d'interactions entre apprenants dans un environnement social en ligne, et d'autre part

l'*utilité* des données divulguées par rapport au contexte de divulgation et besoin d'apprentissage.

Rôle de la confiance dans la décision

Rappelons que dans cette recherche nous considérons deux facettes de la confiance à savoir la personnalité et la réputation. La première permet de s'assurer que l'observateur des données a une prédisposition à agir de manière favorable (c.à.d. n'est pas abusif) alors que la deuxième consiste en la croyance que l'observateur des données a toujours agit d'une manière efficace et fiable dans le passé.

Le score de confiance T est utilisé, dans le module de Décision de divulgation, pour décider de la quantité des données à divulguer à chaque pair sélectionné dans le cas où le risque, calculé par le sous-module estimateur du risque, est situé entre un seuil minimal S_{min} et le seuil maximal S_{max} . Tel que déjà mentionné, nous proposons de considérer le seuil prédéfini par *k*-anonymat comme seuil maximal :

$$S_{max} = \log_2(\frac{N}{k})$$

avec *N* le nombre d'enregistrements dans la table et *k* la valeur d'anonymat. Nous proposons de prendre S_{min} comme l'inverse de S_{max} :

$$S_{min} = 1/\log_2(\frac{N}{k})$$

L'intérêt de définir un seuil minimal de risque est de garantir que la divulgation des données n'est faite que lorsque la probabilité de ré-identification est très faible. Ceci étant dit, nous définissons des niveaux différents de divulgation selon le risque calculé et les scores de confiance T des pairs sélectionnés. Pour distinguer ces niveaux, nous définissons un *seuil de confiance* que nous désignons par S_T permettant de contextualiser la divulgation. Etant donné que le score de confiance est dans [0,1], nous fixons le seuil S_T à 0.5.

Rôle de l'utilité de données

Dans cette recherche, nous désignons par *utilité* la pertinence des données divulguées par rapport au contexte de leur utilisation incluant les co-apprenants sélectionnés pour fournir l'aide. Dans un contexte d'entraide entre apprenants, l'utilité d'une donnée à divulguer peut être examinée selon deux points de vue : du point de vue de l'*apprentissage* et du point de vue

de la *protection de vie privée*. En effet, nous croyons que divulguer les données similaires (ou communes) entre l'apprenant ayant besoin d'aide et celui qui l'a fournie est plus **pertinent** du point de vue de l'apprentissage. En guise d'exemple, supposons qu'un apprenant, ayant pour langue= Français, ait fait une requête d'aide. Divulguer cette donnée aux pairs sélectionnés, ayant également pour langue= Français, pourrait les aider à mieux adapter les feedbacks d'aide.

Du point de vue protection de vie privée, divulguer une donnée **rare** est très utile pour fournir un feedback personnalisé, mais il peut poser un **risque** de ré-identification. Par exemple, divulguer qu'un apprenant, ayant besoin d'aide, ait pour langue=Abénaqui pourrait être risqué : d'une part, la donnée est rare et donc peut permettre de ré-identifier l'apprenant en question, et d'autre part, elle permet d'inférer l'origine *amérindienne* de l'apprenant (une donnée non divulguée).

L'idée est donc de définir deux variables pour calculer l'utilité d'une donnée. Inspiré par le travail de Hage et Aïmeur (2009), nous proposons une mesure d'utilité de données composée de deux variables :

- *la pertinence*, notée U_p : Il s'agit d'examiner les données communes entre l'apprenant qui demande l'aide et les pairs sélectionnés pour la fournir
- *la rareté* notée U_r : Il s'agit d'examiner la rareté de la donnée divulguée

Ces deux variables, déterminant l'utilité, servent à décider de la suppression des données en cas de risque de divulgation. La mesure d'utilité d'une donnée peut s'écrire alors comme suit :

$$U = \frac{U_p}{U_r}$$

Pour évaluer la pertinence d'une donnée pour l'interaction, nous calculons le nombre des pairs sélectionnés dont les *quasi-identificateurs* sont les mêmes que celui de l'apprenant demandant de l'aide.

Pour illustrer cela, considérons un apprenant Bob, ayant comme données divulguées : < *âge = [15-20] ; origine = Europe>,* a demandé l'aide de ses pairs.

Supposons maintenant qu'un ensemble de pairs ait été sélectionné pour lui fournir l'aide, tel qu'illustré dans la table 4. Pour déterminer l'utilité de deux attributs *âge* et *origine,* nous

calculons les deux variables de *pertinence* et *rareté* pour chaque attribut en se basant sur la table 4 des pairs sélectionnés.

Table 4 – Exemple de pairs sélectionnés

Id	Age	Origine	Pays actuel	Cycle
1	[15-20]	Amérique	Chine	Maitrise
2			Australie	Maitrise
3			Chine	Bac
4	[25-30]	Europe	France	Doctorat
5			Chine	Doctorat
6	[30-35]	Afrique	Canada	Doctorat
7			Brésil	Maitrise

La pertinence de deux attributs *âge* et *origine* est calculée en premier lieu ($U_{p_{age=[15-20]}} = 3$ et $U_{p_{origine=Europe}} = 2$). Ensuite, pour déterminer la deuxième variable de l'utilité, qui est la rareté nous calculons le nombre d'occurrences de chaque attribut dans toute la table. Supposons par exemple que nous avons en total dans notre table 10 apprenants dont Age = [15-20] et 20 apprenants dont Origine = 'Europe', les valeurs de rareté pour les deux attributs sont alors ($U_{r_{age=[15-20]}} = 10$ et $U_{r_{origine=Europe}} = 20$).

On obtient alors comme utilité pour les deux attributs $U_{age} = 3/10$ et $U_{origine} = 2/20$. L'attribut origine, ayant la valeur d'utilité la plus faible, est supprimé et une nouvelle itération du calcul du risque, utilité est lancée comme illustré dans l'algorithme décisionnel, détaillé dans la prochaine section.

Algorithme décisionnel

La décision de divulgation dépend du risque calculé par l'information mutuelle $I(X\ ;\ \widetilde{X})$ et de deux seuils du risque S_{min} et S_{max} alors que le niveau de divulgation dépend du score de confiance T. L'utilité intervient dans la suppression des données en cas du risque élevé. Un scénario illustrant le processus de décision de divulgation sera présenté dans la section 5.4.

La figure 18 présente un diagramme résumant l'algorithme décisionnel de la divulgation.

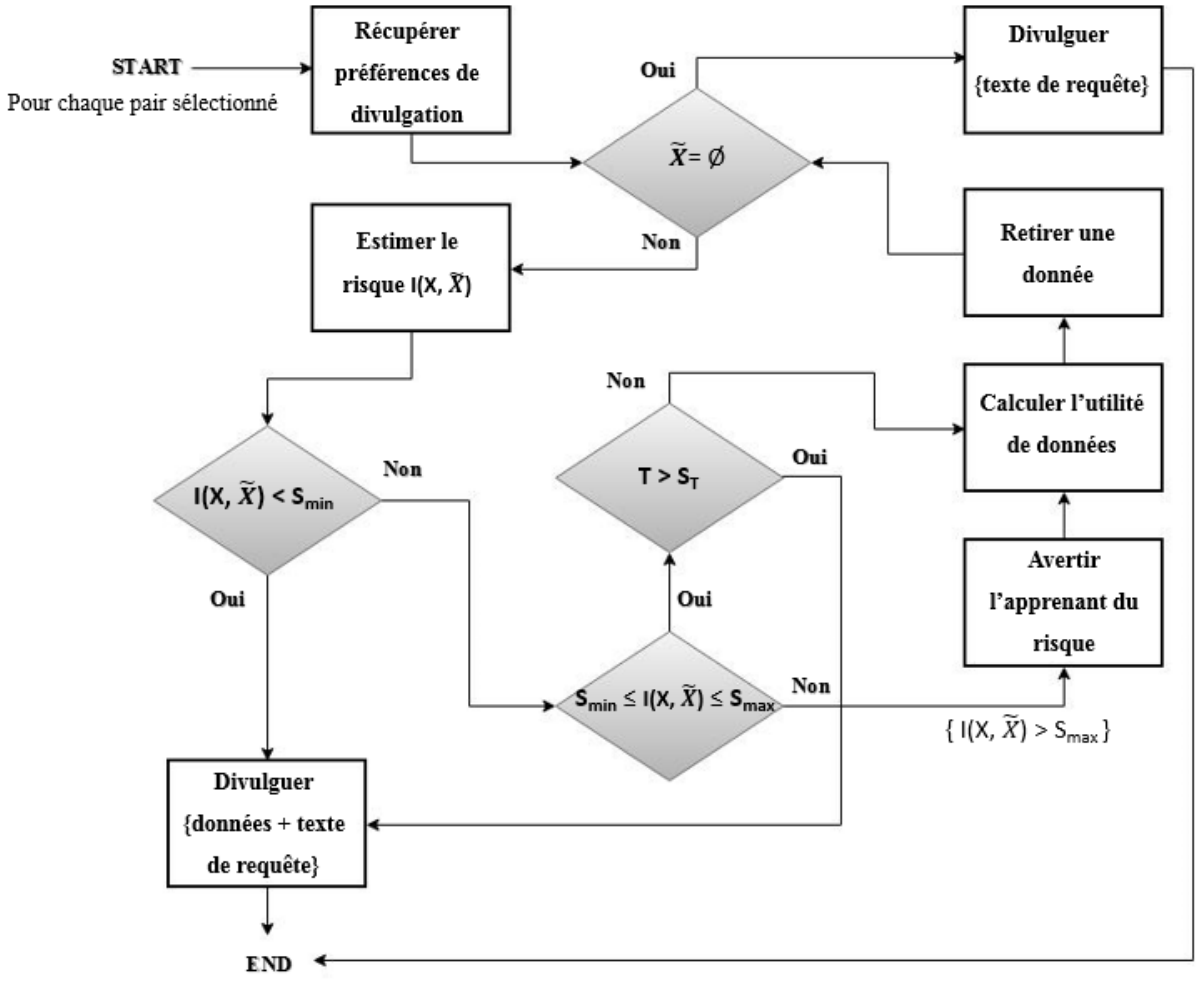


Figure 18 – Aperçu de l'algorithme du module décision de divulgation

Notons qu'une notification est envoyée à l'apprenant ayant besoin d'aide pour l'avertir en cas de risque de divulgation élevé. Cette notification sert à sensibiliser l'apprenant aux risques de divulgation de données et la nécessite de protéger sa vie privée.

Le module décision de divulgation garantit qu'en cas d'absence du risque un maximum de données est révélé aux pairs sélectionnés afin de fournir une aide personnalisée et adaptée aux caractéristiques de l'apprenant qui l'a demandée. En revanche, en cas de risque, moins de données sont divulguées et d'autres facteurs sont examinés pour éviter d'exposer l'apprenant à des risques potentiels entrainés par une divulgation excessive ou une interaction risquée (avec des pairs abusifs).

5.3. Implémentation et prototype

L'objectif de ce travail est de fournir un outil de décision de divulgation permettant aux apprenants, dans un contexte d'apprentissage social en ligne, de divulguer des données personnelles, sans s'exposer aux risques en matière de vie privée. Comme les apprenants n'ont pas les informations nécessaires à propos des pairs sélectionnés et de la sensibilité des données pour pouvoir calculer ces risques, nous leur demandons uniquement de choisir l'ensemble de données à divulguer correspondant aux préférences de divulgation. Pour cela, nous proposons une interface simple leur permettant d'écrire le texte de la requête d'aide et de sélectionner l'ensemble d'attributs à divulguer, tel qu'illustré dans la figure 19.

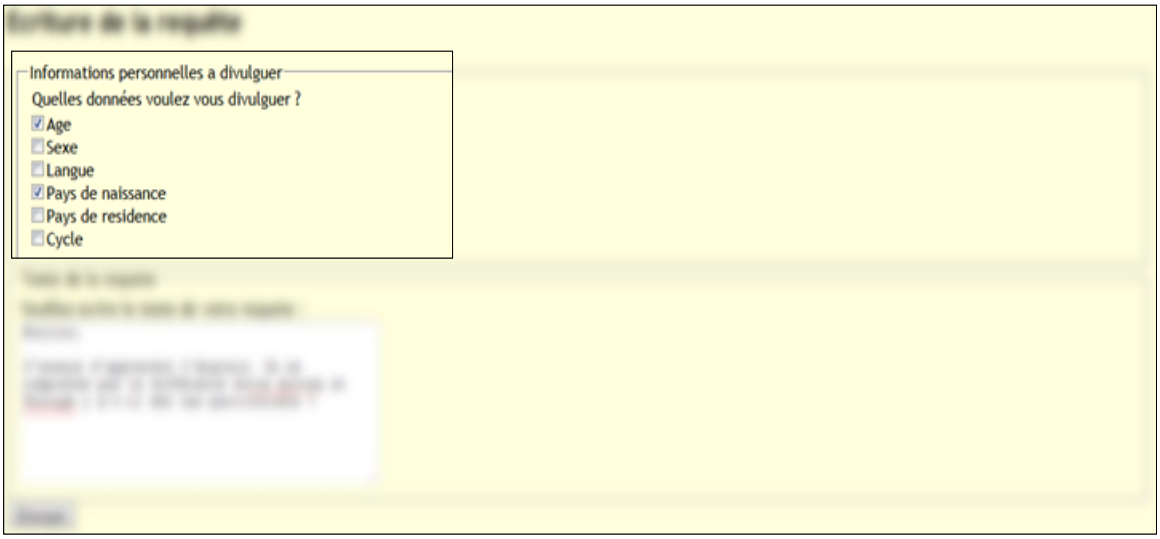


Figure 19 – Préférences de divulgation

Une fois l'ensemble des pairs qui vont fournir l'aide sélectionné, la décision de divulgation est prise tel qu'expliqué dans la section précédente.

Si le risque dépasse la valeur du seuil maximal, une notification est envoyée à l'apprenant pour l'informer de la présence d'un risque élevé.

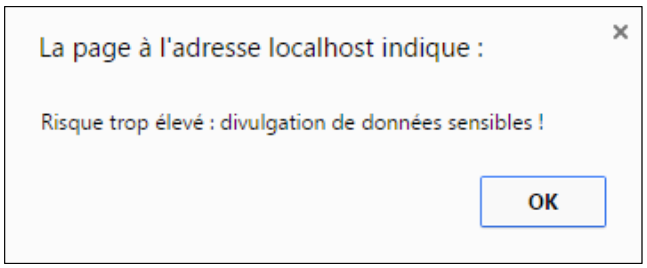


Figure 20 – Notification du risque élevé

Avant de divulguer les données aux pairs, il faut les anonymiser. Pour ce faire, nous utilisons et adaptons l'algorithme *Datafly* de l'outil d'anonymisation de l'UT Dallas[5]. Cet algorithme est de nature heuristique, il ne considère qu'un petit ensemble des données pour trouver une solution d'anonymisation. Ainsi, du point de vue temps, il est très efficace (d'où le nom Datafly). La figure 21 présente le pseudocode de l'algorithme Datafly.

1. *Soit une table T = PT [QID] (prend en considération que les attributs quasi-identificateurs)*

2. *Tant que k-anonymat n'est pas atteint et le nombre des lignes restantes non conformes à k-anonymat est plus grand que k :*

> ***a.*** *Obtenez le nombre de valeurs distinctes de chaque attribut dans T*
>
> ***b.*** *Généraliser l'attribut avec les valeurs les plus distinctes*

Figure 21 – Pseudocode de Datafly (Sweeney, 1998)

Nous utilisons une méthode de généralisation dite *Domain Generalization Hierarchy* (Campan *et al.*, 2011), notée DGH (attribut), pour généraliser les quasi-identificateurs dans notre travail. Cela est fait en créant des classes de fréquence similaire, et des niveaux plus élevés (niveaux plus généraux) de la hiérarchie. En faisant cela, les valeurs deviennent de plus en plus générales dans chaque itération.

[5] http://www.cs.utdallas.edu/dspl/cgi-bin/toolbox/

S'il y a un problème qui revient souvent dans le cas de *k*-anonymat, c'est la sélection d'une valeur *k* initiale. Le choix de cette valeur est crucial, et dépend profondément du domaine et des données en question. Nous croyons, cependant, qu'avec de plus grandes valeurs de *k* plus d'attributs sont choisis pour être anonymisés, et donc, la précision globale du modèle diminue. Nous avons fait plusieurs tests sur des ensembles de données avec moins d'attributs et des fonctions DGH (attribut) plus spécifiques sur les quasi-identificateurs pour pouvoir sélectionner une valeur initiale de *k* pour le jeu de données utilisé dans cette recherche.

5.4. Tests et validation

Pour tester le bon fonctionnement de notre module de décision, nous avons utilisé un jeu de données que nous avons produit à l'aide d'un générateur de données, plus précisément *Fake Name Genenerator*[6]. Ce jeu de données contient 5000 enregistrements correspondants aux profils d'apprenants (c.à.d. 5000 apprenants) avec 10 différents attributs : 5 attributs générés par *Fake Name Genenerator* (nom, âge, origine, adresse, genre) et 5 attributs que nous avons ajoutés pour les besoins de tests (langue, cycle, cours, niveau cours, score confiance). Le jeu de données résultant a été utilisé pour tester l'anonymisation, l'estimation du risque et la décision de divulgation.

Nous avons lancé une série de tests sur le jeu de données en simulant des scénarios d'exécution. Pour cela, nous avons créé un ensemble de requêtes d'apprenants avec différentes préférences de divulgation pour pouvoir calculer à chaque fois le risque de ré-identification et définir les niveaux de divulgation selon les scores de confiance des pairs sélectionnés. Nous avons évalué notre module de décision avec l'ensemble suivant des attributs de l'apprenant :

< âge, origine, pays actuel, genre, langue, cycle, niveau cours >

Afin de garder un certain niveau d'utilité des données, nous avons considéré les attributs *<âge, origine>* pour composer les quasi-identificateurs, avec une valeur initiale d'anonymisation *k=10* et un seuil de confiance S_T= 0.5.

Pour illustrer notre propos, prenons un exemple d'un apprenant ayant besoin d'aide dans un cours d'anglais. Afin d'avoir des feedbacks de la part de ses pairs, il a formulé la requête

[6] www.fakenamegenerator.com/

suivante : « *I'm not speaks much English and feel frustrated, if help me please for learn thanks and what's your advice for my thanksssss ».*

L'apprenant a choisi de divulguer un ensemble de ses données pour avoir des feedbacks personnalisés, tel qu'illustré par la table 5.

Table 5 – Scénario d'exécution et données à divulguer

Attributs	**Age**	**Origine**	**Langue**	**Cycle**
Données brutes	35	Tunisie	Français	Maitrise
Données anonymisées	[32-36]	Afrique	Français	Maitrise

Pour simuler le fonctionnement de module de décision, nous avons mis en place une procédure permettant de sélectionner un nombre aléatoire de pairs pour répondre à la requête. Nous avons également extrait les scores de confiance T des pairs sélectionnés ainsi que leurs âges et origines anonymes. Pour ce scénario d'exécution, quatre pairs ont été sélectionnés tel que le montre la table 6.

Table 6 – Scénario d'exécution et pairs sélectionnés

	Score de confiance (T)	**Age anonyme**	**Origine anonyme**
Pair n°1	0.4	[17-21]	Amérique
Pair n°2	0.8	[42-46]	Asie
Pair n°3	0.2	[27-31]	Amérique
Pair n°4	0.3	[17-21]	Afrique

La première étape dans le processus de décision de divulgation est d'anonymiser les données de l'apprenant (voir table 5) afin de calculer le risque de ré-identification $I(X\ ;\ \widetilde{X})$. Le calcul de I est basé sur les probabilités des données et ne concerne que les quasi-identificateurs (âge et origine dans ce scénario). La décision de divulgation se fait en premier lieu en comparant le risque calculé I aux seuils prédéfinis S_{min} et S_{max} de valeurs respectives 0.11 et 8.96.

La première itération du calcul peut être résumée dans la table 7.

Table 7 – Scénario d'exécution et première itération du calcul

Itération	$\widetilde{X}$	I(X, $\widetilde{X}$)	Interprétation	Décision de divulgation
1	{âge, origine}	2.1	$S_{min} < I < S_{max}$	➔vérifier niveau de confiance T des pairs ➔calculer utilité âge et origine ➔2ème itération du calcul

Pour la première itération, le risque calculé est entre les deux seuils, ce qui implique que le score de confiance des pairs doit être considéré pour décider de la quantité de données à divulguer à chacun. Les pairs ayant un score de confiance $T > S_T$ reçoivent les données anonymisées de l'apprenant ainsi que le texte de la requête, tel qu'illustré par la table 9.

Pour les pairs ayant un score de confiance $T < S_T$, une deuxième itération du calcul est nécessaire pour réduire le nombre de données à divulguer. Pour cela, un calcul d'utilité doit être effectué afin de déterminer la donnée à supprimer soit âge soit origine. Pour calculer l'utilité de l'attribut âge, nous considérons le nombre de pairs sélectionnés ayant le même âge que l'apprenant ayant besoin d'aide ($U_{p_{age=[32-36]}} = 0$, voir table 6) et le nombre d'apprenants dont l'âge dans [32-36] dans le jeu de données ($U_{r_{age=[32-36]}} = 10$). Ainsi, l'utilité de l'attribut âge est $U_{age} = 0/10=0$.

De même, pour calculer l'utilité de l'attribut origine, nous considérons le nombre de pairs sélectionnés dont origine= Afrique ($U_{p_{origine=Afrique}} = 1$, voir table 6) ainsi que le nombre d'apprenants, dans le jeu de données, ayant comme origine= Afrique ($U_{r_{origine=Afrique}} = 200$). Ainsi, l'utilité de l'attribut origine est : $U_{origine} = 1/200=0.005$.

L'attribut âge, ayant la plus faible utilité, est alors supprimé. Notons que pour des raisons de simplification, nous avons considéré un nombre réduit des pairs sélectionnés dans ce scénario.

Si le risque est toujours supérieur au risque minimum tolérable S_{min} pour les pairs dont le score de confiance est inférieur à S_T, une nouvelle itération d'évaluation d'utilité, suppression de données et évaluation du risque est lancée jusqu'à avoir un risque minimum, tel qu'illustré par la table 8.

Table 8 – Scénario d'exécution et itérations du calcul

Itération	Pairs	$\widetilde{X}$	I(X, $\widetilde{X}$)	Interprétation	Décision de divulgation
2	$T > S_T$	{âge, origine}	2.1	$S_{min} < I < S_{max}$	➔divulguer {données+ texte de requête}
	$T < S_T$	{origine}	1.15		➔supprimer origine ➔$3^{ème}$ itération du calcul
3	$T > S_T$	{âge, origine}	2.1	$S_{min} < I < S_{max}$	➔divulguer {données+ texte de requête}
	$T < S_T$	Ø	0	$I < S_{min}$	➔ne pas divulguer {âge, origine}

La sortie de l'exécution du scénario, présentée dans la table 9, permet de distinguer deux niveaux de divulgation de données aux pairs sélectionnés définis par le module décision de divulgation.

Table 9 – Scénario d'exécution et décision de divulgation

Pairs	Score de confiance	Décision divulgation
$T<S_T$		
Pair n°1	0.4	{Langue= Français, Cycle= Maitrise} + Texte de requête= « *I'm not… thankssssss »*
Pair n°3	0.2	
Pair n°4	0.3	
$T>S_T$		
Pair n°2	0.8	{Age= [32-36], Origine= Afrique, Langue= Français, Cycle= Maitrise} + Texte de requête= *« I'm not… thankssssss »*

Pour valider le module de décision proposé dans cette recherche, nous l'avons comparé aux travaux similaires dans la littérature qui ont proposé des solutions au problème de décision de divulgation dans différents contextes, et en particulier dans les réseaux sociaux. Dans cette comparaison, illustrée dans la table 10, nous avons considéré les facteurs pris en compte dans les solutions proposées ainsi que les méthodes utilisées.

Table 10 – Comparaison avec des travaux similaires

Travaux	Facteurs sociaux	Facteurs contextuels	Protection de risques	Méthodes utilisées
Assistant de vie privée (Fang et LeFevre, 2010)	comportement de divulgation	destinataires	aucune	algorithms d'apprentissage machine
Private Personal Learning (Na, 2015)	influence sociale	destinataires	aucune	gestion d'identité et d'accès
Prédiction de comportement de divulgation (Dong *et al.*, 2015)	- tendance de divulgation - confiance	destinataires	recommandation de protection	algorithmes d'apprentissage machine
Notre Module	- préférences de divulgation - confiance	destinataires et utilité de données	anonymisation et estimation	*k*-anonymity et information spécifique

Bien que certains des travaux illustrés dans la table ci-dessus considèrent différents facteurs, ils ne quantifient pas les risques potentiels de divulgation de données. En effet, ils visent à faciliter la décision de divulgation pour l'utilisateur plutôt qu'à le protéger des risques potentiels. C'est cela qui distingue le module décision de divulgation que nous proposons dans cette recherche des travaux similaires.

5.5. Conclusion

Dans ce chapitre, nous avons proposé un module de décision de divulgation de données personnelles dans un contexte d'apprentissage social informel. L'objectif de ce module est de trouver un compromis entre la divulgation de données, nécessaire pour améliorer l'interaction entre apprenants, et la protection de leur vie privée. Pour ce faire, nous avons étendu une approche de quantification des données anonymes et défini un module de décision intégrant différents facteurs dont la confiance des co-apprenants et l'utilité des données. L'avantage du module proposé réside dans le fait de mettre en œuvre une nouvelle conceptualisation de la vie privée en tant que processus de négociation considérant à la fois les préférences de divulgation de l'apprenant et les exigences de protection de leur vie privée. Cependant, même si des facteurs sociaux incluant les co-apprenants, formant la communauté dans laquelle

l’apprenant évolue et interagit, sont considérés dans ce module, la décision de la divulgation reste individuelle. Cette vision de décision suppose que les décisions individuelles et optimales de protection de vie privée aboutissent à des résultats de protection qui sont socialement optimaux pour la communauté ; ce qui n’est pas toujours le cas, et encore moins dans un contexte d’apprentissage, où il convient d’inclure les co-apprenants dans la décision pour mettre en œuvre un vrai processus de négociation de vie privée.

Chapitre 6 : Analyse d'interactions entre apprenants

Une fois que l'on a mis en place les modules de sélection des pairs et de décision de divulgation, la dernière étape de *gestionnaire de vie privée* est d'analyser les feedbacks fournis par les pairs avant de les envoyer à l'apprenant ayant besoin d'aide. L'analyse des feedbacks vise à aider l'apprenant à repérer les feedbacks pertinents parmi tous les feedbacks fournis par les pairs sélectionnés. Cela revient à écarter les feedbacks pouvant affecter négativement l'état émotionnel de l'apprenant en question et à supprimer toute divulgation des données faites par les pairs dans les feedbacks fournis. L'analyse des feedbacks est effectuée par le module **Composition des feedbacks** (Voir figure 5) que nous détaillons dans les sections suivantes. Mais avant cela, nous commençons par souligner les facteurs à considérer dans cette analyse et nous présentons un aperçu des travaux portant sur l'analyse des interactions entre apprenants.

6.1. Analyse d'interactions entre apprenants

D'une manière générale, l'interaction dans un contexte d'apprentissage formel diffère de celle dans un contexte informel par plusieurs éléments. En effet, la principale motivation de joindre un environnement d'apprentissage informel selon les apprenants est la recherche de la valeur sociale et la satisfaction des *besoins socio-émotionnels* (De Wever *et al.*, 2010), alors que l'acquisition de nouvelles connaissances est la principale motivation dans l'apprentissage formel. Ceci étant dit, analyser les interactions entre apprenants dans les contextes formels vise à trouver des indicateurs de l'apprentissage réalisé en se basant sur un ensemble de critères tels que les *arguments* et les contre arguments construits par les apprenants dans les interactions (Weinberger et Fischer, 2006).

Par ailleurs, des études de Lin *et al.* (2013) et kasdali (2014) ont démontré la marginalité de la dimension cognitive et la prédominance de la dimension **sociale et affective** dans les contextes informels. Les auteurs ont suggéré de considérer des indicateurs socio-émotionnels tels que le *partage d'émotions* et l'*empathie* entre apprenants afin d'évaluer l'apprentissage réalisé dans ces contextes. Ceci étant dit analyser les interactions dans les contextes informels revient à trouver des indicateurs socio-émotionnels témoignant les *émotions*, l'*attitude* et la *perception* des apprenant vis-à-vis un cours ou un matériel didactique. Dans ce sens, Ortigosa

et al. (2014) ont analysé des interactions dans le but de déduire les sentiments d'un apprenant et lui recommander des activités d'apprentissage adéquates en se basant sur des indices socio-émotionnels et en utilisant des techniques d'analyse des sentiments.

D'autres chercheurs se sont focalisés à l'étude de l'impact de l'interaction sur l'apprentissage en examinant les indices socio-émotionnels dans les interactions entre apprenants. Dans cette optique, une étude de Mangenot et Nissen (2013) a montré que les apprenants ayant bénéficié des feedbacks affectifs positifs lors de leurs interactions avec des pairs ont plus progressé que les autres dans leur apprentissage. En effet, de point de vue socio-émotionnel, un feedback est considéré *positif* s'il provoque des *sentiments positifs* et stimule l'*intérêt* de l'apprenant, sa *motivation* et son *auto-efficacité*, même quand ce feedback n'est pas orienté sur la tâche d'apprentissage (Kulkarni *et al.*, 2015). En revanche, un feedback est désigné comme étant *négatif* s'il inclut un message *décourageant*, *démotivant*, *ridiculisant* l'apprenant ou le *harcelant* psychologiquement lors de son interaction avec ses pairs. Ce type de feedback est vu comme une *forme de punition* auprès des apprenants décourageant ces derniers de demander l'aide et de poursuivre leurs objectifs d'apprentissage (Kulkarni *et al.*, 2015).

La perception du feedback, un élément nécessaire de l'analyse des interactions, est étroitement liée aux émotions : les émotions qui ont initié le besoin d'aide et celles qui en résultent. En effet, des états émotionnels et psychologiques tels que la motivation et l'engagement ont un rôle fondamental non seulement dans les interactions mais aussi l'apprentissage surtout que l'impact des émotions sur l'apprentissage n'est plus à démontrer (Lipman, 2003).

6.1.1. Rôle des émotions dans l'interaction

L'effet de l'émotion sur l'interaction a été étudié sous différentes perspectives. En effet, des chercheurs voient que la relation entre ces deux facteurs est bidirectionnelle, ce qui veut dire que les émotions suscitent le besoin de l'interaction et cette dernière peut affecter positivement ou négativement les émotions d'un apprenant (Nummenmaa *et al.*, 2012). Les auteurs ont attiré l'attention sur le fait que des états émotionnels et psychologiques tels que l'*incertitude*, la *confusion*, l'*anxiété* jouent un rôle important dans le processus de recherche et de demande d'aide entre apprenants, et que les émotions doivent être considérées comme nécessaires pour l'apprentissage dans ces contextes.

Précisons ici que nous nous intéressons dans cette recherche à l'effet de l'interaction sur l'apprenant qui a demandé l'aide et non pas sur celui qui l'a fournie. Dans cette optique, O'Regan (2003) a suggéré de considérer des émotions négatives et positives des étudiants en ligne tels que la *frustration* ou l'*anxiété* face au regard des pairs inconnus ou face aux feedback des autres, l'*embarras* ou la *honte* liés aux interactions, la *fierté* ou la *joie* résultante de la réussite d'une tâche ou de la réception d'un feedback positif d'un pair.

En outre, Hage et Aïmeur (2009) voient qu'examiner l'effet de l'émotion dans l'apprentissage est intéressant mais instaurer un environnement préservant la vie privée est indispensable. Dans ce qui suit, nous verrons le rôle de la protection de la vie privée dans les interactions sociales entre apprenants.

6.1.2. Rôle de la protection de la vie privée dans l'interaction

Les apprenants inscrits dans les environnements et les communautés virtuelles d'apprentissage ont souvent mentionné ne pas se sentir en sécurité pour pourvoir demander de l'aide de leurs pairs (Amichai-Hamburger, 2012). En effet, il semble que beaucoup d'apprenants trouvent que l'accès non contrôlé et les messages persistants sont un obstacle à leur vie privée et leur sécurité et donc les freine de participer aux interactions en ligne même quand ils en ont besoin. Dans ce contexte, Malinen et Nurkka (2015) soulignent que la vie privée et la sécurité ne sont pas souvent garanties dans les interactions sociales en ligne. Bien que ces deux notions soient liées, elles ne sont pas identiques. La sécurité (*safety*) se réfère à la protection physique et psychologique des utilisateurs alors que la vie privée désigne davantage la protection des données personnelles (Amichai-Hamburger, 2012).

Bien que la plupart des interactions dans les situations d'apprentissage soient positives, force est de constater la prévalence des feedbacks négatifs visant à *ridiculiser*, *embarrasser* ou *harceler* l'autre. Ainsi, les apprenants peuvent être mal à l'aise avec les feedbacks négatifs et le ton et l'hostilité de leurs pairs et se sentent plus à l'aise quand ils peuvent rester anonymes car ils ne se sentent pas être personnellement visés par les commentaires des autres (Malinen et Nurkka, 2015). Pour cela, afin de protéger les apprenants, toute *divulgation non intentionnelle* ou *non contrôlée* doit être détectée et supprimée afin d'éviter qu'un pair *mal intentionné* ou *abusif* puisse acquérir des connaissances sur l'identité des apprenants en se basant sur certaines *informations divulguées* dans leurs interactions.

6.2. Module d'analyse d'interactions proposé

L'objectif du module *Composition des feedbacks* est de minimiser les interactions négatives, induisant des émotions négatives chez l'apprenant, dans le but d'instaurer un environnement favorisant la coopération entre apprenants, ce qui garde l'apprenant motivé et engagé dans son apprentissage. Il vise aussi à supprimer toute divulgation des données personnelles dans les feedbacks fournis par les pairs afin de préserver leur vie privée.

Pour ce faire, nous proposons une analyse d'interactions en deux étapes : la **fouille** (ou *mining* en anglais) et la **composition** comme illustré dans la figure 22. La première étape a pour rôle de supprimer les *feedbacks négatifs* envoyés par certains pairs. Tandis que la deuxième étape de l'analyse *détecte et supprime les feedbacks divulguant des données personnelles* afin de protéger la vie privée des apprenants impliqués dans l'interaction. Malgré que la suppression des feedbacks divulguant des données personnelles ne soit pas demandée par l'apprenant qui a révélé ses données, par **indifférence** ou par **ignorance**, minimiser les risques et préserver la vie privée est nécessaire pour garantir un environnement interactionnel favorisant l'entraide et la coopération.

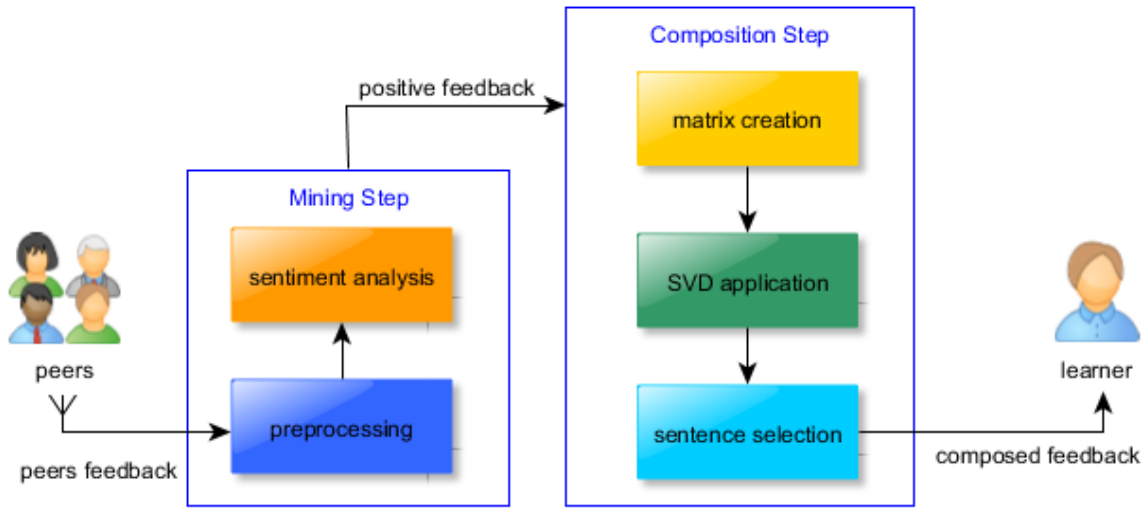


Figure 22 – Architecture du module composition des feedbacks

Les deux étapes de l'analyse des interactions sont détaillées dans les sections suivantes.

6.2.1. Étape de fouille

L'objectif de cette étape est de supprimer les feedbacks négatifs donnés par les pairs qui peuvent affecter négativement l'apprenant ayant besoin d'aide et gêner son apprentissage.

Pour ce faire, nous proposons de classifier ces feedbacks : *positifs* à envoyer à l'apprenant ayant besoin d'aide et *négatifs* à supprimer.

Avant la classification, il convient de faire des prétraitements (*preprocessing*) sur les feedbacks fournis par les pairs - voir figure 22. Ces prétraitements consistent à extraire de chaque feedback toutes les unités linguistiques correspondantes aux mots lemmatisés. La *lemmatisation* consiste à regrouper les différentes formes que peut revêtir un terme : le nom, le pluriel, le verbe à l'infinitif, etc. En plus, certains types grammaticaux sont éliminés tels que les déterminants et la ponctuation vu qu'ils sont assez fréquents et n'ont pas d'impact sur la classification. Par exemple, la présence d'un point d'interrogation ou d'un point d'exclamation ne rajoute aucune information à propos d'un feedback s'il est négatif ou positif.

En guise d'exemple, prenons le feedback suivant : « *I am a begginer; but I want to speak English faster and I need and I want to practice... but let me learn more English vocabulary before practicing with u* ».

Les prétraitements appliqués sur ce feedback suppriment les mots creux, c.-à-d. les pronoms, les déterminants, les adverbes, etc., et convertissent les termes «*practice*» *et* «*practicing*» à un seul terme «*practic*» avec un nombre d'occurrences égal à 2. Le résultat de prétraitements de ce feedback est un vecteur d'unités linguistiques avec le nombre d'occurrences de chaque unité comme suit :

[*Beginner, want (2), speak, English (2), need, practic (2), let, learn, vocabulary*]

Pour classifier les feedbacks, nous effectuons une **analyse des sentiments** (ou *sentiment analysis* en anglais) à tous les feedbacks donnés par les pairs sélectionnés en réponse à une requête d'aide. L'analyse des sentiments se concentre sur l'attribution d'une polarité à des opinions, sentiments et attitudes présente dans un texte ou un ensemble de texte (Pang *et al.*, 2002). Pour ce faire, nous utilisons des techniques d'apprentissage machine dédiées à l'analyse de sentiment parce qu'elles sont indépendantes de la langue et peuvent être étendues pour tenir compte du contexte des termes. Afin de classifier les feedbacks correctement, la machine est entraînée à détecter des modèles représentant des termes à valeur positive ou négative en la faisant travailler sur un premier corpus de test. Elle doit être capable de détecter ensuite ces modèles dans le corpus lui-même, voire d'en détecter de nouveaux, proches de ceux qu'elle connaît déjà. Des algorithmes comme le *classifieur de Bayes*, *k-plus proches*

voisins (k-NN), les *arbres de décision* (par exemple C4.5), les *règles d'association* pourraient être appliqués dans notre travail.

Comme nous nous intéressons à la facette socio-émotionnelle de l'interaction, nous supposons que **l'état émotionnel** de l'apprenant ayant besoin d'aide affecte grandement la perception des feedbacks reçus. En effet, un feedback peut être perçu comme positif ou négatif dépendamment de l'apprenant mais aussi des émotions qu'il éprouve au moment de la réception de ce feedback. Pour illustrer notre propos, prenons l'exemple du feedback suivant donné par un pair en réponse à une requête d'aide : « *No pain... no gain* ». Étant *démotivé*, *frustré*, *heureux*, ou *neutre*, un apprenant interprètera ce feedback différemment.
Ainsi, la considération de cet aspect contextuel est indispensable vu qu'il permet d**'adapter** l'interaction aux émotions de l'apprenant. Pour reconnaitre et détecter les émotions de l'apprenant, nous lui demandons de spécifier son état émotionnel au moment de l'écriture de sa requête d'aide. Comme le soutien entre apprenants dans cette recherche est *synchrone*, nous présumons que l'état émotionnel de l'apprenant au moment de la réception du feedback est le même que lorsqu'il a fait la requête d'aide. Nous nous focalisons dans cette recherche particulièrement sur les *émotions négatives* reliées à l'apprentissage tel que la *frustration*, l'*anxiété*, l'*ennui*, la *démotivation*, etc.
Ceci étant dit, pour classifier un feedback comme négatif ou positif les algorithmes d'apprentissage machine tiennent compte des attributs suivant : l'**état émotionnel** de l'apprenant ayant besoin d'aide et **les vecteurs d'unités linguistiques** extraites après les prétraitements de chaque feedback.

Une fois que la classification faite, seuls les feedbacks positifs seront retenus pour l'étape de composition.

6.2.2. Étape de composition

L'objectif dans cette étape est de *détecter* et de *supprimer* toute divulgation de données personnelles faites par certains apprenants dans les feedbacks qu'ils fournissent afin de préserver leur vie privée contre les menaces potentielles de divulgation. Ces menaces surviennent quand un apprenant divulgue des données permettant de le ré-identifier dans une requête d'aide ou dans un feedback fourni en réponse à une requête d'un co-apprenant. Le principal défi consiste donc à évaluer les possibilités de *détecter* et *d'extraire* des *indicateurs sur la divulgation* de données personnelles dans ces feedbacks. Pour ce faire, nous utilisons la

technique **d'analyse sémantique latente** (*Latent Semantic Analysis* ou LSA) (Deerwester *et al.*, 1990). LSA est une méthode statistique utilisée dans l'analyse des termes d'un texte ou d'un corpus de textes pour détecter automatiquement la sémantique, représentée par un ensemble de **concepts latents**. Pour ce faire, LSA se base sur le contexte d'utilisation ou d'apparition des termes dans un texte donné ou en voisinage avec d'autres termes.

Notre motivation d'utiliser LSA repose sur une représentation mathématique solide des textes indépendante des langues et des connaissances linguistiques (dictionnaires, ontologies, grammaires, étiquettes morphosyntaxiques, etc.). Cela rend l'analyse largement généralisable selon les langues et les domaines des textes de spécialité étudiés. L'analyse de la sémantique latente se fait en trois étapes :

1. *Construction de la matrice d'occurrences*
2. *Décomposition de la matrice*
3. *Réduction de dimensionnalité*

Dans la **première étape**, la matrice d'occurrences *A* est construite. Il s'agit d'une matrice dont les lignes et colonnes représentent respectivement les termes et les unités textuelles (paragraphe, phrase ou document). L'élément *(i, j)* de la matrice *A,* de dimensions t×d*,* correspond ainsi au nombre d'occurrences du terme *i* dans le document *j*.

$$A = d_j \downarrow \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{m,1} & \cdots & x_{m,n} \end{bmatrix} \\ t_i^T \rightarrow$$

En guise d'exemple, prenons les trois feedbacks suivants donnés par des pairs en réponse à une requête d'aide :

> **Requête :** « *Hello. I am from Georgia and I want speak English. Who can help me to practice my English?? Can you for me some advice?* »
> **Feedback 1 :** « *I would like to practice English with you. Please add me on skype. My skype id is* **** »
> **Feedback 2 :** « *No pain... no gain* »
> **Feedback 3 :** « *I will study English with u every day* »

Pour l'analyse sémantique, nous supposons que chaque feedback ou requête représente un document. Nous pouvons alors représenter l'occurrence simple des termes dans les feedbacks par la matrice *A* de dimensions t×d tel que l'illustre la table 11.

Table 11 – Exemple de matrice d'occurrences

	Requête	Feedback1	Feedback 2	Feedback 3
Georgia	1	0	0	0
want	1	0	0	0
speak	1	0	0	0
English	1	1	0	1
help	1	0	0	0
practice	1	1	0	0
like	0	1	0	0
add	0	1	0	0
Skype	0	1	0	0
pain	0	0	1	0
gain	0	0	1	0
study	0	0	0	1

Dans cet exemple, nous n'avons pas tenu compte des mots creux (par exemple I, to, with, you, on, etc.) et ne sont pas considérés dans l'analyse sémantique.

La deuxième étape dans le processus de LSA consiste à **identifier les valeurs singulières** de la matrice *A* afin de pouvoir la **décomposer en trois matrices** dont la multiplication donne *A*. Pour ce faire, LSA se base sur une méthode dite *Décomposition en valeurs singulières* (Singular Value Décomposition ou SVD). La décomposition en valeurs singulières de la matrice *A* donne :

$$A = U\Sigma V^T$$

où Σ est une matrice diagonale de valeurs singulières de dimensions m×m et U et V deux matrices orthogonales de dimensions respectives t×m et m×d.

Nous interprétons cette décomposition dans l'optique de la sémantique par le fait que les **concepts latents importants**, associés aux termes et aux feedbacks, sont ceux qui présentent une structure ou une présence plus marquée par rapport à l'ensemble des concepts de départ. Ainsi en annulant certaines valeurs de la matrice diagonale Σ et reconstruisant une matrice approchée de la matrice de départ, nous obtenons les concepts dominants de l'ensemble de concepts de départ. Comme nous supposons que la divulgation des données dans les feedbacks fournis n'est pas fréquente, utiliser la méthode LSA permet *d'écarter les concepts, les termes et feedbacks associés à la divulgation des données personnelles*.

Pour illustrer cela, reprenons la matrice *A* de l'exemple précédent, et décomposons la en trois matrices U, *Σ* et V. La matrice *Σ* obtenue est composée de 4 valeurs singulières obtenue comme le montre la figure 23.

```
S  =

   1.    0.          0.          0.
   0.    0.6613761   0.          0.
   0.    0.          0.5032796   0.
   0.    0.          0.          0.4571310
   0.    0.          0.          0.
   0.    0.          0.          0.
   0.    0.          0.          0.
   0.    0.          0.          0.
   0.    0.          0.          0.
   0.    0.          0.          0.
   0.    0.          0.          0.
   0.    0.          0.          0.
```

Figure 23 – Exemple de matrice de valeurs singulières

La décomposition en valeurs singulières est nécessaire pour **la troisième étape** dans LSA, qui est la *réduction des dimensions*. Elle consiste à ne conserver que les *k* plus grandes valeurs singulières pour reconstituer une matrice approchée de la matrice de départ *A*, de dimensions *k*. La réduction permet de mieux représenter les relations sémantiques entre les termes ou les feedbacks (ou les feedbacks des pairs et la requête d'aide). Cela revient à se concentrer uniquement sur les liens existants entre les feedbacks et les termes si l'on réduit l'espace sémantique à ses *k* dimensions (ou *k* concepts) les plus influentes dans les feedbacks. La valeur de dimensions *k* est importante car une réduction à un espace sémantique trop grand ne fait pas suffisamment émerger les liaisons sémantiques entre les termes et les feedbacks, et un espace trop petit conduit à une trop grande perte d'informations.

Après la réduction, il convient donc de reconstruire la matrice approchée de *A* de dimensions *k* à partir de laquelle nous allons pouvoir comparer les feedbacks avec la requête afin de déterminer si un feedback fourni par un co-apprenant répond bien à la requête à laquelle il a été donné.

Supposons que l'on veuille faire une *réduction au rang 3* de notre matrice *A* de la table 11 ce qui reviendrait à annuler la plus petite valeur singulière de la matrice S à savoir 0.4571310 (voir figure 23). Nous réduisons donc les rangs des matrices U, S et V pour obtenir des matrices représentant principalement les trois dimensions, ou concepts, les plus importantes

associées aux trois valeurs singulières conservées. Ensuite, nous reconstruisons la matrice *A'* qui représente l'approximation de *A* au rang *k*=3. Nous obtenons alors le résultat suivant :

```
ans  =

   0.3504278  - 0.0094777    0.           0.0426393
   0.3504278  - 0.0094777    0.           0.0426393
   0.3504278  - 0.0094777    0.           0.0426393
   0.3835894    0.4041210    0.           0.1388072
   0.3504278  - 0.0094777    0.           0.0426393
   0.3409500    0.3298962    0.           0.1168641
 - 0.0094777    0.3393739    0.           0.0742248
 - 0.0094777    0.3393739    0.           0.0742248
 - 0.0094777    0.3393739    0.           0.0742248
   4.492D-19    3.612D-17    0.3558724  - 7.045D-17
   4.492D-19    3.612D-17    0.3558724  - 7.045D-17
   0.0426393    0.0742248    0.           0.0219431
```

Figure 24 – Exemple de matrice approchée de A au rang 3

La matrice *A'* ainsi obtenue est une matrice approchée (et donc simplifiée) de la matrice initiale A ne contenant que la sémantique latente des termes les plus importants d'un point de vue statistique pour le corpus composée dans cet exemple par la requête et les 3 feedbacks (voir table 11). Nous pouvons donc utiliser cette matrice pour déterminer les feedbacks pertinents en utilisant une mesure de similarité telle que cosinus permettant d'évaluer les distances entre les feedbacks et la requête.

Dans cet exemple simple, chaque ligne représente un terme et chaque colonne représente un feedback ou requête de la matrice *A* (voir table 11). Dans cette matrice, nous avons considéré la *fréquence binaire* (1 si le terme apparait et 0 sinon) pour designer l'importance d'un terme dans un feedback. L'importance d'un terme dans ce contexte désigne son poids dans un feedback ou dans un corpus dépendamment de *l'approche de pondération* utilisée. La pondération est l'un des paramètres à considérer lors de l'utilisation de LSA. En effet, la performance de LSA dépend d'une série de paramètres qui doivent être fixés durant les étapes de l'analyse sémantique (Jorge-Botana *et al.*, 2015).

Étant donné que l'espace de ces paramètres est pratiquement grand, nous nous concentrons dans cette recherche principalement sur ces trois paramètres : la *pondération des termes*, la valeur *de réduction de dimensionnalité* et les *mesures de similarité*.

Pondération des termes

L'objectif de l'application de la pondération est de mieux représenter les termes importants dans le corpus en leur attribuant des poids plus élevés et des valeurs inférieures pour les

moins importants. Ainsi, plutôt que de se baser sur les occurrences de chacun des termes comme dans la table 10, la pondération permet de s'appuyer sur une estimation de l'importance de chaque terme dans le contexte d'usage. On distingue principalement trois approches de pondération (Dumais, 1992) :

- *globale* mettant en évidence les termes non fréquents dans un corpus donné (par exemple *Inverse Document Frequency*, etc.)
- *locale* donnant plus d'importance aux termes assez fréquents dans un document (par exemple *Term Frequency*, *Binary Term Frequency*, etc.)
- *hybride* permettant d'éviter la grande asymétrie dans les fréquences des termes (par exemple *Log-Entropy*, *TF-IDF*, etc.).

Prenons l'exemple du terme *English* dans la requête de la table 11. Soit t_1=*English*, R, F1, F2 et F3 désignent la requête, feedback 1, feedback 2 et feedback 3 :

- **Calcul de TF**

  TF (t_1, R) = nombre d'occurrence de t_1/ nombre de termes dans R

  TF (t_1, R) = 2/24
- **Calcul d'IDF**

  IDF (t_1)= logarithme de (nombre total de documents dans le corpus / nombre de documents où le terme t_1 apparaît)

  IDF (t_1)= $\log 4/3$
- **Calcul de TF-IDF**

  TF-IDF (t_1, R) = $\frac{2}{24} * \log\frac{4}{3}$= 0.04

  Les poids de ce terme dans les feedbacks sont alors :

  TF-IDF (t_1, F1) = $\frac{1}{18} * \log\frac{4}{3}$= 0.04

  TF-IDF (t_1, F2) = $\frac{0}{4} * \log\frac{4}{3}$= 0

  TF-IDF (t_1, F3) = $\frac{1}{8} * \log\frac{4}{3}$= 0.06

Cet exemple illustre l'impact de la pondération TF-IDF qui est basée sur l'idée que le poids d'un terme augmente proportionnellement au nombre de ses occurrences dans un document donné.

Rappelons que notre objectif dans l'étape de composition est de détecter et supprimer les feedbacks divulguant des données personnelles. Pour cela, nous supposons que la divulgation

de données personnelles dans les feedbacks fournis est non fréquente. Ceci étant dit, une approche de pondération attribuant des poids élevés aux termes moins fréquents (par exemple les approches globales) pourrait ne pas être appropriée pour supprimer les termes et feedbacks liés à la divulgation de données personnelles.

Réduction de dimensionnalité

Le deuxième paramètre qui nous intéresse dans cette analyse sémantique est le nombre de dimensions *k* à conserver dans la troisième étape de SVD. Tel que mentionné plus haut, en réduisant le nombre de dimensions, LSA peut mieux représenter les liens sémantiques entre termes et feedbacks ou requête et feedback dans notre cas.

Cependant, la valeur de la réduction *k* est un paramètre empirique dépendant de la nature et la taille des données. Il n'y a pas une méthode précise permettant de déterminer la valeur optimale de *k*, bien qu'une valeur de k=300 dimensions a été proclamée comme pouvant produire la meilleure performance (Troncy *et al.*, 2011).

Dans cette recherche, nous visons à explorer l'effet de ce paramètre sur la sensibilité de LSA à la divulgation de données. Cependant, nous croyons que la réduction de dimensionnalité permet de supprimer les dimensions associées à la divulgation de données car les concepts latents associés à la divulgation ne sont pas importants et ils seront donc écartés par LSA.

Mesures de similarité

En plus de la pondération et de la réduction de dimensionnalité, il convient de choisir une mesure de similarité appropriée afin de déterminer la distance entre chaque requête et les feedbacks associés dans l'espace sémantique construit par LSA. Cela revient à représenter la requête et les feedbacks comme des vecteurs d'unités linguistiques à utiliser une mesure comme le cosinus (ou par exemple la distance euclidienne) pour évaluer la similarité (ou la distance) entre les deux vecteurs (Jorge-Botana *et al.*, 2015). Ceci étant dit, pour représenter chaque nouvelle requête et les feedbacks associés nous utilisons une méthode dite de *Folding-in* permettant de projeter les nouveaux feedbacks dans l'espace sémantique en se basant sur les termes qu'ils contiennent (Jorge-Botana *et al.*, 2015); ce qui permet de mesurer leur similarité. Le choix de la mesure de similarité est un paramètre très important parce qu'il y a des mesures qui évaluent les ressemblances (comme le cosinus) alors qu'il y a d'autres qui tiennent compte aussi des différences entre vecteurs sémantiques (comme les mesures de distance de Jaccard par exemple).

Pour illustrer ces différences, reprenons l'exemple de la table 11 et mesurons la similarité entre la requête R et le feedback F1 en utilisant le cosinus comme suit :

$$\cos(R, F1) = \frac{R.F1}{\|R\|\|F1\|} = 0.36$$

Utilisons maintenant la distance Jaccard :

$$\mathrm{d}(R, F1) = \frac{|R \cap F1|}{|R \cup F1|} = 0.25$$

Cet exemple démontre qu'en conservant le cosinus, nous nous focalisons plus sur les termes en commun entre les deux vecteurs sémantiques pour exprimer la similarité. De plus, cette mesure n'est pas sensible à la norme des vecteurs, donc ne tient pas compte de la longueur des feedbacks ou de la requête. En revanche, la distance Jaccard considère la longueur des documents et tient compte aussi des différences entre les vecteurs sémantiques. Ceci étant dit, nous présumons que les mesures de distance, tout en considérant les différences entre le feedback et la requête, permettent mieux d'exprimer la similarité entre vecteurs dans l'espace sémantique de LSA; et donc elles permettent mieux d'écarter les feedbacks divulguant des données personnelles.

Afin d'examiner les effets des paramètres évoqués ci-hauts sur la suppression de la divulgation dans les interactions entre apprenants, nous avons mené deux études expérimentales. Les résultats de ces études sont présentés dans la section suivante.

6.3. Expérimentations

L'évaluation de la performance du module proposé consiste à comparer les résultats obtenus dans les deux étapes, à savoir la fouille et la composition, avec les valeurs attribuées par des experts humains. Pour cela, nous fixons deux objectifs de l'évaluation : le premier étant d'évaluer la performance des algorithmes d'analyse des sentiments utilisés dans l'étape de la fouille lors de la suppression des feedbacks négatifs des interactions entre apprenants. Le deuxième objectif d'évaluation est d'examiner la sensibilité de LSA à la divulgation de données personnelles. Pour ce faire, nous commençons par collecter les données à utiliser pour construire notre corpus d'interactions entre apprenants.

6.3.1. Caractéristiques du corpus étudié

Tandis que la majorité des travaux antérieurs ont porté sur l'utilisation des données *formelles* et académiques dans les évaluations des interactions entre apprenants, nous avons décidé de construire un corpus en langage naturel reflétant la réalité des interactions dans un contexte d'apprentissage informel. Le volume croissant de données accessibles sur le web tel que celui dans les forums de discussion fournit une opportunité de comprendre l'utilisation du langage naturel et d'examiner les caractéristiques de l'apprentissage social spontané et informel. De plus, dans ce contexte, les apprenants expriment fréquemment et spontanément leurs états émotionnels en demandant l'aide des autres membres de forum et divulguent généralement leurs données personnelles. Ainsi, un tel corpus nous permet d'évaluer nos deux objectifs à savoir supprimer les feedbacks négatifs et écarter toute divulgation des données dans les interactions.

Nous utilisons un corpus extrait de différents sites d'apprentissage *d'Anglais Seconde Langue* (par exemple *learn-english-forum.org*). Comme le modèle de LSA nécessite l'utilisation d'un large corpus, un total de plus de 1000 requêtes, avec les feedbacks associés, ont été recueillis pour construire l'espace sémantique.

Les interactions textuelles entre apprenants dans les environnements sont pleines de fautes d'orthographe et de saisie qui peuvent influencer les performances des algorithmes. Pour cela, il convient d'analyser les données collectées et de les traiter avant de les fournir en entrée aux algorithmes d'analyse des sentiments. Nous avons également utilisé des techniques de prétraitements pour diviser les feedbacks en unités linguistiques en se basant sur les signes de ponctuation (voir section 6.2.1).

Un exemple des interactions extraites des forums sont illustrées dans la table suivante.

Table 12 – Exemple d'interactions entre apprenants

Requêtes et feedbacks		Scores attribués	
		Expert 1	**Expert 2**
Requête 1	*Hello. I am from Georgia and I want speak English. Who can help me to practice my English?? Can you for me some advice?*		
Pair 1	*I would like to practice English with you. Please add me on skype. My skype id is *******	**2**	**1**
Pair 2	*No pain... no gain*	**2**	**2**
Pair 3	*I will study English with u every day*	**3**	**4**
Pair 4	*I'm from Colombia. I'm 22 years old and I want to practice my English with someone... It don't care who you are... if you want to practice English too*	**1**	**3**
Requête 2	*I'm not speaks much English and feel frustrated, if help me please for Learn thanks and what's your advice for my thanksssss*		
Pair 1	*I am a begginer ; but I want to speak English faster and I need and I want to practice... but let me learn more English vocabulary before practicing with u ☺*	**4**	**3**
Pair 2	*You have all been hyponotized by the cursed English language*	**1**	**1**
Pair 3	*Recently I visit mnemonic dictionary.com This website has tremendous English vocabulary data and it has different methods to learn it. Visit this website you will also enjoy learning new words*	**3**	**4**

Dans la table 12, les scores attribués désignent les notes attribuées par deux chercheurs (correspondant à nos experts humains) à chaque feedback d'un pair en réponse à la requête associée. Ces scores servent à l'évaluation de l'analyse et sont détaillés dans la section suivante.

6.3.2. Protocole expérimental

Pour chaque feedback, les deux experts humains ont évalué sa pertinence sur une échelle de Likert à 4 points : '1' désigne un feedback «très mauvais» (s'il est négatif, ridiculisant, démotivant ou divulguant des données personnelles) et '4' se réfère à «très bon».

Nous avons demandé aux chercheurs d'examiner dans leur évaluation deux aspects du feedback, à savoir la *pertinence du contenu* étant donné la requête et l'état émotionnel de l'apprenant et la *divulgation des données personnelles*. Afin d'estimer le niveau de

concordance globale entre les deux experts sur les scores attribués aux feedbacks, nous avons calculé un coefficient kappa de Cohen (1960). L'avantage du kappa de Cohen (κ) par rapport au calcul plutôt sommaire de la proportion d'accords observée (proportion observée notée P_o) entre deux juges est qu'il tient compte de la probabilité d'obtenir ce niveau d'accord de manière aléatoire (proportion estimée notée P_e). L'analyse des scores attribués par les experts humains a montré qu'il y a une concordance globale de κ=0.68, qui peut être considérée comme très satisfaisante étant donnée l'échelle de Likert à 4 catégories. Pour évaluer la performance des algorithmes d'analyse des sentiments utilisés dans l'étape de fouille, le score moyen donné par les deux chercheurs à chaque feedback est converti en *un modèle binaire :* un **score inférieur à 3** désigne un feedback *négatif,* alors qu'un **score supérieur à 3** réfère à un feedback *positif*. Cela sert à évaluer la précision de la classification des feedbacks en positifs et négatifs, ce qui constitue notre premier objectif d'évaluation.

En ce qui concerne le deuxième objectif d'évaluation, nous avons examiné la sensibilité de LSA à la divulgation en utilisant **plusieurs régressions multiples** et en considérant différentes variables dérivées de LSA qui seront détaillées dans les prochaines sections.

6.3.3. Évaluation de l'étape de fouille

Les émotions les plus rapportées dans les interactions entre apprenants formant notre corpus d'étude sont principalement l'*ennui*, la *frustration*, l'*anxiété*, la *démotivation* ainsi que l'*engagement*. Toutefois, nous n'avons pas considéré dans la classification l'*ennui* et l'*engagement* car il est difficile pour les deux experts humains d'évaluer si un feedback est positif/négatif étant donné un état d'engagement ou d'ennui.

Compte tenu de *l'état émotionnel* et des vecteurs d'unités linguistiques des feedbacks, l'algorithme d'analyse des sentiments doit pouvoir classifier correctement les feedbacks positifs de ceux négatifs qui ne seront pas envoyés à l'apprenant ayant besoin d'aide. En ce qui concerne les vecteurs d'unités linguistiques, nous examinons deux types de représentations linguistiques à savoir le **sac de mots** et le **bi-gramme**. La première représentation consiste à considérer chaque feedback comme un sac de mots indépendamment des propriétés linguistiques tel que l'ordre des mots. Par exemple, le prétraitement du feedback « *no gain…no pain* » donne le vecteur d'unités [*gain*, *pain*].

La *deuxième représentation* en bi-gramme consiste à trouver les pairs des mots qui occurrent souvent ensemble dans tous le corpus et les compter comme un bi-gramme tout en tenant

compte de l'ordre des mots. Pour illustrer reprenons l'exemple de « *no gain… no pain* ». Les deux bi-grammes extraits de ce feedback sont [*no-gain*, *no-pain*]. L'intérêt de considérer cette deuxième représentation est d'évaluer surtout l'effet de la négation comme dans l'exemple sur la classification des feedbacks.

Nous utilisons pour la classification les *arbres de décision C4.5*, le *classifieur naïf de Bayes*, les *règles d'association*, et les *k-plus proches voisins*. Afin de minimiser le nombre d'erreurs de classification sur l'ensemble de données d'apprentissage, nous avons mené une série de tests avec des configurations de classification différentes. Les résultats de ces tests sont présentés dans la section résultats.

6.3.4. Évaluation de l'étape de composition

Rappelons que pour évaluer la sensibilité de LSA à la divulgation de données, nous avons considéré trois paramètres : la pondération, le nombre de dimensions et la mesure de similarité. La performance de LSA dépend de l'interaction entre ces paramètres qui peuvent être représentés par des variables dérivées de l'espace sémantique construit par l'application de LSA. Ces variables servent alors à l'évaluation de l'impact de chaque paramètre testé et à l'évaluation de la performance de LSA par rapport aux experts humains (reflétés dans les scores moyens attribués à chaque feedback).

Pour cela, nous considérons principalement trois variables :

- le nombre de mots, désigné par *N_mots*
- le cosinus entre le feedback et la requête associée, désigné par *Feed_Req*
- la moyenne de cosinus entre le feedback et l'ensemble de tous les feedbacks fournis en réponse à la même requête, désignée par *Avg_Feed*.

Ces variables servent comme des variables indépendantes dans la régression linéaire multiple, menée pour évaluer la performance de LSA. La table 13 présente les corrélations de Pearson entre la moyenne des scores attribués par les deux experts humains et les variables indépendantes susmentionnées.

Table 13 – Corrélation entre variables indépendantes et scores humains

Variable	Corrélation
N_mots	0.233
Feed_Req	0.458
Avg_Feed	0.464

$p<0.01$

La faible corrélation de 0.233 entre la moyenne des scores des experts et le nombre de mots du feedback indique que cette variable n'affecte pas l'évaluation du feedback. Cela signifie que la longueur du feedback n'a pas affecté les scores attribués par les experts humains. Donc, cette variable est exclue de la régression.

Bien que les corrélations entre Feed_Req, Avg_Feed et la moyenne des scores des experts ne soient pas très fortes, elles sont satisfaisantes par rapport à notre objectif d'évaluation. Nous considérons uniquement ces deux dernières variables pour examiner l'impact des paramètres évoqués ci-haut, à savoir la pondération, la réduction et la mesure de similarité sur la performance de LSA.

6.4. Résultats et discussion

Nous examinons les résultats des tests menés dans chacune de deux étapes séparément. Chaque test a été exécuté plusieurs fois et les résultats sont la valeur moyenne sur les différentes itérations.

6.4.1. Résultats de l'étape de fouille

Dans cette étape, nous avons utilisé 2 outils Rapid Miner[7] et Weka[8] permettant d'expérimenter de nombreuses configurations de notre modèle de classification avec des fonctionnalités de prétraitement pour les données.

L'évaluation de la classification binaire (positif et négatif dans notre cas) est généralement effectuée en utilisant différentes mesures (Pang *et al.*, 2002) tels que la **précision** (mesurant la proportion des feedbacks correctement classifiés parmi toutes les classifications) et le **rappel** (mesurant la proportion des feedbacks correctement classifiés parmi les feedbacks appartenant à une classe). La précision est la métrique sélectionnée pour évaluer la

[7] rapidminer.com
[8] weka.wikispaces.com

performance dans notre recherche, car notre objectif est d'obtenir un classifieur qui généralise bien.

Les résultats obtenus pour les différents classificateurs sont présentés dans la table 14. Les précisions ainsi obtenues diffèrent d'un classificateur à l'autre et dépendent de la représentation linguistique utilisée en sac de mots ou bi-gramme.

Table 14 – Résultats de la classification des feedbacks

Algorithmes	**Configurations**	**Précision (%)**	
		Sac de mots	*Bi-gramme*
Classifieur de Bayes		86.11	**87.19**
K-NN	*k*=3	67	60.51
	k=5	55.51	49.49
C4.5	confiance=0.25	78.50	79.51
Règles d'association	support=0.1 confiance=0.8	55.51	65.76

Les résultats reportés ci-haut démontrent que le classifieur de Bayes fournit une meilleure précision en se basant sur un modèle bi-gramme. L'algorithme de Bayes classifie 87.19% de feedbacks correctement au coût d'une perte de 0.66% de bonnes corrections. La précision obtenue est considérée pertinente par rapport aux résultats des travaux similaires indiquant des précisions de 82.90% (Pang *et al.*, 2002) et 86.84% (Martínez-Cámara *et al.*, 2014) lors de la classification des critiques des films.

Nous estimons que la précision que nous avons trouvée est bonne et prometteuse dans le contexte des feedbacks entre apprenants dans les contextes d'apprentissage informel. En effet, ces données sont généralement considérées comme très difficiles à analyser car les messages échangés entre apprenants contiennent beaucoup d'erreurs et de symboles (voir table 12) ce qui rend leur prétraitement très couteux.

6.4.2. Résultats de l'étape de composition

Pour examiner l'impact des paramètres considérés dans l'étape de composition, nous avons choisi de les évaluer deux à deux pour pouvoir comprendre les interactions entre eux et leurs effets sur la performance de LSA par rapport aux experts humains.

Afin d'évaluer l'interaction entre la pondération et la dimensionnalité et leur impact sur les résultats de LSA, nous avons effectué une analyse de régression en se basant sur les deux variables indépendantes, Feed_Req et Avg_Feed, décrites dans la table 13. Dans ce test, nous utilisons le cosinus comme mesure de similarité pour calculer les variables indépendantes. Étant donné que ce sont des variables mesurées automatiquement, nous utilisons toutes les requêtes et leurs feedbacks associés dans le corpus et nous calculons les valeurs moyennes de régression.

La figue 25 présente les valeurs moyennes de régression obtenues pour les différentes valeurs de réduction considérées (25 %, 50 %, 70 %, 80% et 100 %) et les approches de pondération testées (IDF, Binary Term Frequency, TF-IDF et Log-Entropy). Notons que nous avons considéré des pourcentages de réduction plutôt que des valeurs exactes afin de mieux représenter l'effet de la réduction sur la performance de LSA.

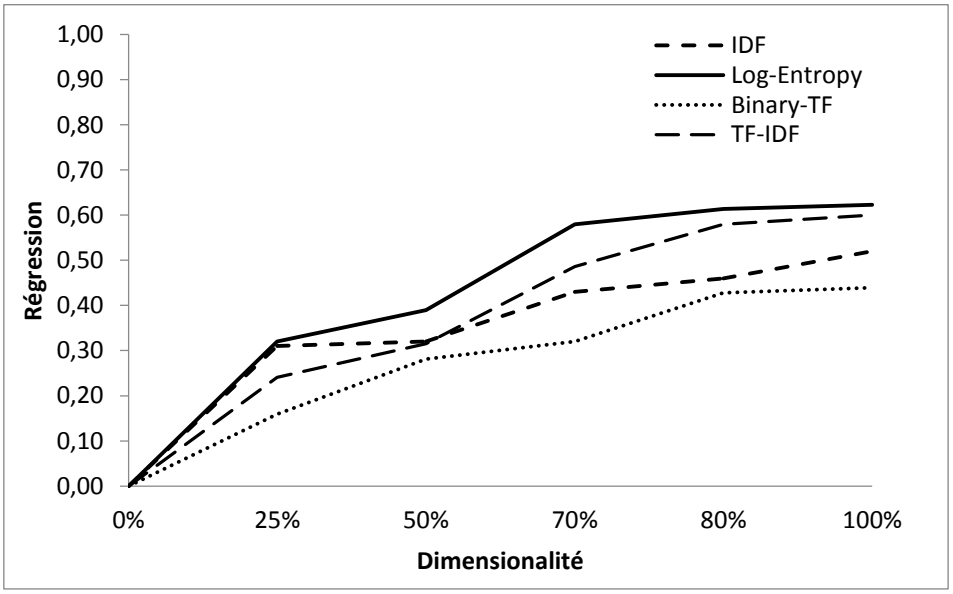


Figure 25 – Interaction entre dimensionnalité et pondération

D'après les résultats dans la figure 25, TF-IDF a démontré une bonne performance et a été la *deuxième meilleure* option après la fonction de pondération communément utilisée de Log-Entropy (avec r = 0.62, p <0.001). La différence entre les deux fonctions n'est pas

significative, bien que l'entropie soit généralement préférée dans la littérature lorsque LSA est utilisée.

Par ailleurs, la réduction de dimensionnalité a démontré une mauvaise performance par rapport au modèle sans réduction (correspondant à 100%). Bien que cela puisse être surprenant dans notre contexte, ce résultat est cohérent avec certaines études antérieures qui ont utilisé un corpus de taille limitée pour construire l'espace sémantique. Ces études ont postulé que la réduction de dimensionnalité est plus compatible avec les mesures de distance que le cosinus dans certains corpus (Boling et Das, 2015).

Afin d'examiner cela, nous avons mené une série de tests pour étudier l'interaction entre la dimensionnalité et la mesure de similarité. Nous utilisons TF-IDF pour la pondération, la distance euclidienne et la distance de Jaccard respectivement pour calculer les variables indépendantes de Feed_Req et Avg_Feed.

Pour chaque mesure de similarité (cosinus, distance euclidienne et distance de Jaccard), nous considérons différentes valeurs de réduction de dimensionnalité (25 %, 50 %, 70 %, 80% et 100 %) pour calculer les variables Feed_Req et Avg_Feed. Ensuite, nous calculons les corrélations obtenues entre les moyennes de valeurs des variables indépendantes et ceux des experts humains. Les résultats de ces tests sont illustrés dans la figure 26.

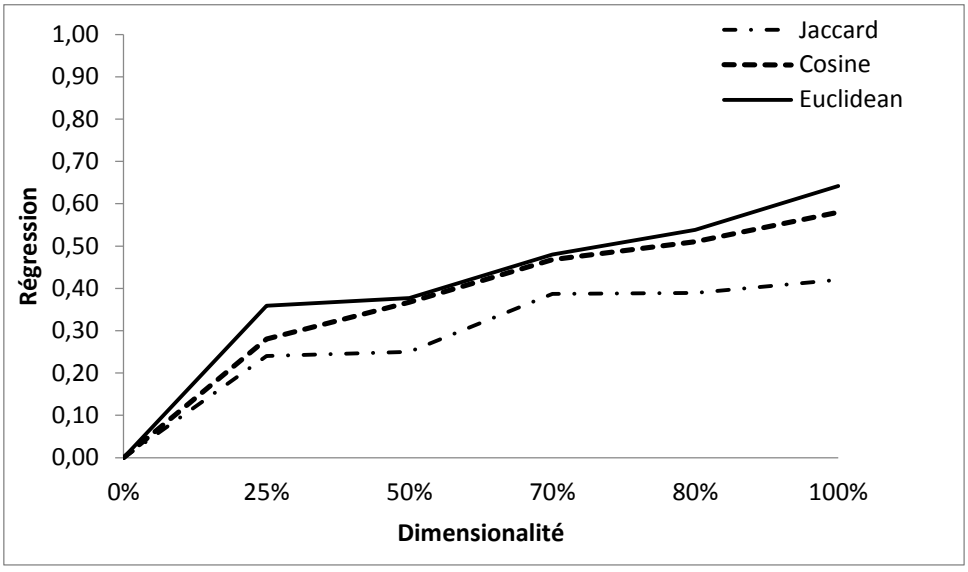


Figure 26 – Interaction entre dimensionnalité et mesure de similarité

La corrélation entre le modèle de LSA basé sur TF-IDF pour la pondération, n'ayant aucune réduction et basé sur la distance euclidienne comme mesure de similarité, et (que nous

désignons par modèle M1) avec les experts humains est très significative. En effet, bien qu'elle soit considérée comme modérée, cette corrélation de $r = 0.64$ ($p < 0.001$) est statistiquement équivalente à la concordance entre les experts humains ($\kappa = 0.68$). Dans les faits, lorsque les juges humains classifient un feedback comme négatif ou divulguant des données personnelles (score de 1 ou 2), alors le sous-module composition le classifie comme étant négatif en se basant sur les variables dérivées du modèle M1.

L'interaction entre la dimensionnalité et la mesure de similarité (pondération étant fixée à TF-IDF) montre que le processus de LSA est complexe et très dépendant de la combinaison de paramètres utilisés. Après avoir testé différents modèles, y compris différentes approches de pondération, valeurs de réduction et mesures de similarité, la meilleure corrélation obtenue est effectuée en se basant sur une combinaison de **TF-IDF** pour pondération, **sans réduction** de dimensions et **distance euclidienne** comme mesure de similarité.

Cela nous amène à conclure que les approches hybrides, plus particulièrement TF-IDF, semblent plus avantageuses, dans notre contexte, car elles semblent offrir de meilleures performances par rapport aux autres approches de pondération globale et locale examinées dans cette étude. De plus, nous constatons que la réduction de dimensionnalité a diminué les performances de LSA. Bien que cela puisse paraitre surprenant, cela pourrait être justifié par la nature des données constituant le corpus des interactions composé des feedbacks de longueur plus ou moins limitée.

En ce qui concerne les mesures de similarité, nous constatons que la distance, en particulier euclidienne, se comportent nettement mieux que Jaccard et cosinus. Ce résultat a été aussi validé récemment dans la littérature dans l'étude de (Jorge-Botana *et al.*, 2015) mais en se basant sur un corpus de données académiques.

Pour expliquer le rôle de ces paramètres sur le plan pratique, nous analysons le nombre des feedbacks des pairs qui pourraient être envoyés à l'apprenant qui a fait la requête d'aide si notre modèle de LSA avait été mis en œuvre pour éliminer les feedbacks négatifs et divulguant des données personnelles. Pour cela, nous calculons les scores attribués pour chaque feedback en modifiant les paramètres du modèle LSA. Ensuite, nous convertissons les valeurs des scores obtenues pour chaque feedback en une évaluation binaire (c'est-à-dire pour un score supérieur à 3, le feedback est envoyé à l'apprenant qui a demandé l'aide, pour un score inférieur à 3 le feedback est supprimé). Pour ce faire, nous avons considéré le modèle M1 basé sur la combinaisons de *TF-IDF* pour la pondération, n'ayant *aucune réduction de*

dimensions, et basé sur la *distance euclidienne* pour la similarité et un autre modèle M2 basé sur *Log-Entropy* pour la pondération, n'ayant *aucune réduction de dimensions*, et basé sur le cosinus pour la similarité. Le pourcentage des feedbacks correctement évalués est de **41%** pour M1; et **39%** pour M2.

Notons ici que bien que la différence des pourcentages ne soit pas trop grande entre les deux modèles considérés, le problème pourrait résider dans les scores attribués par les experts humains même. En effet, dans le but d'examiner la sensibilité humaine quant à la divulgation, nous avons délibérément omis de fournir aux experts des critères d'évaluation spécifiques. Cela implique que leur évaluation pouvait exclure certains feedbacks pertinents de point du vue de l'apprentissage, mais comportant une divulgation de données. Cela peut être clairement illustré dans l'exemple suivant de la table 12 :

Pair 4	*I'm from Colombia. I'm 22 years old and I want to practice my English with someone... It don't care who you are... if you want to practice English too*	**1**	**3**

Ce feedback est classifié comme négatif car la moyenne des scores attribués par les experts humais est inférieure à 3 (1+3/2=2). Le premier juge qui a considéré que le feedback divulgue des données personnelles (pays= Colombia et âge=22) lui a attribué un score de 1, bien que le feedback ne soit pas intimidant ou négatif en se basant sur les termes qu'il contient. En revanche le deuxième juge lui a attribué un score de 3, considérant que les données divulguées ne peuvent entrainer la ré-identification de la personne. Cela montre la différence de sensibilité entre les individus mêmes vis-à-vis de la divulgation des données personnelles et qui constitue un défi majeur dans l'étude d'interactions en langage naturel.

6.5. Conclusion

Dans ce chapitre, nous avons proposé un module pour analyser les interactions entre apprenants dans un contexte d'apprentissage informel. Le module proposé vise à améliorer les interactions et à favoriser l'apprentissage en instaurant un espace interactionnel encourageant les interactions positives et préservant la vie privée. Les résultats obtenus montrent qu'il est possible de prédire avec succès si un feedback donné par un co-apprenant est pertinent ou non pour un apprenant dans un contexte social et émotionnel donné. Cela permet d'adapter les

interactions de l’apprenant à son état émotionnel d’une part et de préserver sa vie privée, d’autre part, améliorant ainsi l’apprentissage.

Ce travail est très différent des travaux similaires portant sur l’analyse des interactions entre apprenants qui ont considéré surtout l’aspect cognitif de l’interaction et ont ignoré, pour la majorité, l'état émotionnel de l'apprenant qui affecte grandement la perception du feedback et son utilité pour celui qui l'a demandé. Il est également différent des travaux similaires dans le fait de proposer une solution pour la divulgation des données personnelles assez présentes dans les interactions sociales dans les environnements informels ainsi que formels incluant des outils d’interaction (tels que les forums et la discussion instantanée). Bien que les algorithmes d’apprentissage machine supervisé ne peuvent pas être utilisés dans ces environnement étant donné le cout élevé de leur entrainement, des algorithmes d’apprentissage semi-supervisé ou non-supervisé peuvent être une bonne option pour détecter et supprimer automatiquement la divulgation des données personnelles, dans des travaux futurs.

Chapitre 7 : Étude de cas de la cyberintimidation

Le gestionnaire de vie privée que nous proposons dans cette recherche vise à protéger les apprenants, impliqués dans des interactions sociales, des risques de divulgation de données personnelles et de ses conséquences. L'un de ces risques est notamment la *cyberintimidation* qui a connu une augmentation remarquable dans les environnements sociaux ces dernières années (Wingate *et al.*, 2013). L'étude de cas de la cyberintimidation comme étant un des risques potentiels de la divulgation permet d'analyser en profondeur ce phénomène dans son contexte.

Le gestionnaire de vie privée protège les apprenants de la cyberintimidation en *sélectionnant des pairs de confiance pour fournir l'aide*, en *contrôlant la divulgation de données* et en *supprimant les divulgations non intentionnelles et les feedbacks négatifs*. Afin d'évaluer l'utilité globale du gestionnaire dans la protection des risques de cyberintimidation, nous avons mené une étude empirique visant à examiner les corrélations entre les différents facteurs de risque et de protection considérés dans cette recherche, et la cyberintimidation dans les interactions sociales en ligne. Les détails du déroulement et des résultats de cette étude sont présentés dans ce chapitre.

7.1. Interaction et cyberintimidation

Les interactions sociales sont particulièrement bénéfiques pour l'apprentissage informel, tout au long de la vie et l'apprentissage à distance (Zheng et Warschauer, 2015). Néanmoins, avec ces avantages viennent certains inconvénients et risques. Alors que la plupart des interactions en ligne sont positives, des échanges *négatifs* incluant un *langage abusif*, de l'*intimidation* et du *harcèlement* sont aussi très fréquents (Wingate *et al.*, 2013). Ce phénomène, connu sous le nom de cyberintimidation, a suscité l'intérêt de nombreux chercheurs sur le plan social, psychologique et éducatif. Dans ce dernier contexte, la cyberintimidation a des effets négatifs sur les étudiants tels que la *baisse de rendement scolaire*, *l'abandon des écoles* et *d'apprentissage* (West, 2015). À cela s'ajoutent des *conséquences psychologiques* très sérieuses allant de la *détresse émotionnelle* jusqu'au *suicide* dans des cas extrêmes (Wingate *et al.*, 2013).

Malgré sa prévalence et ses conséquences incontestables, la cyberintimidation est un concept difficile à définir en théorie. Elle est associée à tout comportement antisocial, abusif, agressif et répétitif incluant le dénigrement, le sarcasme excessif, l'exclusion, le harcèlement, la menace, etc., qu'une personne ou un groupe de personnes commettent envers une autre personne pour sa **vulnérabilité** due à **un partage des informations inappropriées** ou **sensibles**, parfois avec ignorance ou indifférence (Kowalski *et al.*, 2014). Dans ce sens, une étude menée par Lee *et al.* (2013) a révélé que les utilisateurs divulguent souvent des informations personnelles très sensibles, dans leurs interactions en ligne, allant des informations démographiques tels que l'âge, le sexe, et l'adresse à des informations sur la santé dans certains cas, ce qui les rend plus vulnérables à la cyberintimidation, si ces informations sont utilisées contre eux.

Beaucoup de gens croient que seuls les enfants peuvent être victimes de ce comportement, mais en fait, des recherches récentes ont montré que plus de 22% des adultes avaient été victimes de cyberintimidation au moins une fois au cours des six derniers mois (Levy *et al.*, 2012). Dans cette optique, Kowalski *et al.* (2014) ont identifié certaines caractéristiques des interactions sociales en ligne facilitant et encourageant la cyberintimidation. Parmi ces caractéristiques, les auteurs ont mentionné essentiellement *l'accessibilité à l'autre*, *l'anonymat en ligne* et *le manque de réactivité émotionnelle*. En effet, plus spécifiquement dans l'interaction textuelle en ligne, certains utilisateurs pourraient être plus enclins à blesser et offenser plus facilement les autres du fait qu'ils ne perçoivent pas les émotions de ces derniers et les conséquences de leurs comportements offensifs sur leurs victimes.

Nous avons mené une étude pour déterminer particulièrement le rôle de l'auto-divulgation des données personnelles dans les risques potentiels de cyberintimidation. Nous examinons également les facteurs étudiés dans cette recherche telle que la confiance et leurs associations à la cyberintimidation. Le modèle et nos hypothèses de recherche, la méthodologie adoptée ainsi que les résultats obtenus sont présentés dans les sections suivantes.

7.2. Hypothèses et modèle de recherche

Récemment, plusieurs études dont Vivolo-Kantor *et al.* (2014) ont commencé à examiner les facteurs derrière l'implication dans la cyberintimidation en essayant de répondre aux questions suivantes : Quelles sont les caractéristiques des *intimidateurs* et celles des *intimidés* ? Y a-t-il des prédicteurs de la victimisation et la perpétration d'actes de cyberintimidation?

Dans ce sens, certains chercheurs se sont focalisés sur les facteurs psychologiques ou sociaux liés à la perpétration d'actes de cyberintimidation ont constaté que le *narcissisme* (Fanti *et al.,* 2012) et le *désengagement moral* (Hemphill et Heerde, 2014) ont un rôle considérable à jouer dans la perpétration d'actes de cyberintimidation. En revanche, d'autres études ont trouvé différents facteurs tels que l'*hyperactivité* et l'*extraversion* comme de forts prédicteurs de la victimisation à la cyberintimidation (Kowalski *et al.*, 2014). En effet, il est clair que la personnalité, qui implique une combinaison particulière des modèles émotionnels, psychologiques et réponse comportementale d'un individu, a une influence sur la façon dont ce dernier se comporte et ses réponses à l'interaction avec les autres. Par exemple, les traits de personnalité peuvent affecter le choix de contenu en ligne ou peuvent conduire à un modèle général de comportement dans une situation spécifique. Cela signifie que la personnalité influe les comportements des utilisateurs en ligne et leurs stratégies d'auto-présentation (Nevin, 2015).

Dans cette étude, nous nous intéressons aux associations entre la *personnalité*, le *comportement en ligne* et la *cyberintimidation* à savoir la *victimisation et* la *perpétration d'actes de cyberintimidation*. Les associations entre ces facteurs constituent les hypothèses de notre modèle de recherche, détaillé dans cette section.

7.2.1. Personnalité, comportement en ligne et perpétration d'actes de cyberintimidation

La compréhension du rôle que jouent les traits de personnalité dans les comportements abusifs et dans la cyberintimidation peut aider à mieux concevoir des solutions de prévention/intervention visant à réduire la prévalence de ce phénomène dans les interactions sociales. Dans les faits, cela permet de prédire si un individu pourrait être un intimidateur ou s'il est plus vulnérable à la cyberintimidation et par conséquent le protéger avant que le mal ne soit fait. Dans ce contexte, des chercheurs ont étudié les relations entre les cinq facteurs de l'inventaire de personnalité Big Five et la cyberintimidation (Festl et Quandt, 2013). Rappelons que cet inventaire comprend cinq traits qui sont : *extraversion*, *agréabilité*, *ouverture à l'expérience*, *conscienciosité* et *névrosisme*.

L'extraversion est associée à la sociabilité et la loquacité, alors que **l'agréabilité** est généralement associée à la cordialité, l'esprit de coopération, et la serviabilité. **L'ouverture à l'expérience**, elle, est associée à la créativité, la recherche de la nouveauté et l'excitation,

tandis que la **conscienciosité** se rattache à la discipline, la crédibilité et l'organisation. Enfin, le **névrosisme** est associé à l'anxiété et l'instabilité émotionnelle.

Dans l'une des études reliant la cyberintimidation au Big Five, Festl et Quandt (2013) ont constaté que le névrosisme et l'extraversion étaient de forts prédicteurs de la perpétration d'actes de cyberintimidation. Néanmoins, *deux autres traits* pourraient être de bons prédicteurs de la cyberintimidation, bien qu'ils y soient négativement associés. Le *premier trait* est l'agréabilité qui se rattache aux individus de confiance, coopératifs qui préfèrent maintenir des relations positives avec les autres (Foody *et al.*, 2015). Le *second trait* est la conscienciosité qui concerne la façon dont les gens contrôlent, règlent et dirigent leurs réactions envers les autres.

Les individus ayant de **faibles scores d'agréabilité et de conscienciosité**, dits *égocentriques*, sont généralement indifférents à la fois aux règles conventionnelles et aux émotions des autres (Foody *et al.*, 2015). Ils sont généralement décrits par les autres comme peu coopératifs, irrespectueux, égoïstes et prétentieux (Kowalski *et al.*, 2014). Nous estimons que, dans un contexte d'interaction en ligne, ces deux traits de personnalité auraient un impact sur la volonté de coopération des individus et leurs réactions face aux requêtes d'aide des autres, ce qui augmente la probabilité de s'engager dans des comportements abusifs et intimidants.

Par conséquent, nous formulons les hypothèses suivantes :

> **H1.** *L'agréabilité est négativement associée à la probabilité d'implication dans des comportements abusifs*
>
> **H2.** *La conscienciosité est négativement associée à la probabilité d'implication dans des comportements abusifs*
>
> **H3.** *L'implication dans des comportements abusifs est positivement associée à la perpétration d'actes de cyberintimidation.*

7.2.2. Personnalité, comportement en ligne et victimisation

Il est à noter que les individus présentant différents facteurs de vulnérabilité sont bien souvent ceux qui adoptent des comportements plus risqués en ligne en s'engagement dans une divulgation excessives des données souvent sensibles et s'y exposent de façon plus hasardeuse (Xu *et al.*, 2012). Soutenu souvent par l'anonymat et le manque de supervision significative en ligne, certains utilisateurs pourraient réagir défavorablement à l'information

divulguée ou révélée en s'impliquant dans des comportements abusifs ou dans la cyberintimidation. Ceci dit en s'engageant dans une pratique d'auto-divulgation qui inclut souvent des *informations personnelles* très *sensibles*, des *émotions intimes*, *attitudes, ou des sentiments*, les individus peuvent devenir plus *vulnérables* (Kokolakis, 2015).

Compte tenu de ces constatations, nous considérons l'hypothèse suivante :

> **H4.** *Les personnes s'engageant dans l'auto-divulgation sont plus susceptibles d'adopter des comportements à risque.*

Les processus d'auto-divulgation et d'auto-présentation sont des aspects importants de l'interaction sociale (Giota et Kleftaras, 2014) recouvrant la manière dont un individu se présente aux autres. Les individus ont tendance à mettre en évidence leurs aspects positifs et négatifs dans la création de leurs identités sociales virtuelles en utilisant de nombreuses stratégies (Sampasa-Kanyinga et Hamilton, 2015). Ces stratégies sont principalement divisées en deux catégories : *assertive* et *défensive* (Dredge *et al.*, 2014). **Les stratégies défensives** sont utilisées pour justifier ou rétablir une situation, alors que celles **assertives** visent à créer une identité particulière de l'individu (Sadler *et al.*, 2010). Par exemple, au cours de leurs échanges en ligne avec les autres, certains individus ne se soucient pas d'être détestés, ils cherchent plutôt à être craints et à paraitre puissants. Cette stratégie *assertive*, dite d'*ingratiation*, est l'une des plus étudiées dans la littérature sur l'auto-présentation (Sadler *et al.*, 2010). Ainsi, cela peut être considéré comme un *comportement à risque* de s'engager dans certaines stratégies négatives d'auto-présentation lors de ses interactions avec les autres, soit dans des requêtes d'aide ou en répondant aux requêtes des autres. Cela nous mène à formuler l'hypothèse suivante :

> **H5.** *Les personnes qui se livrent à l'auto-présentation sont plus susceptibles d'adopter des comportements à risque.*

7.2.3. Impact de la victimisation sur la perpétration d'actes de cyberintimidation

Peu d'études se sont intéressées à la relation et l'effet de la victimisation sur la perpétration d'actes de cyberintimidation. Par exemple, Pabian et Vandebosch (2015) ont étudié l'impact de la participation à l'intimidation traditionnelle sur l'implication dans la cyberintimidation, mais ils n'ont pas étudié les relations bidirectionnelles entre la victimisation et l'engagement ultérieur dans la cyberintimidation. Tandis que Kowalski *et al.* (2014) ont démontré qu'une

exposition à une intimidation préalable augmente le risque de la participation à la cyberintimidation.

La recherche sur l'intimidation a montré qu'il existe deux types d'intimidateurs : les **purs intimidateurs** et les **intimidateurs-victimes** (Law *et al.*, 2012). Les premiers sont ceux qui sont les plus susceptibles de s'engager dans l'intimidation afin d'améliorer leurs situations sociales en croyant rétablir de cette manière un rapport de pouvoir envers l'autre par exemple (Foody *et al.*, 2015). Les *intimidateurs-victimes*, eux, sont plus susceptibles de se livrer à un comportement abusif où à une intimidation dans le but de se venger ou se défendre suite à une victimisation. En se basant sur ces constatations, nous établissons les hypothèses suivantes :

> **H6.** *Les personnes qui s'engagent dans des comportements à risque sont plus susceptibles de se livrer à des comportements abusifs*
>
> **H7.** *Les comportements à risque sont positivement associés à l'implication dans la cyberintimidation*

La figure 27 présente le modèle de recherche et résume les hypothèses évoquées ci-haut.

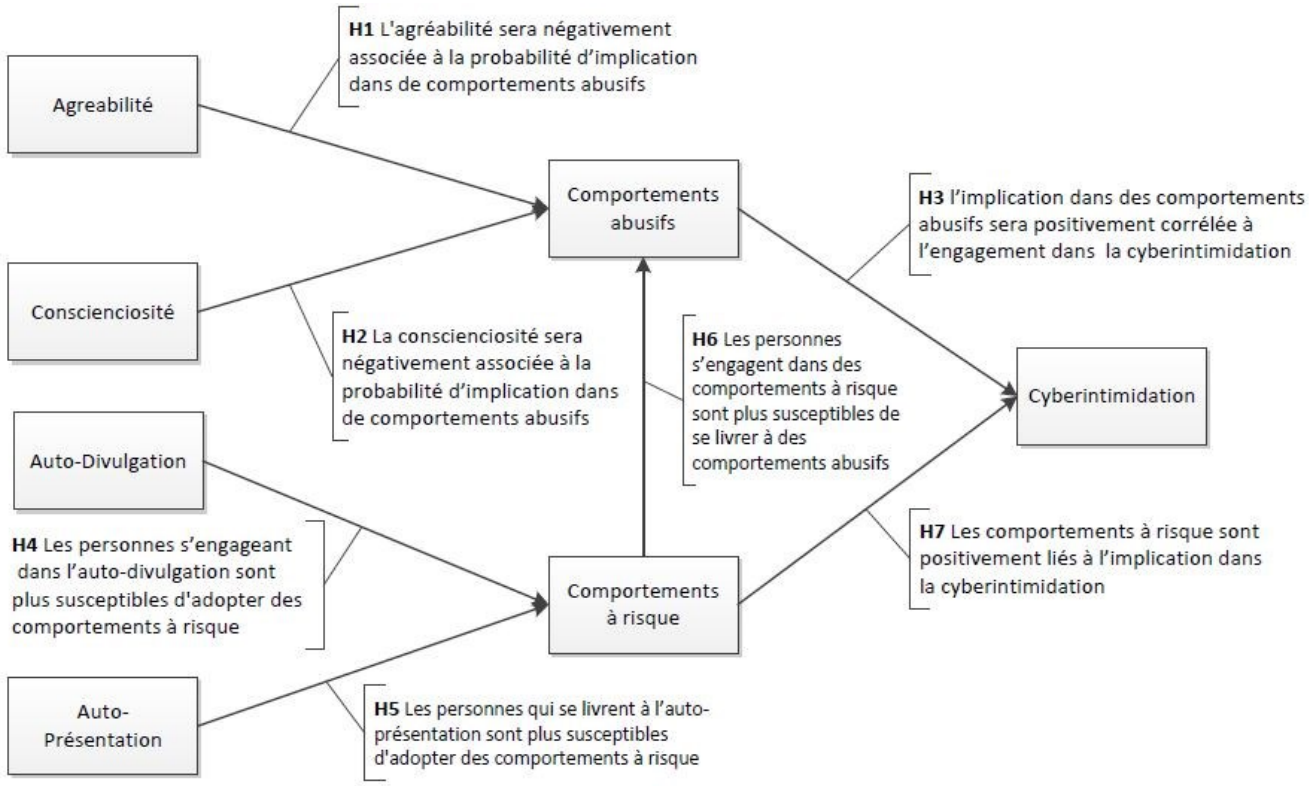


Figure 27 – Modèle et hypothèses de recherche

Après avoir présenté nos hypothèses, nous décrivons dans la section suivante la méthodologie ainsi que les différentes mesures utilisées dans cette étude pour tester et évaluer ces hypothèses.

7.3. Méthodologie

7.3.1. Objectif de la présente étude

Dans cette recherche, nous considérons la confiance comme un facteur clé dans le compromis entre auto-divulgation et risque d'atteinte à la vie privée. La confiance, plus précisément l'aspect psychologique de la confiance, est mesuré dans ce travail en se basant sur les traits d'agréabilité et de conscienciosité. Ceci étant dit, nous cherchons dans cette étude à trouver les preuves que les cyberintimidateurs et les individus qui s'engagent dans des comportements abusifs sont ceux dont les scores d'agréabilité et de conscienciosité sont les plus faibles.

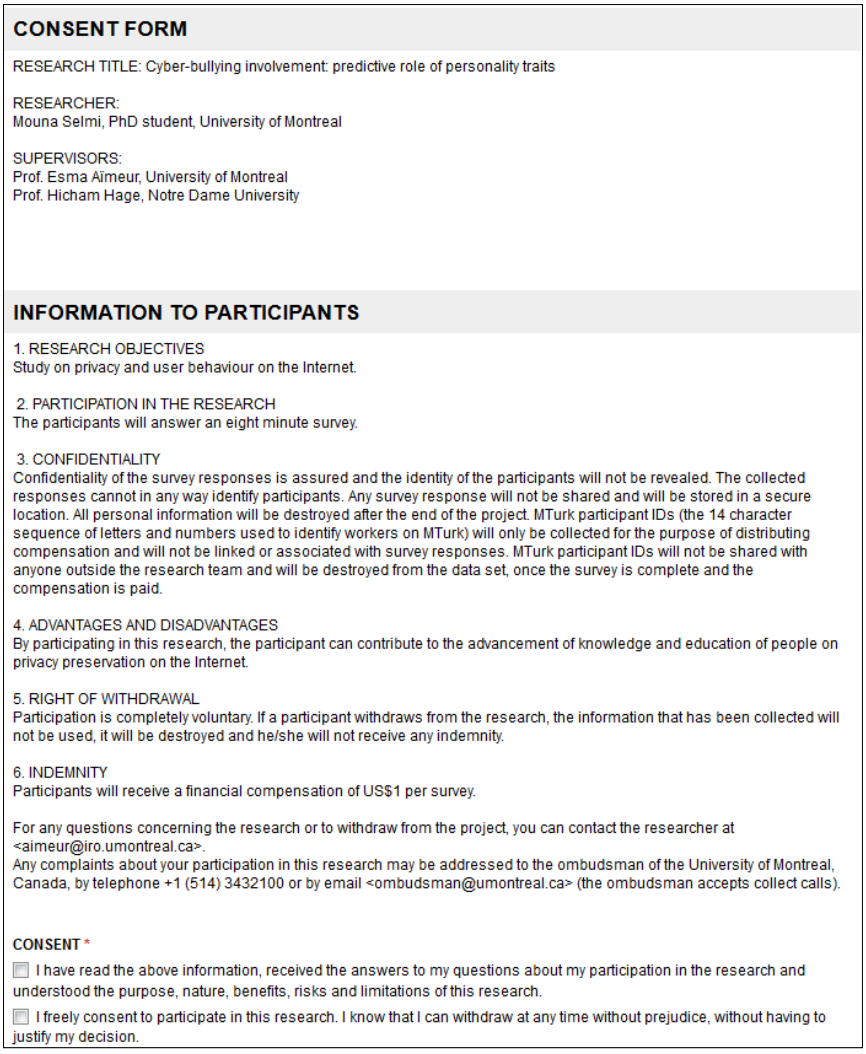
Nous nous intéressons également, dans cette étude, à examiner *les relations bidirectionnelles* entre la victimisation et la perpétration d'actes de cyberintimidation. Cela revient à déterminer si les victimes de cyberintimidation s'engagent à leur tour dans des comportements abusifs et intimidants. Cela est important dans notre contexte car nous voulons nous assurer que notre choix de supprimer les feedbacks négatifs et intimidants des interactions est la meilleure option pour réduire le phénomène de cyberintimidation. En plus de cela, nous testons nos hypothèses initiales liées au rôle de l'auto-divulgation, et de l'auto-présentation, dans les risques d'atteinte à la vie privée dans les interactions sociales en ligne.

7.3.2. Données et Échantillon

Cette étude a utilisé *Amazon Mechanical Turk* (MTurk) pour recruter des participants en Août 2015. Nous avons choisi la plateforme MTurk pour le recrutement des participants, car elle offre l'avantage d'avoir un grand échantillon de sujets de diverses cultures, avec un large éventail d'âge et pays d'origine, ce qui facilite la recherche multiculturelle et la généralisation des résultats (Mason et Suri, 2012). Les chercheurs ont démontré que la qualité des données de MTurk pour des études comportementales en ligne est meilleure que des études utilisant des méthodes d'enquête traditionnelles parce qu'elle offre un échantillon représentatif.

Les turkers (le nom donné aux participants sur cette plateforme) ayant effectué au moins 100 tâches sur la plateforme dont 95% ont été validées, ont été invités à répondre à un test de huit minutes pour une indemnité de 1 $.

Avant de collecter les réponses, un consentement a été obtenu de tous les participants expliquant la confidentialité de leurs réponses et la possibilité de contacter les chercheurs responsables de l'étude s'il y a des questions ou pour le retrait de leur participation, tel qu'illustré dans la figure 28.



CONSENT FORM

RESEARCH TITLE: Cyber-bullying involvement: predictive role of personality traits

RESEARCHER:
Mouna Selmi, PhD student, University of Montreal

SUPERVISORS:
Prof. Esma Aïmeur, University of Montreal
Prof. Hicham Hage, Notre Dame University

INFORMATION TO PARTICIPANTS

1. RESEARCH OBJECTIVES
Study on privacy and user behaviour on the Internet.

2. PARTICIPATION IN THE RESEARCH
The participants will answer an eight minute survey.

3. CONFIDENTIALITY
Confidentiality of the survey responses is assured and the identity of the participants will not be revealed. The collected responses cannot in any way identify participants. Any survey response will not be shared and will be stored in a secure location. All personal information will be destroyed after the end of the project. MTurk participant IDs (the 14 character sequence of letters and numbers used to identify workers on MTurk) will only be collected for the purpose of distributing compensation and will not be linked or associated with survey responses. MTurk participant IDs will not be shared with anyone outside the research team and will be destroyed from the data set, once the survey is complete and the compensation is paid.

4. ADVANTAGES AND DISADVANTAGES
By participating in this research, the participant can contribute to the advancement of knowledge and education of people on privacy preservation on the Internet.

5. RIGHT OF WITHDRAWAL
Participation is completely voluntary. If a participant withdraws from the research, the information that has been collected will not be used, it will be destroyed and he/she will not receive any indemnity.

6. INDEMNITY
Participants will receive a financial compensation of US$1 per survey.

For any questions concerning the research or to withdraw from the project, you can contact the researcher at <aimeur@iro.umontreal.ca>.
Any complaints about your participation in this research may be addressed to the ombudsman of the University of Montreal, Canada, by telephone +1 (514) 3432100 or by email <ombudsman@umontreal.ca> (the ombudsman accepts collect calls).

CONSENT *

☐ I have read the above information, received the answers to my questions about my participation in the research and understood the purpose, nature, benefits, risks and limitations of this research.

☐ I freely consent to participate in this research. I know that I can withdraw at any time without prejudice, without having to justify my decision.

Figure 28 – Formulaire de consentement

Un total de 520 participants a répondu à cette étude. La participation d'un seul répondant a été retirée à cause de ses réponses uniformes à un grand nombre de questions. Ainsi, nous avons basé notre étude sur un échantillon de 519 participants. La table 15 présente les caractéristiques démographiques de l'échantillon résultant se composant de 302 hommes (58.4%) et de 215 femmes (41.4%).

Table 15 – Caractéristiques démographiques des participants

Attributs	Catégories	Nombre	Pourcentage
Genre	Homme	302	58.4%
	Femme	214	41.4%
	Pas de réponse	1	0.2%
Age	18-24	92	17.8%
	25-34	236	45.6%
	35-44	112	21.7%
	45-54	47	9.1%
	55+	30	5.8%
Scolarité	Secondaire	163	31.7%
	École technique/Métiers	82	15.9%
	Licence	210	40.6%
	Maitrise	36	7%
	Doctorat	9	1.7%
	Pas de réponse	17	3.1%
Occupation	Étudiant	60	11.6%
	Fonctionnaire	151	29.2%
	Professionnel	86	16.6%
	Travailleur autonome	102	19.7%
	Gérant/Directeur	22	4.3%
	Retraité / En chômage	65	12.6%
	Pas de réponse	31	6%

7.3.3. Instruments de mesures

Le modèle de recherche présenté dans la figure 27 comprend sept variables, qui sont bien étayées par la littérature et la recherche sur la personnalité, le comportement en ligne et la cyberintimidation. Les instruments de mesures utilisés pour évaluer l'association entre ces variables sont divisés en quatre parties comme suit :

- **Partie 1** mesure les traits de personnalité à savoir l'*agréabilité*, la *conscienciosité*, *l'auto-divulgation* et *l'auto-présentation*.
- **Partie 2** contient des questions sur les types de *comportements risqués* et *abusifs* des utilisateurs en ligne.
- **Partie 3** examine l'expérience de l'utilisateur en termes de *victimisation* ainsi que de *perpétration* d'actes de cyberintimidation.
- **Partie 4** se rapporte aux données démographiques des participants.

Toutes les questions ont été évaluées sur une échelle de Likert à 5 points allant de 1 = «entièrement en désaccord» à 5 = «entièrement d'accord» pour la partie 1 et de 1 = «jamais» à 5 = «très fréquemment» pour les parties 2 et 3.

L'étude est composée de 30 questions, inspirées et adaptées de plusieurs recherches pour être cohérentes avec notre contexte de cyberintimidation dans les interactions sociales en ligne. Les instruments de mesures utilisés dans la présente étude sont détaillés ci-dessous dans le même ordre de leur apparition dans l'enquête.

Inventaire de personnalité Big Five

Les variables de personnalité sont mesurées en utilisant l'instrument Mini-IPIP (pour *Mini International Personality Item Pool*). Bien qu'il soit une forme réduite de l'inventaire de Big Five (ou FFM), Mini-IPIP constitue un repère pour l'étude de la personnalité qui a été validé par (Donnellan *et al.*, 2006).

Cet instrument est composé de 20 questions extraites de Big Five, avec quatre questions pour chacun des cinq traits. Chaque question (ou *item*) de cet instrument est une phrase décrivant un comportement (par exemple, "Je suis serviable et généreux avec les autres"). Les participants sont tenus à indiquer le degré avec lequel cette phrase les décrit comme ils le sont généralement, non pas comme ils veulent paraître.

Bien que le Big Five comprenne cinq traits différents, nous nous intéressons uniquement dans cette étude à l'agréabilité et à la consciencieusité, tel que nous l'avons mentionné plus haut. Par conséquent, seuls les items de ces deux traits ont été inclus dans le questionnaire. Ils comprennent des items tels que "Je sympathise avec les sentiments des autres" (agréabilité) et "Je fais les choses efficacement" (consciencieusité).

Auto-divulgation

L'auto-divulgation est mesurée en s'inspirant de l'instrument de mesure *Attachement vs Détachement* initialement proposé par Cloninger *et al.* (1994). L'instrument comprend 10 questions : cinq sont *positivement formulées* (par exemple, "Je suis ouvert à propos de mes sentiments") et cinq autres sont *négativement formulées* (par exemple, "Je ne parle pas beaucoup").

Nous choisissons cet instrument de mesure pour évaluer l'auto-divulgation car il offre un aperçu d'un certain nombre de dimensions importantes de l'auto-divulgation correspondant à

notre contexte d'interactions sociales en ligne, et particulièrement celles textuelles. De plus, il a été utilisé avec succès dans des travaux antérieurs pour évaluer l'auto-divulgation en ligne (Ellison *et al.*, 2006).

Auto-Présentation

Nous évaluons ce facteur en se basant sur l'instrument des *stratégies d'auto-présentation* (*Self-Presentation Tactics*) proposé par Lee *et al.* (1999). L'instrument se compose de 63 items divisés en deux types de stratégies : *assertives* et *défensives*. Les stratégies **défensives** concernent les comportements non verbaux tels que la stratégie d'évitement (il s'agit d'éviter des situations menaçantes ou des situations de compétition par exemple), tandis que les stratégies **assertives** se rapportent aux comportements verbaux telle que l'idéalisation verbale de soi.

Nous nous focalisons sur les stratégies assertives parce qu'elles incluent des *pratiques verbales négatives* pouvant affecter l'image créée par un utilisateur lors de ses interactions avec les autres, ce qui le rend plus vulnérable à la cyberintimidation. Nous considérons alors les stratégies assertives suivantes : (a) l'*intimidation*, (b) l'*arrogance* (ou *entitlement* en anglais) et (c) le caractère de *rabaisser les autres* (ou *blasting* en anglais).

Un exemple d'un item de stratégies considérées est "Lorsque je travaille sur un projet avec un groupe je fais en sorte que ma contribution semble supérieure à ce qu'elle est". Un autre exemple est "J'exagère les défauts de personnes qui me sont concurrents". Enfin, un exemple d'un item d'intimidation est "Je menace les autres quand je pense que ça va m'aider à obtenir ce que je veux d'eux."

Comportements de l'utilisateur en ligne

Ce facteur se rapporte aux *comportements à risque* et *comportements abusifs* d'un utilisateur lors de ses interactions sociales en ligne. Les items utilisés sont inspirés et adaptés à partir de divers travaux antérieurs sur le comportement et la vie privée en ligne, notamment les travaux de Walker *et al.* (2011). Ceci inclut des items évaluant la vulnérabilité d'un utilisateur comme "Je fais confiance à toute personne en ligne" (comportements à risque), et des items identifiant certains comportements abusifs dans lesquels un utilisateur peut s'engager en ligne par exemple "Je me moque des autres" (comportements abusifs). Pour examiner les facteurs des *comportements à risque* et *comportements abusifs*, les participants indiquent à quelle

fréquence il leur arrive de s'engager dans les différents comportements inclus dans cette étude.

Expérience de cyberintimidation

L'expérience de cyberintimidation est mesurée en utilisant une version modifiée de l'instrument de cyberintimidation développé par Walker *et al.* (2011) et adapté au contexte de l'interaction sociale en ligne. Cette variable comprend des items de *perpétration d'actes de cyberintimidation* ainsi que ceux de *victimisation*.

Nous avons demandé aux répondants d'indiquer à quelle fréquence ils avaient reçu ou vécu l'un des quatre items suivants en ligne : (1) *une personne diffusant une rumeur sur vous et sabotant votre réputation*, (2) *une personne affichant des informations embarrassantes sur vous sans votre permission*, (3) *une personne prenant un message privé que vous lui avez envoyé et le transmettant à quelqu'un d'autre ou le publiant où les autres pourraient le voir*, et (4) *une personne vous envoyant des messages, feedbacks ou des commentaires insultants et offensifs (y compris les taquineries excessives ou le sarcasme) afin de vous humilier*.

Nous avons également demandé aux répondants d'indiquer comment ils réagissent à un tel comportement en sélectionnant toutes les options auxquelles ils en ont eu recours. Les options incluent : (a) *répondre au comportement négatif avec le même comportement*, (b) *se retirer de l'environnement en ligne*, (c) *confronter la personne en ligne (insulte, intimidation, menace, etc.)*, (d) *confronter la personne face à face*, (e) *rompre le contact ou bloquer la personne*, (f) *changer le nom d'utilisateur ou supprimer le profil*, (g) *discuter le problème en ligne pour obtenir un soutien*, (h) *ignorer*, (i) *non applicable* et (j) *autres* pour en ajouter d'autres options.

Après avoir présenté la méthodologie et les instruments utilisés dans cette étude, il est question dans la prochaine section de présenter les résultats obtenus.

7.4. Résultats

Le modèle théorique proposé dans cette recherche (figure 27) suggère l'utilisation des équations structurelles. Adoptant la démarche en deux étapes recommandée par Anderson et Gerbing (1988), nous présentons, dans un premier temps, le *test des modèles de mesure* puis, dans un deuxième temps, le *test du modèle structurel*. Mais avant cela, nous présentons un bref aperçu des résultats obtenus.

7.4.1. Présentation des résultats préliminaires

Une première observation des items de victimisation indique que 45.7% des personnes interrogées ont déclaré avoir reçu des messages et des commentaires insultants et offensifs, y compris des taquineries excessives et du sarcasme (avec 20.3% rarement, 12.2% occasionnellement, 9.7% fréquemment et 3.5% très fréquemment). À cela s'ajoute 32.7% des répondants qui ont indiqué avoir été victimes de propos diffamatoires et sabotage de réputation. Suite à cela, environ un répondant sur deux (67%) a indiqué qu'ils étaient victimes de cyberintimidation au moins une fois pendant les 12 derniers mois. En examinant l'âge des victimes, nous constatons que les personnes dans le groupe d'âge de [45-54] ont rapporté le plus haut pourcentage de victimisation (40.6%) suivi par ceux dans le groupe de [25-34] (39.6%).

Ces résultats sont relativement surprenants par rapport à ce qui a été rapporté dans la littérature indiquant que ce sont les adolescents qui ont le plus haut pourcentage de victimisation, car ils passent beaucoup de temps sur internet et en particulier sur les sites de réseaux sociaux (Peluchette *et al.*, 2015).

Bien que la plupart des répondants aient affirmé qu'ils ne seraient pas susceptibles de commettre tous les cinq types de comportements à risque inclus dans cette étude, environ un sur trois des victimes (31.9%) ont admis qu'ils avaient réagi à la cyberintimidation avec le même comportement. Toutefois, une exploration de la variable de perpétration d'actes de cyberintimidation a démontré que seulement 3% ont déclaré être des intimidateurs, malgré que 30.8% et 28.8% des participants aient admis commettre des comportements abusifs tels que "faire plus des critiques négatives en ligne qu'en présence physique" et "se moquer des autres". Bien que ces résultats puissent paraitre contradictoires, ils sont compatibles avec les conclusions de Hinduja et Patchin (2013) qui ont trouvé que la majorité des utilisateurs s'engageant dans des comportements abusifs ne savaient pas ou du moins n'avouaient pas que ce qu'ils faisaient était de la cyberintimidation. Cela nous amène à discuter le manque de définition et l'ambiguïté qui entoure la cyberintimidation, qui sera détaillé dans la section discussion.

Avant cela, passons au test de modèles de mesure qui constitue la première étape de l'approche de test proposée par Anderson et Gerbing (1988).

7.4.2. Test des modèles de mesure

Dans cette étape, des *analyses factorielles exploratoires* (AFE) et *confirmatoires* (AFC) ont été effectuées pour vérifier la validité des modèles de mesure. **La première analyse,** l'AFE**,** permet de découvrir l'existence éventuelle de *facteurs sous-jacents* synthétisant l'information contenue dans les *variables mesurées* (Tabachnick *et al.*, 2001). En revanche, L'**analyse confirmatoire** sert à déterminer la pertinence du modèle hypothétique par rapport à l'échantillon (Tabachnick *et al.*, 2001).

Pour l'AFE, une *analyse en composantes principales* avec *rotation Varimax* a été sélectionnée car on s'attendait à ce que les facteurs ne soient pas corrélés. La rotation Varimax permet de faire en sorte que pour chaque facteur, il y ait peu de valeurs de saturation factorielles (*loadings*) élevées, et beaucoup de faibles. Cela veut dire que les variables initiales (mesurées par les questions) seront surtout associées à l'un des facteurs (Kaiser et Specker, 1956). Pour cela, nous fixons un seuil de 0.35 au-delà duquel une saturation factorielle (loading) est considérée comme étant importante. Les résultats de l'analyse exploratoire ont permis la suppression de 2 items (ou questions) dans chacun des facteurs «comportements à risque», «comportements abusifs» et «victimisation» en raison de leurs faibles contributions dans la variance des facteurs associés. Tel que présenté dans la table 16, tous les items conservés ont des saturations factorielles supérieures à 0.35 avec un minimum de 0.369 pour l'item CBP1 et un maximum de 0.956 pour l'item SDC1.

Afin de confirmer les résultats obtenus dans l'analyse exploratoire, des analyses factorielles confirmatoires ont été réalisées (avec IBM SPSS Statistics 22 et IBM SPSS Amos 22). Cela revient, selon Anderson et Gerbing (1988), à évaluer la *validité* et la *fiabilité* du modèle de l'étude en deux étapes :

- *validité convergente* : consiste à s'assurer que les items n'ont pas des corrélations élevées avec d'autres facteurs que ceux avec lesquels ils doivent théoriquement être reliés
- *validité discriminante :* consiste à s'assurer que les facteurs sont statistiquement différents.

Pour déterminer la **première étape** de la validité convergente, nous utilisons le test de Fornell et Larcker (1981) qui consiste à considérer la *variance moyenne extraite* (AVE ou Average Variance Extracted en anglais). Ce test mesure la quantité de la variance capturée par le

facteur en relation avec la quantité de variance attribuée à l'erreur de mesure. Pour qu'il soit jugé adéquat, les AVE doivent être égaux ou supérieurs à 0.5. Dans notre cas, la table 16 montre que la plupart des AVE obtenus sont satisfaisants ou tolérables.

Toujours dans l'étape de la validité convergente, il convient d'évaluer également la fiabilité globale de chaque facteur en se basant sur le *coefficient de fiabilité composite* (CR pour *Composite Reliability*). Ce **coefficient de fiabilité composite** représente la proportion de variance expliquée par le facteur dans un ensemble de questions observées, ce qui fournit une estimation plus précise de la fiabilité que le *coefficient alpha de Cronbach* également utilisé pour évaluer la cohérence interne d'un facteur (Raykov, 1997). Le **coefficient alpha** entraîne souvent une précision moins bonne de la fiabilité parce qu'il suppose qu'un facteur explique une variance comparable pour chaque question connexe. En général, des valeurs CR et alpha de 0.70 ou plus suggèrent une fiabilité satisfaisante pour les questions composées d'un facteur (Fornell et Larker, 1981).

Tel qu'illustré dans la table 16, pour presque tous les facteurs, les valeurs alpha de Cronbach varient entre 0.70 et 0.89 et les valeurs de la fiabilité composite CR sont supérieures aux valeurs recommandées de 0.70 à l'exception du facteur «comportements à risque». Les valeurs de ce dernier sont légèrement en dessous des seuils (avec alpha de 0.686 et CR de 0.651), mais restent tolérables.

Quant au facteur «perpétration», en raison de la taille limitée des participants dans l'échantillon étudié qui ont admis être des intimidateurs (seulement 3% des participants), les valeurs de saturations factorielles, CR et AVE sont très faibles. Ainsi, ce facteur ne sera pas considéré dans le reste du chapitre.

Table 16 – Cohérence interne des facteurs

Facteurs	Items	Saturations factorielles standardisées	CR	AVE	Alpha
Agréabilité (AGR)	**AGR1**	0.729	0.842	0.573	0.835
	AGR2	0.773			
	AGR3	0.664			
	AGR4	0.808			
Conscienciosité (CST)	**CST1**	0.570	0.790	0.494	0.788
	CST2	0.772			
	CST3	0.589			
	CST4	0.847			
Auto-Divulgation (SDC)	**SDC1**	0.956	0.897	0.687	0.898
	SDC2	0.941			
	SDC3	0.608			
	SDC4	0.606			
Auto-Présentation (SPT)	**SPT1**	0.677	0.814	0.524	0.813
	SPT2	0.639			
	SPT3	0.788			
	SPT4	0.749			
Comportements à risque (RSB)	**RSB1**	0.710	0.651	0.483	0.686
	RSB2	0.573			
	RSB3	0.534			
Comportements abusifs (ABB)	**ABB1**	0.576	0.849	0.740	0.841
	ABB2	0.794			
	ABB3	0.942			
	ABB4	0.571			
Victimisation (CBV)	**CBV1**	0.574	0.779	0.638	0.724
	CBV2	0.914			
Perpétration (CBP)	**CBP1**	0.369	0.498	0.357	0.722
	CBP2	0.760			

La **deuxième étape** de l'évaluation est la **validité discriminante** des items et des facteurs. Il s'agit de vérifier que la variance partagée entre un facteur et tout autre facteur dans le modèle est inférieure à la variance que partage le facteur avec ses items (Fornell et Larcker, 1981). La validité discriminante signifie que *deux facteurs différents théoriquement* sont également *distincts dans la pratique*. Cela revient à démontrer que les éléments hors diagonales (corrélation des facteurs) doivent être inférieurs ou égaux aux valeurs racines carrées des AVE portées en diagonale et mises en gras dans la table 17.

Table 17 – Matrice de corrélation des facteurs et racine carrée de l'AVE

Facteurs	AGR	CST	SDC	SPT	RSB	ABB	CBV
Agréabilité (AGR)	**0.757**						
Conscienciosité (CST)	0.198	**0.703**					
Auto-Divulgation (SDC)	0.262	-0.211	**0.829**				
Auto-Présentation (SPT)	-0.322	-0.295	0.268	**0.724**			
Comportements à risque	-0.119	-0.473	0.500	0.459	**0.695**		
Comportements abusifs	-0.262	-0.328	0.288	0.622	0.505	**0.860**	
Victimisation (CBV)	-0.128	-0.235	0.269	0.403	0.675	0.400	**0.799**

Tel qu'illustré dans la table ci-dessus, la validité discriminante est démontrée. Après avoir démontré les validités convergente et discriminante de notre modèle, nous procédons à l'étape du test du modèle structurel.

7.4.3. Test du modèle structurel

Le modèle d'équations structurelles (MES) précédemment présenté dans la figure 27 a été testé au moyen du logiciel IBM SPSS Amos 22. Afin d'évaluer dans quelle mesure le modèle théorique proposé reproduit les données observées, nous considérons les indices de la qualité d'ajustement suivants :

- **GFI** (pour *Goodness of Fit Index*) : une mesure de l'ajustement entre le modèle hypothétique et la matrice de covariance observée
- **GFI ajusté** (pour *Adjusted GFI*) : une mesure qui corrige le GFI affecté par le nombre d'indicateurs de chaque variable latente
- **Khi-carré ou χ^2** : un test statistique permettant de comparer la matrice de covariances prédite par le modèle proposé avec celle que donnerait un modèle saturé qui prédirait parfaitement les données observées
- **Erreur d'approximation quadratique moyenne** (ou RMSEA pour *Root Mean Square Error of Approximation*) : un indicateur de la taille de corrélations entre résidus standardisés. Il constitue avec χ^2 une mesure globale d'ajustement

Les résultats des tests d'ajustement du modèle global d'équations structurelles ainsi que celui obtenu précédemment dans l'analyse factorielle confirmatoire (AFC) sont présentés dans la table 16. Les valeurs des coefficients GFI et AGFI, respectivement de 0.837 et 0.796, sont proches des standards couramment acceptés de 0.9 et 0.8 respectivement. La valeur du

coefficient RMSEA (0.089) est quant à elle légèrement supérieure à la norme couramment admise comme seuil de 0.08. Enfin, compte tenu de la sensibilité de χ^2 à la taille de l'échantillon (χ^2 augmente avec la taille de l'échantillon), nous utilisons dans cette étude, le χ^2 / degré de liberté (χ^2 /dl), comme suggéré par Hair *et al.* (2006). La valeur obtenue de 5.132 est légèrement supérieure à la limite suggérée de 5, tel qu'illustré dans la table 18.

Table 18 – Valeurs de AFC et MES des indices d'ajustement du modèle

	χ^2 /dl	GFI	AGFI	RMSEA
AFC	4.000	0.875	0.832	0.076
MES	5.132	0.837	0.796	0.089
Seuils recommandés	< 5	> 0.90	> 0.80	< 0.08

L'ensemble des résultats sont compatibles avec les valeurs tolérées dans la littérature. Il semble dès lors envisageable d'effectuer l'analyse des résultats du modèle de relations structurelles.

L'examen de la valeur des coefficients obtenus et de leur degré de signification, présentés au sein de la table 19 et la figure 29, permet de vérifier l'existence de relations entre les facteurs du modèle conceptuel proposé.

Table 19 – Résultats de test d'hypothèses

Hypothèse	Estimation	p-value	État de l'hypothèse	
AGR → ABB	-0.196	0.001	H1	soutenue
CST → ABB	-0.102	0.021	H2	soutenue
ABB → CBV	-0.045	0.525	H3	non soutenue
SDC → RSB	0.398	0.001	H4	soutenue
SPT → RSB	0.543	0.001	H5	soutenue
RSB → ABB	0.590	0.001	H6	soutenue
RSB → CBV	0.694	0.001	H7	soutenue

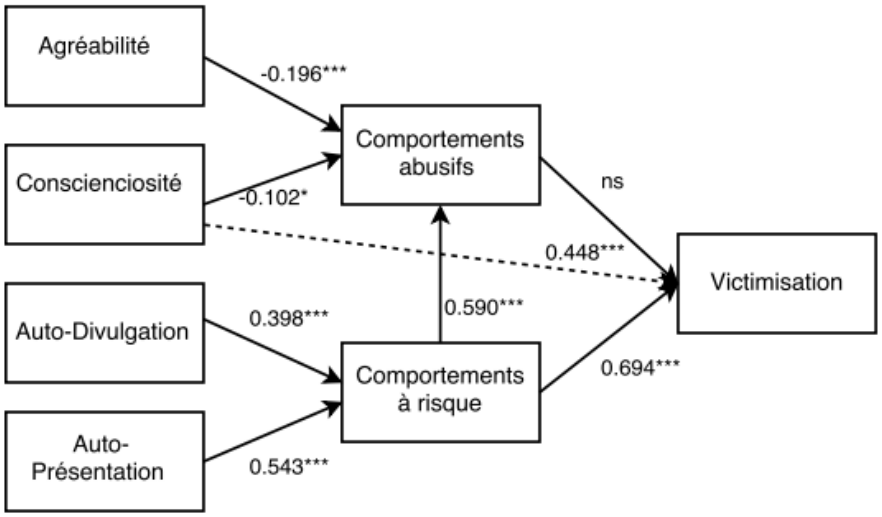


Figure 29 – Modèle final estimé de la victimisation

(*, p<0.05; **, p<0.01; ***, p<0.001; ns, non significatif)

Toutes les hypothèses posées sont significatives à l'exception de H3 qui explore la corrélation entre le facteur « comportements abusifs » et le facteur « victimisation ». Comme cette hypothèse n'est pas soutenue sur la base des résultats obtenus, aucune conclusion ne peut être tirée à propos d'une hypothèse alternative. Cependant, une analyse plus approfondie des données des *intimidateurs-victimes* (ceux qui ont indiqué répondre à la cyberintimidation par le même comportement) a démontré des corrélations significatives entre «comportements à risque» et «comportements abusifs» tel qu'illustré dans la figure 30. Il a été également constaté que les « comportements abusifs » sont un fort prédicteur de la « perpétration » d'actes de cyberintimidation avec un coefficient de 0.477. Ces derniers résultats sont présentés dans la figure 30 illustrant les coefficients du modèle structurel de la perpétration d'actes de cyberintimidation.

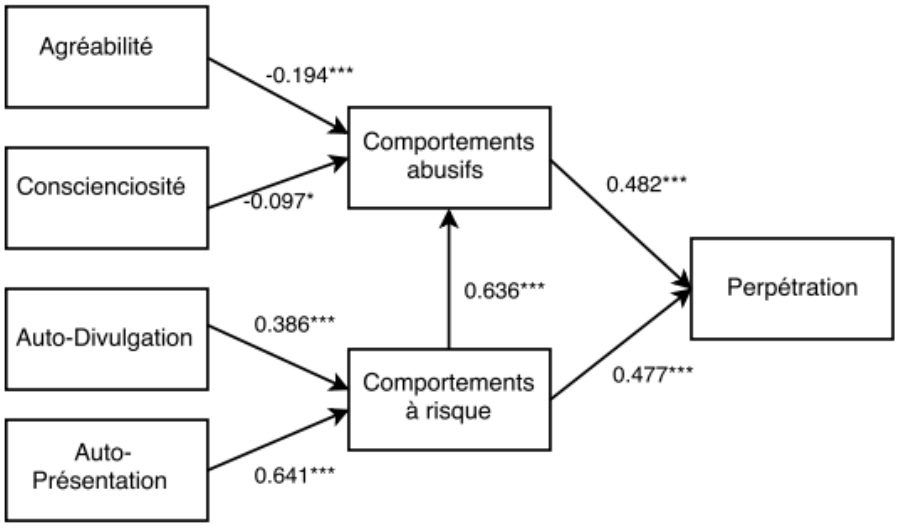


Figure 30 – Modèle structurel de la perpétration d'actes de cyberintimidation

(*, p<0.05; **, p<0.01; ***, p<0.001; ns, non significatif)

Dans le modèle de la figure 30, toutes les hypothèses sont statistiquement significatives. L'hypothèse H3 est également soutenue avec un coefficient assez significatif de 0.482, démontrant la forte corrélation entre le comportement abusif et la perpétration d'actes de cyberintimidation. Cela veut dire que si un utilisateur s'est engagé au moins une fois dans un comportement abusif, il a tendance à répéter le même comportement abusif plusieurs fois ce qui devient une cyberintimidation.

Comme nous avons pris en compte dans ce modèle, les données des répondants admettant être intimidateurs-victimes, cette hypothèse s'est trouvée confirmée. Dans les faits, les répondants se sentaient plus à l'aise d'admettre s'engager dans la cyberintimidation comme une réaction et un moyen de se défendre, parce que dans ce cas-ci leur comportement semble être moins négatif que d'être de pures intimidateurs.

Les modèles rapportés dans les figures 29 et 30 laissent apparaitre des corrélations significatives entre l'auto-divulgation et les comportements à risque ainsi qu'entre l'auto-présentation et les comportements à risque avec des coefficients respectifs de 0.398 et 0.543. À cela s'ajoute la corrélation assez significative de 0.694 entre les comportements à risque et la victimisation. Cela confirme nos hypothèses de recherche postulant que l'auto-divulgation, l'auto-présentation (négative) étant des pratiques risquées ont un grand rôle à jouer dans la victimisation en rendant l'utilisateur plus vulnérable.

D'un autre côté, les corrélations négatives, moins grandes mais significatives, entre l'agréabilité et les comportements abusifs (0.196), d'une part, et la conscienciosité et les comportements abusifs (0.102), d'une autre part, signifient que les individus abusifs ont généralement de faibles scores d'agréabilité et de conscienciosité comme nous l'avons supposé. Ceci étant dit, la considération de ces deux facteurs dans l'évaluation de l'aspect psychologique de la confiance d'un utilisateur dans notre recherche semble être validée.

Enfin, les résultats de cette étude révèlent la prévalence de la victimisation (voir figure 29) ainsi que la perpétration d'actes de cyberintimidation (voir figure 30) dans les interactions sociales en ligne. Il est question dans la section suivante de discuter ces résultats et leur impact sur les interactions entre apprenants dans les contextes informels d'apprentissage.

7.5. Discussion

Bien que de plus en plus de chercheurs sont sensibilisés à la cyberintimidation chez les adultes, force est de constater que les connaissances sont encore insuffisantes pour bien en saisir la portée et comprendre les enjeux qui s'y rattachent. Le fait que cette étude ait été basée sur un échantillon relativement important de différents groupes d'âge fournit une preuve que la cyberintimidation est un problème sérieux pouvant toucher n'importe qui. Au meilleur de notre connaissance, cette étude est la première à examiner de près la prévalence du risque de la cyberintimidation (victimisation ainsi que perpétration d'actes de cyberintimidation) chez les adultes issus de différents milieux étant donné que les participants ont été recrutés sur MTurk (voir table 15). Néanmoins, les comportements de cyberintimidation entre adultes demandent à être étudiés davantage, surtout que la littérature s'est intéressée plus à son étude chez les enfants et les adolescents (Sampasa-Kanyinga et Hamilton, 2015).

Nous n'avons pas considéré un groupe d'âge bien déterminé dans cette étude parce que notre recherche s'intéresse à étudier les contextes d'apprentissage social informel où différents individus de différents âges interagissent et coopèrent afin de poursuivre des buts d'apprentissage individuels ou collaboratifs.

Les résultats indiquent que les prédicteurs les plus puissants de la victimisation sont particulièrement *la divulgation des contenus négatifs* sur soi et sur les autres avec 57.8% et 21.8% des participants respectivement. Conformément aux conclusions de Peluchette *et al.* (2015), il semble que la mauvaise auto-présentation d'un individu et son comportement

d’auto-divulgation influencent son image et identité sociales ce qui le rend aussi vulnérable à la cyberintimidation. En effet, les individus ne peuvent pas réaliser que la divulgation et le partage de certains contenus peuvent susciter des commentaires et des remarques abusifs et offensifs de la part d'autres utilisateurs.

En réaction, la victime peut s’engager à son tour dans un comportement abusif afin de se défendre. Cela a été confirmé dans notre étude par 31.9% des répondants qui ont déclaré avoir réagi en réponse à la cyberintimidation par le même comportement (intimidation, insulte, menace, etc.). De plus, la grande corrélation entre le comportement à risque et le comportement abusif confirme ce résultat et explique la prévalence de ce phénomène. Bien qu'il ne soit pas la meilleure façon de se défendre, il semble que la majorité des individus s’engageant dans des comportements à risque finissent par être abusifs. Dans un contexte d’apprentissage social informel, cela signifie que **l’interaction pourrait ne plus être un moyen pour coopérer et s’entraider**, mais plus pour être intimidé et s’engager dans des comportements abusifs, ce qui *omet toute opportunité d’apprentissage et de coopération entre apprenants*.

Cette constatation est d'une grande importance et rend l'intervention pour minimiser et éradiquer la cyberintimidation très urgente. Les solutions proposées dans la littérature qui ont mis en œuvre des techniques pour **signaler la cyberintimidation** tels que (Cohen *et al.*, 2014) semblent être inopérantes : d’une part parce que le *mal a déjà été fait* et que l’utilisateur a été intimidé en lisant le message ou feedback négatif et abusif et d’autre part parce que la victime, connaissant généralement son harceleur (Dadvar *et al.*, 2012), peut s’engager dans l’intimidation comme réaction. Ceci étant dit, notre solution de détecter et de supprimer les feedbacks négatifs et intimidants a l’avantage de *protéger la vie privée* de l’utilisateur (quand il n’est pas confronté aux feedbacks intimidants de ses pairs) et de *minimiser la prévalence* de la cyberintimidation puisque nous supprimons ces feedbacks au lieu de les envoyer à l’utilisateur.

Les résultats de cette étude ont des implications importantes pour la compréhension de la divulgation et de comportements à risque en ligne. Ceci est fortement nécessaire dans le contexte d'éducation vu que la cyberintimidation entre étudiants aboutit parfois à des résultats tragiques (West, 2015). Comme les outils d’interaction sociale sont intégrés dans les contextes d'apprentissage informel et formel, il est indispensable de créer un environnement

d'apprentissage préservant la vie privée des apprenants et favorisant ainsi la coopération et l'entraide.

Cette étude a quelques limitations qui devraient être reconnues. La **première** est l'utilisation d'Amazon Mechanical Turk comme méthode de collecte. En fait, même si nous disposons relativement d'un important échantillon (N = 520), les données ont compris des participants de différents milieux et cultures. Ainsi, il est difficile de savoir si les résultats de l'étude seraient bien généralisés à d'autres contextes ou à des échantillons variés.

Une **autre limite** de notre étude est le biais de *désirabilité sociale* due au questionnaire d'auto-évaluation utilisé. Comme expliqué par King et Bruner (2000), les participants ont tendance à choisir des réponses qu'ils jugent être plus socialement souhaitables ou acceptables. Bien que les participants aient rempli le sondage anonymement, la sous-déclaration des comportements abusifs et de cyberintimidation ont peut-être pu se produire en raison de ce biais.

Enfin, il serait impossible de considérer tous les facteurs de la cyberintimidation dans un modèle de recherche. Des études antérieures ont obtenu des résultats significatifs en étudiant les effets de plusieurs facteurs cognitifs (Vivolo-Kantor *et al.*, 2014), émotionnels, psychologiques et sociaux (Berne *et al.*, 2013) sur la cyberintimidation. Tous ces facteurs et résultats devraient être utilisés pour développer des solutions à cette menace sociale, notamment lorsqu'un nombre de plus en plus croissant de personnes déclarent y être impliquées que ce soit comme intimidés ou intimidateurs.

Bien que nous nous sommes focalisés sur la cyberintimidation en particulier, qui est à la fois un risque et une conséquence de l'auto-divulgation, les risques potentiels en termes de vie privée dans les interactions sociales sont nombreux et divers. Étant donné que les autres types de risques sont difficiles à observer et à évaluer (par exemple le vol d'identité), nous avons choisi d'étudier ce phénomène dans notre recherche vu ses conséquences graves dans un contexte d'apprentissage. Les futurs travaux devraient envisager d'étudier d'autres risques d'atteinte à la vie privée afin de mettre en place des solutions de prévention et de protection.

7.6. Conclusion

Pour conclure, les résultats de cette étude corroborent la prévalence de la cyberintimidation et indiquent que ce phénomène indésirable est en train de devenir un problème mondial. En explorant le rôle du comportement d'auto-divulgation et d'auto-présentation des victimes dans

leur victimisation, nous visons à encourager les chercheurs à considérer l'effet de ces facteurs importants, mais peu étudiés, dans la prévalence de la cyberintimidation; particulièrement depuis que les sites de médias sociaux ont été mis en place pour encourager les utilisateurs à se livrer à plus d'auto-divulgation et d'auto-présentation. Bien qu'il n'y ait pas de solution magique pour éradiquer la cyberintimidation, au meilleur de nos connaissances, un compromis entre l'auto-divulgation, l'auto-présentation en ligne et la protection de la vie privée pourrait être trouvé en intégrant des facteurs sociaux tels que la confiance et la gestion de la réputation comme nous l'avons proposé dans cette recherche. La considération de ces facteurs pourrait contribuer à réduire la cyberintimidation ou du moins à protéger les individus de ses conséquences. La compréhension des facteurs soutenant la cyberintimidation et ceux permettant de la prédire est d'une importance significative. Ceci pourrait aboutir au développement des solutions appropriées afin de préserver la vie privée des individus et de minimiser les occurrences de ce phénomène.

Chapitre 8 : Conclusions

De l'apprentissage collaboratif jusqu'aux environnements personnels d'apprentissage, en passant par les communautés et les réseaux d'apprentissage, le dénominateur commun est l'interaction et la construction collective de connaissances qui se développent avec les évolutions technologiques et sociales. Dans le contexte actuel de socialisation numérique, de nombreux outils sont utilisés pour soutenir les activités collaboratives et les interactions entre apprenants. Tout en reconnaissant le rôle important que jouent ces outils pour soutenir l'apprentissage d'aujourd'hui, plus précisément dans les contextes informels, la littérature portant sur l'analyse des interactions entre apprenants montre les limites de ces outils et de leur usage pour l'apprentissage. Ces limites sont principalement liées au manque de structuration des flux d'interactions dus à la dynamique différente des interactions mises en place dans ces contextes d'apprentissage et à l'absence des rôles précis dans les interactions; ce qui donne l'impression de désordre et augmente la confusion des apprenants et leur charge cognitive.

De plus, l'usage de ces outils de socialisation a apporté de nouvelles pratiques pouvant gêner la coopération et l'apprentissage. Nous parlons plus précisément de la divulgation de données personnelles et les risques inhérents en matière de vie privée. Pour obtenir des bénéfices cognitifs des interactions, il apparaît nécessaire de créer un espace interactionnel socio-affectif favorisant la coopération entre apprenants et soutenant l'apprentissage social, par l'utilisation de scénarios qui structurent l'interaction et attribuent des rôles aux différents acteurs impliqués. C'est dans cette perspective que nous proposons, dans cette thèse, le gestionnaire de vie privée permettant de structurer et réguler les interactions entre apprenants dans les situations d'apprentissage social informel.

8.1. Contributions

Dans une remise en question du besoin de considérer la vie privée dans les interactions sociales, qui sont généralement centrées sur la divulgation de données personnelles et la visibilité sociale, nous proposons un cadre visant à gérer la protection de la vie privée tout au long de l'interaction et sur trois niveaux correspondant à nos trois contributions dans cette thèse.

Notre première contribution a été de remédier aux limites actuelles des contextes d'apprentissage social informel dans la modélisation des activités d'aide et interactions entre

apprenants. Pour cela, nous avons proposé un module de sélection des pairs afin d'aider les apprenants à trouver des pairs appropriés pour répondre à leur besoin d'apprentissage. Le processus de sélection tient compte des variables d'apprentissage pour garantir une réponse au besoin d'apprentissage, mais il considère aussi des variables sociales nécessaires pour instaurer un climat socio-affectif favorable à la coopération et préservant la vie privée. Ainsi, nous avons défini un *score de confiance* pour chaque apprenant.

Ce score peut renseigner sur la personnalité d'un apprenant de point de vue attitude vis-à-vis de l'entraide et de la coopération. En particulier, une valeur élevée de score de confiance, plus précisément **un score de personnalité** mesuré en se basant sur les deux traits d'*agréabilité* et de *conscienciosité*, indique que l'apprenant est *coopératif*, *agréable* et *digne de confiance*. Cela veut dire que cet apprenant n'est pas *abusif* et donc il peut être sélectionné pour fournir l'aide à ses pairs. Le score de confiance peut également aider à suivre les contributions et les feedbacks d'un apprenant en réponse aux demandes d'aide de ses pairs, dans la mesure où l'apprenant qui fournit des feedbacks utiles aurait de meilleurs scores que ceux qui donnent des feedbacks non pertinents.

Bien que nous ayons mené une simulation pour évaluer le fonctionnement du module proposé, les résultats de tests ont montré que le score de confiance a permis de faire de meilleures sélections de pairs. L'évaluation de sélections a été faite en se basant sur les scores attribués aux feedbacks fournis par les pairs. Bien que cette approche d'évaluation présente quelques limites que nous discutons plus tard, elle est compatible avec notre définition d'un *tuteur approprié* comme celui qui fournit un feedback pertinent de point de vue d'apprentissage et vie privée.

Notre **deuxième contribution** a été de proposer un module de divulgation des données personnelles en vue de résoudre le paradoxe de vie privée. Pour ce faire, nous avons considéré les préférences de divulgation de l'apprenant demandant l'aide (1), anonymisé ses données (2), étendu une approche de quantification de divulgation pour évaluer les risques potentiels (3) et défini un modèle de décision de divulgation intégrant de nombreux facteurs, dont la confiance des apprenants et l'utilité des données divulguées (4). L'intégration de ces facteurs dans un module de décision a permis d'adapter la divulgation aux contextes et besoins d'apprentissage et de distinguer des niveaux différents de divulgation. Il a également permis de mettre en œuvre une nouvelle conceptualisation de la vie privée en tant que processus de

négociation considérant à la fois les préférences de divulgation de l'apprenant et les exigences de protection de sa vie privée.

La capacité d'estimer automatiquement les risques potentiels de la divulgation de données personnelles et de prendre des décisions en matière de vie privée fournit une méthode potentiellement utile pour les apprenants, leur permettant de réduire la disparité entre préoccupations de vie privée et comportements de divulgation (paradoxe de vie privée) d'une part, et d'éviter de s'engager dans une divulgation excessive ou une interaction risquée.

Notre troisième contribution dans cette recherche a été de proposer un module d'analyse automatique des interactions visant à aider l'apprenant à trouver les contenus pertinents répondant à son besoin d'apprentissage et préservant sa vie privée. Le module proposé se base sur des techniques d'analyse des sentiments et d'analyse sémantique latente pour écarter les feedbacks pouvant influencer négativement l'apprentissage et instaurant un climat interactionnel non favorable à la coopération et l'entraide entre apprenants. Pour cela, nous avons réalisé *deux études expérimentales*. Dans **la première**, nous avons étudié la performance des algorithmes d'analyse des sentiments dans la classification des interactions en langage naturel.

Les modèles d'analyse des sentiments ont été étendus pour considérer l'état émotionnel de l'apprenant en vue de soutenir la présence sociale qui s'exprime faiblement dans les interactions entre apprenants ce qui peut causer l'incertitude chez ces derniers. Plus précisément, notre approche consiste à utiliser dans un premier temps des algorithmes d'apprentissage machine sur des données issues d'interactions sociales entre apprenants extraits des forums de discussion et de les valider ensuite pour évaluer les résultats.

La deuxième étude expérimentale avait pour objectif d'examiner la sensibilité de l'analyse sémantique latente à la divulgation des données. Pour cela, nous avons étudié différents modèles de LSA en considérant trois paramètres pouvant influencer sa performance : *la pondération*, *la réduction de dimensionnalité* et *la mesure de similarité*. Ensuite nous avons soumis ces modèles à l'évaluation de deux experts humains.

L'analyse des résultats nous a permis de montrer la performance du module proposé dans la classification des feedbacks et la suppression de divulgation non intentionnelle des données personnelles par rapport aux jugements humains. L'analyse automatique des interactions est nécessaire dans le contexte d'apprentissage social informel pour aider l'apprenant à repérer les contenus pertinents dans les interactions sans augmenter sa charge cognitive.

La validation pratique (avec de vrais apprenants) d'un cadre, comme le nôtre, demande du temps, des ressources financières, matérielles et humaines que nous ne possédons pas. En effet, cette validation requiert l'élaboration d'un environnement complet d'apprentissage, la sollicitation de participation des apprenants aux interactions, et l'observation et la collecte d'informations sur une longue durée de temps.

Pour ces raisons, et dans le but de valider globalement l'utilité du cadre de protection proposé dans cette thèse, nous avons procédé à **l'étude du cas de cyberintimidation** qui représente un risque potentiel dans les interactions sociales en ligne. Pour cela, nous avons mené une étude empirique visant à examiner les corrélations entre les différents facteurs de risque et de protection. Parmi les corrélations examinées, nous pouvons citer à titre d'exemple la relation entre la confiance et les comportements abusifs dans les interactions sociales en ligne et le rôle de cette variable de confiance dans la protection des risques de l'auto-divulgation.

Les résultats de cette étude ont montré la prévalence de la cyberintimidation dans les interactions, tant pour la victimisation (45.7% des répondants ont indiqué avoir été victimes au moins une fois pendant les 12 derniers mois) que pour la perpétration d'actes de cyberintimidation (31.9% des participants dans l'étude) ce qui montre la nécessité de préserver la vie privée dans les interactions sociales. En effet, la prévalence de ce phénomène indésirable peut créer des interactions sociales non productives et omettre toute opportunité d'apprentissage ou de coopération entre apprenants.

L'étude a également révélé que l'auto-divulgation, même si elle ne peut être considérée comme une cause directe de la victimisation, contribue à accroitre sa probabilité. Ainsi, le fait d'adapter la divulgation aux besoins d'apprentissage peut aider à diminuer les risques; étant donné qu'on ne peut plus espérer arrêter la divulgation des données dans le contexte actuel de socialisation numérique.

8.2. Travaux futurs

De nos jours, socialiser et apprendre sont devenues deux facettes d'une même activité. C'est participer à un processus social par lequel les apprenants exploitent leurs différences de manière constructive pour élaborer et mettre en œuvre des connaissances qui vont au-delà des possibilités individuelles de chacun. Toutefois, les interactions sociales dans les contextes d'apprentissage informel ne peuvent être assimilées à des activités collaboratives ni coopératives. Les connaissances acquises et co-construites à partir des interactions dans ces

contextes sont intégrées dans l'expérience personnelle de l'individu et répondant à un besoin et un objectif individuel d'apprentissage.

L'exploitation de ce type d'apprentissage au sein d'institutions éducatives pourrait être un moyen efficace pour faire rapprocher les apprentissages formel et informel et augmenter ainsi l'engagement et la motivation des apprenants. Il est à noter que pour le moment il n'existe pas de cadre théorique accepté par la majorité des chercheurs pouvant expliquer la conciliation entre les caractéristiques de l'apprentissage social formel et informel sans toutefois perdre le caractère libre et spontané de ce dernier type d'apprentissage.

À cet égard, le cadre proposé dans cette recherche pourrait être intégré dans une plateforme d'apprentissage informel pour soutenir l'apprentissage formel en accompagnant les apprenants à trouver l'aide appropriée et les contenus pertinents tout en préservant leur vie privée.

De plus, le cadre pourrait être étendu en ajoutant *un module d'apprentissage* permettant d'adapter davantage les interactions aux besoins de l'apprenant. En effet, dans la sélection des pairs, nous pouvons mettre en place des critères permettant à l'apprenant ayant besoin d'aide d'affiner ses préférences. Par exemple, si dix pairs ont été sélectionnés pour fournir l'aide dont cinq ayant comme langue le français et les autres parlant d'autres langues, l'apprenant peut spécifier qu'il préfère recevoir des feedbacks de la part des pairs parlant français. Compte tenu des pairs sélectionnés et de la requête, le module apprentissage adapte les sélections aux préférences enregistrées de l'apprenant. Cela permet de personnaliser le feedback, et l'interaction en général, aux préférences et besoins de l'apprenant.

Une autre piste pour étendre le cadre proposé est d'impliquer plus les apprenants dans la décision de protection et de divulgation des données. Dans les faits, le module Décision de divulgation supprime les données moins utiles quand le risque dépasse les seuils prédéfinis. Nous pouvons mettre en place *un module de négociation* de divulgation impliquant l'apprenant ayant besoin d'aide et les pairs sélectionnés. Ces derniers peuvent négocier avec l'apprenant en question l'ensemble des données à divulguer afin de fournir des feedbacks personnalisés. Ce module permet d'adopter une nouvelle conceptualisation de la protection de la vie privée en tant que négociation collective dans laquelle les transformations technologiques et sociales contemporaines peuvent trouver leur place.

En ce qui concerne la protection de la vie privée, la performance du module composition des feedbacks dans l'analyse des interactions pourrait être améliorée afin de diminuer l'erreur de

classification et le taux de suppression de feedbacks en considérant un *nouvel index de divulgation*. Cet index servirait à définir des modèles de divulgation et à les associer à des niveaux de risques différents.

Pour illustrer notre propos, prenons l'exemple suivant : un feedback divulguant des données ne permettant pas de ré-identifier avec précision l'apprenant (par exemple son âge ou son pays) aurait moins de probabilité d'être supprimé qu'un feedback divulguant des données explicitement identifiables (comme le nom ou l'adresse email). Les expressions régulières pourraient être une bonne solution pour mettre en œuvre ce nouvel index de divulgation.

Bibliographie

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Ahmadi, H., Pham, N., Ganti, R., Abdelzaher, T., Nath, S., & Han, J. (2010). *Privacy-aware regression modeling of participatory sensing data.* Paper presented at the Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems.

Aïmeur, E., Brassard, G., & Rioux, J. (2013). Data Privacy: An End-User Perspective.

Aïmeur, E., & Hage, H. (2010). Preserving Learners' Privacy *Advances in Intelligent Tutoring Systems* (pp. 465-483): Springer.

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When Changing the Look of Privacy Policies Affects User Trust: An Experimental Study. *Computers in Human Behavior*.

Alava, S. (2010). Les pratiques en communautique au cœur des apprentissages en ligne. *Questions Vives. Recherches en éducation, 7*(14), 55-70.

Alloing, C., & Pierre, J. (2012). Construire un cadre d'analyse avec les SIC pour comprendre les pratiques et les enjeux de la réputation en ligne (des individus et des organisations).

Amichai-Hamburger, Y. (2012). Reducing intergroup conflict in the digital age. *The handbook of intergroup communication*, 181-193.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin, 103*(3), 411.

Anwar, M., & Greer, J. (2011). Role-and relationship-based identity management for privacy-enhanced E-Iearning. *International Journal of Artificial Intelligence in Education, 21*(3), 191-213.

Artino, A. R., La Rochelle, J. S., & Durning, S. J. (2010). Second-year medical students' motivational beliefs, emotions, and achievement. *Medical education, 44*(12), 1203-1212.

Balsam, P., & Tomie, A. (2014). *Context and learning*: Psychology Press.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*: Prentice-Hall, Inc.

Basse, S. (2003). A Gift of Fire: Social, Legal, and Ethical Issues for Computers and Internet: Prentice Hall, Upper Saddle River, New Jersey.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*(4), 1017-1042.

Bernaud, J.-L. (2008). *Les méthodes d'évaluation de la personnalité-2ème édition*: Dunod.

Berne, S., Frisén, A., Schultze-Krumbholz, A., Scheithauer, H., Naruskov, K., Luik, P., . . . Zukauskiene, R. (2013). Cyberbullying assessment instruments: A systematic review. *Aggression and violent behavior, 18*(2), 320-334.

Bezzi, M. (2010). An information theoretic approach for privacy metrics. *Transactions on Data Privacy, 3*(3), 199-215.

Bezzi, M. (2013). Anonymity measuring device: Google Patents.

Bingham, T., & Conner, M. (2015). *The new social learning*: Association For Talent Development.

Boling, C., & Das, K. (2015). Semantic Similarity of Documents Using Latent Semantic Analysis. *2014 NCUR*.

Borich, G. D., & Tombari, M. L. (1997). *Educational psychology: A contemporary approach*: Longman Publishing/Addison Wesley L.

Butler, R. (2007). Teachers' achievement goal orientations and associations with teachers' help seeking: Examination of a novel approach to teacher motivation. *Journal of Educational Psychology, 99*(2), 241.

Cáceres, R., Cox, L., Lim, H., Shakimov, A., & Varshavsky, A. (2009). *Virtual individual servers as privacy-preserving proxies for mobile devices.* Paper presented at the Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds.

Campan, A., Cooper, N., & Truta, T. M. (2011). On-the-fly generalization hierarchies for numerical attributes revisited *Secure Data Management* (pp. 18-32): Springer.

Candillier, L., Jack, K., Fessant, F., & Meyer, F. (2009). State-of-the-art recommender systems. *Collaborative and Social Information Retrieval and AccessTechniques for Improved User Modeling*.

Casilli, A. A. (2013). Contre l'hypothèse de la «fin de la vie privée». La négociation de la privacy dans les médias sociaux. *Revue française des sciences de l'information et de la communication*(3).

Cavoukian, A. (2011). Privacy by Design: Origins, Meaning, and Prospects. *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards*, 170.

Celma, Ò., Ramírez, M., & Herrera, P. (2005). *Foafing the music: A music recommendation system based on RSS feeds and user preferences.* Paper presented at the in ISMIR.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *CyberPsychology & Behavior, 12*(3), 341-345.

Cleveland-Innes, M., & Campbell, P. (2012). Emotional presence, learning, and the online learning environment. *The International Review of Research in Open and Distributed Learning, 13*(4), 269-292.

Cloninger, C. R., Przybeck, T. R., & Svrakic, D. M. (1994). *The Temperament and Character Inventory (TCI): A guide to its development and use*: center for psychobiology of personality, Washington University St. Louis, MO.

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*.

Cohen, R., Lam, D., Agarwal, N., Cormier, M., Jagdev, J., Jin, T., . . . Rawat, R. (2014). Using computer technology to address the problem of cyberbullying. *ACM SIGCAS Computers and Society, 44*(2), 52-61.

Cointot, J.-C., & Eychenne, Y. (2014). *La Révolution Big data: Les données au coeur de la transformation de l'entreprise*: Dunod.

Cornelius, C., Kapadia, A., Kotz, D., Peebles, D., Shin, M., & Triandopoulos, N. (2008). *Anonysense: privacy-aware people-centric sensing.* Paper presented at the Proceedings of the 6th international conference on Mobile systems, applications, and services.

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev., 55*, 93.

Crépin, L., Demazeau, Y., Boissier, O., & Jacquenet, F. (2009). Transaction de données sensibles au sein de systèmes multi-agents hippocratiques. *Revue d'Intelligence Artificielle, 23*(5-6), 621-650.

Dadvar, M., de Jong, F., Ordelman, R., & Trieschnigg, R. (2012). Improved cyberbullying detection using gender information.

De Wever, B., Van Keer, H., Schellens, T., & Valcke, M. (2010). Roles as a structuring tool in online discussion groups: The differential impact of different roles on social knowledge construction. *Computers in Human Behavior, 26*(4), 516-523.

Deerwester, S. C., Dumais, S. T., Landauer, T. K., Furnas, G. W., & Harshman, R. A. (1990). Indexing by latent semantic analysis. *JAsIs, 41*(6), 391-407.

Dejean-Thircuir, C. (2010). Développer des compétences interactionnelles en collaborant à distance. *Revue internationale des technologies en pédagogie universitaire/International Journal of Technologies in Higher Education, 7*(1), 33-46.

Derbali, L., & Frasson, C. (2012). Assessment of learners' motivation during interactions with serious games: a study of some motivational strategies in food-force. *Advances in Human-Computer Interaction, 2012*, 5.

Deswarte, Y., & Gambs, S. (2010). Towards a privacy-preserving national identity card *Data Privacy Management and Autonomous Spontaneous Security* (pp. 48-64): Springer.

Deutsch, M. (1980). Fifty years of conflict. *Retrospections on social psychology, 4677*.

Develotte, C. (2008). Approche de l'autonomie dans un dispositif en ligne: le cas du dispositif Le français en (première) ligne. *Revue japonaise de didactique du français, 3*(1), 37-56.

Doise, W., & Mugny, G. (1981). *Le développement social de l'intelligence* (Vol. 1): InterEditions Paris.

Dong, C., Jin, H., & Knijnenburg, B. P. (2015). *Predicting Privacy Behavior on Online Social Networks.* Paper presented at the Ninth International AAAI Conference on Web and Social Media.

Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The mini-IPIP scales: tiny-yet-effective measures of the Big Five factors of personality. *Psychological assessment, 18*(2), 192.

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014). Presentation on Facebook and risk of cyberbullying victimisation. *Computers in human behavior, 40*, 16-22.

Duplàa, E., & Talaat, N. (2012). Connectivisme et formation en ligne. *Distances et savoirs, 9*(4), 541-564.

Duthoit, E. (2014). *Activités d'aide en situations d'apprentissage: interactions, ressources, instrumentations.* Université Paul Valéry Montpellier 3.

Duthoit, E., Mailles-Viard Metz, S., Charnet, C., & Pélissier, C. (2011). *Entraide en ligne: le cas d'un forum de discussion utilisé en tant que ressource externe au contexte d'apprentissage.* Paper presented at the Actes du colloque" Échanger pour apprendre en ligne (EPAL)". Grenoble.

Dwork, C. (2006). Ask a better question, get a better answer a new approach to private data analysis *Database Theory–ICDT 2007* (pp. 18-27): Springer.

Ellison, N., Heino, R., & Gibbs, J. (2006). Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication, 11*(2), 415-441.

Erdt, M., Fernandez, A., & Rensing, C. (2015). Evaluating Recommender Systems for Technology Enhanced Learning: A Quantitative Survey. *Learning Technologies, IEEE Transactions on, 8*(4), 326-344.

Falchikov, N., & Blythman, M. (2001). *Learning together: Peer tutoring in higher education*: Psychology Press.

Fang, L., & LeFevre, K. (2010). *Privacy wizards for social networking sites.* Paper presented at the Proceedings of the 19th international conference on World wide web.

Fazeli, S., Drachsler, H., Brouns, F., & Sloep, P. (2012). A trust-based social recommender for teachers.

Feidakis, M., Daradoumis, T., & Caballé, S. (2011). *Emotion measurement in intelligent tutoring systems: what, when and how to measure.* Paper presented at the Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference on.

Felt, A., & Evans, D. (2008). Privacy protection for social networking apis. *2008 Web 2.0 Security and Privacy (W2SP'08)*.

Festl, R., & Quandt, T. (2013). Social relations and cyberbullying: The influence of individual and structural attributes on victimization and perpetration via the Internet. *Human Communication Research, 39*(1), 101-126.

Foody, M., Samara, M., & Carlbring, P. (2015). A review of cyberbullying and suggestions for online psychological therapy. *Internet Interventions*.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.

Foucher, A.-L., & Pothier, M. (2007). Aides stratégiques dans un environnement d'apprentissage en FLE. *Alsic. Apprentissage des Langues et Systèmes d'Information et de Communication, 10*(1).

Fung, B., Wang, K., Chen, R., & Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (CSUR), 42*(4), 14.

Garrison, D. R., Anderson, T., & Archer, W. (1999). Critical inquiry in a text-based environment: Computer conferencing in higher education. *The internet and higher education, 2*(2), 87-105.

Giota, K. G., & Kleftaras, G. (2014). The Discriminant Value of Personality, Motivation, and Online Relationship Quality in Predicting Attraction to Online Social Support on Facebook. *International Journal of Human-Computer Interaction, 30*(12), 985-994.

Granjon, F. (2009). Inégalités numériques et reconnaissance sociale. *Les cahiers du numérique, 5*(1), 19-44.

Grosjean, S. (2008). Genèse d'une communauté virtuelle d'apprenants dans le cadre d'une démarche d'apprentissage collaboratif à distance. *Canadian Journal of Learning and Technology/La revue canadienne de l'apprentissage et de la technologie, 33*(1).

Hage, H., & Aïmeur, E. (2009). *The Impact of Privacy on Learners in the Context of a Web-Based Test.* Paper presented at the AIED.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (Vol. 6): Pearson Prentice Hall Upper Saddle River, NJ.

Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (2011). Patterns of risk and safety online. *depth analyses from the EU Kids Online survey of*, 9-16.

Hélou, C., Guandouz, A., & Aïmeur, E. (2012). A privacy awareness system for facebook users. *J. Inf. Secur. Res, 31*, 15-29.

Hemphill, S. A., & Heerde, J. A. (2014). Adolescent predictors of young adult cyberbullying perpetration and victimization among Australian youth. *Journal of Adolescent Health, 55*(4), 580-587.

Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of Youth and Adolescence, 42*(5), 711-722.

Hofer, B. K. (2001). Personal epistemology research: Implications for learning and teaching. *Educational Psychology Review, 13*(4), 353-383.

Hough, P. (2013). *Understanding global security* (Third edition. ed.). Milton Park, Abingdon, Oxon: Routledge.

Isabwe, G. M. N., & Reichert, F. (2013). *Revisiting students' privacy in computer supported learning systems.* Paper presented at the Information Society (i-Society), 2013 International Conference on.

Jézégou, A. (2010). Créer de la présence à distance en e-learning. *Distances et savoirs, 8*(2), 257-274.

Jiang, M., Cui, P., Liu, R., Yang, Q., Wang, F., Zhu, W., & Yang, S. (2012). *Social contextual recommendation.* Paper presented at the Proceedings of the 21st ACM international conference on Information and knowledge management.

John-Steiner, V., & Mahn, H. (1996). Sociocultural approaches to learning and development: A Vygotskian framework. *Educational psychologist, 31*(3-4), 191-206.

Johnson, D. W., Johnson, R. T., & Stanne, M. B. (2000). Cooperative learning methods: A meta-analysis.

Jorge-Botana, G., Luzón, J. M., Gómez-Veiga, I., & Martín-Cordero, J. I. (2015). Automated LSA Assessment of Summaries in Distance Education Some Variables to Be Considered. *Journal of Educational Computing Research*, 0735633115571930.

Kaiser, H., & Specker, H. (1956). Evaluation and comparison of methods of analysis. *Z. anal. Chem, 149*, 46.

Karabenick, S., & Newman, R. (2009). Seeking help: Generalizable self-regulatory process and social-cultural barometer. *Contemporary motivation research: From global to local perspectives*, 25-48.

Kasdali, S. (2014). *Modélisation complexe de l'impact des dispositifs de formation à distance.* Université de Cergy Pontoise.

King, M. F., & Bruner, G. C. (2000). Social desirability bias: A neglected aspect of validity testing. *Psychology and Marketing, 17*(2), 79-103.

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies, 71*(12), 1144-1162.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological bulletin, 140*(4), 1073.

Kulkarni, C., Wei, K. P., Le, H., Chia, D., Papadopoulos, K., Cheng, J., . . . Klemmer, S. R. (2015). Peer and self assessment in massive online classes *Design Thinking Research* (pp. 131-168): Springer.

Lanchantin, T., Simoës-Perlant, A., & Largy, P. (2012). The case of Digital Writing in Instant Messaging: When cyber written productions are closer to the oral code than the written code. *PsychNology Journal, 10*(3), 187-214.

Latzko-Toth, G., & Pastinelli, M. (2014). Par-delà la dichotomie public/privé: la mise en visibilité des pratiques numériques et ses enjeux éthiques. *tic&société, 7*(2).

Law, D. M., Shapka, J. D., Domene, J. F., & Gagné, M. H. (2012). Are cyberbullies really bullies? An investigation of reactive and proactive online aggression. *Computers in human behavior, 28*(2), 664-672.

Le Métayer, D., & Piolle, G. (2010). Droits et obligations à l'ère numérique: protection de la vie privée. *L'usager numérique*, 63-88.

Lee, S.-J., Quigley, B. M., Nesler, M. S., Corbett, A. B., & Tedeschi, J. T. (1999). Development of a self-presentation tactics scale. *Personality and Individual differences, 26*(4), 701-722.

Lee, U., Yi, E., & Ko, M. (2013). *Mobile Q&A: beyond text-only Q&A and privacy concerns.* Paper presented at the Proceedings of CHI.

Levy, N., Cortesi, S., Gasser, U., Crowley, E., Beaton, M., Casey, J., & Nolan, C. (2012). Bullying in a networked era: A literature review. *Berkman Center Research Publication*(2012-17).

Lin, P.-C., Hou, H.-T., Wang, S.-M., & Chang, K.-E. (2013). Analyzing knowledge dimensions and cognitive process of a project-based online discussion instructional activity using Facebook in an adult and continuing education course. *Computers & Education, 60*(1), 110-121.

Lipman, M. (2003). *Thinking in education*: Cambridge University Press.

Liu, N.-F., & Carless, D. (2006). Peer feedback: the learning element of peer assessment. *Teaching in Higher education, 11*(3), 279-290.

Lowenthal, P., Muth, R., & Provenzo, E. (2009). Constructivism. Encyclopedia of the Social and Cultural Foundations of Education (Vol. 1). *Thousand Oaks, CA: Sage Publications Inc. Retrieved July, 30*, 2010.

Malinen, S., & Nurkka, P. (2015). Cultural influence on online community use: a cross–cultural study on online exercise diary users of three nationalities. *International Journal of Web Based Communities, 11*(2), 153-169.

Mangenot, F., & Nissen, E. (2013). Collective activity and tutor involvement in e-learning environments for language teachers and learners. *Calico Journal, 23*(3), 601-622.

Manouselis, N., Drachsler, H., Verbert, K., & Duval, E. (2012). *Recommender systems for learning*: Springer Science & Business Media.

Martínez-Cámara, E., Martín-Valdivia, M. T., Urena-López, L. A., & Montejo-Ráez, A. R. (2014). Sentiment analysis in twitter. *Natural Language Engineering, 20*(01), 1-28.

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior research methods, 44*(1), 1-23.

McCrae, R. R., & Costa, P. T. (1999). A five-factor theory of personality. *Handbook of personality: Theory and research, 2*, 139-153.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125.

Moore, A. W. (2001). Cross-validation for detecting and preventing overfitting. *School of Computer Science Carneigie Mellon University*.

Morando, F., Iemma, R., & Raiteri, E. (2014). Privacy evaluation: what empirical research on users' valuation of personal data tells us. *Internet Policy Review, 3*(2), 1-11.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2011). Disclosure antecedents in an online service context: the role of sensitivity of information. *Journal of service research*, 1094670511424924.

Muller, G. (2006). Privacy and security in highly dynamic systems. *Communications of the ACM, 49*(9), 28-31.

Na, L. (2015). *Personal Learning with Social Media: Reputation, Privacy and Identity Perspectives.* ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE.

Naak, A., Hage, H., & Aimeur, E. (2009). A multi-criteria collaborative filtering approach for research paper recommendation in papyres *E-Technologies: Innovation in an Open World* (pp. 25-39): Springer.

Narciss, S., & Huth, K. (2006). Fostering achievement and motivation with bug-related tutoring feedback in a computer-based training for written subtraction. *Learning and Instruction, 16*(4), 310-322.

Nevin, A. D. (2015). Cyber-Psychopathy: Examining the Relationship between Dark E-Personality and Online Misconduct.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*: Stanford University Press.

Nowakowski, S., Ognjanović, I., Grandbastien, M., Jovanovic, J., & Šendelj, R. (2014). Two Recommending Strategies to Enhance Online Presence in Personal Learning Environments *Recommender Systems for Technology Enhanced Learning* (pp. 227-249): Springer.

Nummenmaa, L., Glerean, E., Viinikainen, M., Jääskeläinen, I. P., Hari, R., & Sams, M. (2012). Emotions promote social interaction by synchronizing brain activity across individuals. *Proceedings of the National Academy of Sciences, 109*(24), 9599-9604.

O'loughlin, M. (1992). Rethinking science education: Beyond Piagetian constructivism toward a sociocultural model of teaching and learning. *Journal of research in science teaching, 29*(8), 791-820.

O'Regan, K. (2003). Emotion and e-learning. *Journal of Asynchronous learning networks, 7*(3), 78-92.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701.

Ortigosa, A., Martín, J. M., & Carro, R. M. (2014). Sentiment analysis in Facebook and its application to e-learning. *Computers in Human Behavior, 31*, 527-541.

Pabian, S., & Vandebosch, H. (2015). Short-term longitudinal relationships between adolescents'(cyber) bullying perpetration and bonding to school and teachers. *International Journal of Behavioral Development*, 0165025415573639.

Pang, B., Lee, L., & Vaithyanathan, S. (2002). *Thumbs up?: sentiment classification using machine learning techniques*. Paper presented at the Proceedings of the ACL-02 conference on Empirical methods in natural language processing-Volume 10.

Pekrun, R., & Linnenbrink-Garcia, L. (2012). Academic emotions and student engagement *Handbook of research on student engagement* (pp. 259-282): Springer.

Pélissier, C., & Metz, S. M.-V. (2010). Deviating technologies to design personal and creative help in e-learning. *Procedia-Social and Behavioral Sciences, 2*(2), 3552-3557.

Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior, 52*, 424-435.

Pérez-Ávilas, J., Haya, P. A., & Martín, E. (2011). Do you need help? The importance of helping hubs in offline educational social networks.

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

Poellhuber, B., Chomienne, M., & Karsenti, T. (2008). The effect of peer collaboration and collaborative learning on self-efficacy and persistence in a learner-paced continuous intake model. *International Journal of E-Learning & Distance Education, 22*(3), 41-62.

Proulx, S. (2012). L'irruption des médias sociaux: enjeux éthiques et politiques. *Médias sociaux: enjeux pour la communication, Québec, PUQ*, 9-31.

Puustinen, M. (2012). Aider et être aidé: l'importance de la notion d'aide dans les dispositifs d'apprentissage en ligne. *Revue internationale des technologies en pédagogie universitaire/International Journal of Technologies in Higher Education, 9*(3), 6-9.

Qureshi, A. M. A., & Evans, N. (2013). *A Trust-based Framework for Enhanced Absorptive Capacity: Improving Performance, Innovation and Competitive Advantage'*. Paper presented at the International Conference on Innovation and Entrepreneurship, Amman, Jordan.

Remesal, A., & Colomina, R. (2013). Social presence and online collaborative small group work: A socioconstructivist account. *Computers & Education, 60*(1), 357-367.

Renaud-Deputter, S., Xiong, T., & Wang, S. (2013). *Combining collaborative filtering and clustering for implicit recommender system.* Paper presented at the Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on.

Rochelandet, F. (2010). *Économie des données personnelles et de la vie privée*: La Découverte.

Ryan, A. M., & Pintrich, P. R. (1997). " Should I ask for help?" The role of motivation and attitudes in adolescents' help seeking in math class. *Journal of Educational Psychology, 89*(2), 329.

Sadler, M. E., Hunger, J. M., & Miller, C. J. (2010). Personality and impression management: Mapping the Multidimensional Personality Questionnaire onto 12 self-presentation tactics. *Personality and Individual differences, 48*(5), 623-628.

Sampasa-Kanyinga, H., & Hamilton, H. (2015). Social networking sites and mental health problems in adolescents: The mediating role of cyberbullying victimization. *European Psychiatry, 30*(8), 1021-1027.

Seedhouse, P. (1999). Task-based interaction. *ELT journal, 53*(3), 149-156.

Shani, G., & Gunawardana, A. (2011). Evaluating recommendation systems *Recommender systems handbook* (pp. 257-297): Springer.

Shannon, C. E. (1948). A note on the concept of entropy. *Bell System Tech. J, 27*, 379-423.

Sharples, M., Kloos, C. D., Dimitriadis, Y., Garlatti, S., & Specht, M. (2015). Mobile and Accessible Learning for MOOCs. *Journal of interactive media in education, 2015*(1), Art. 4.

Shea, P., & Bidjerano, T. (2009). Community of inquiry as a theoretical framework to foster "epistemic engagement" and "cognitive presence" in online education. *Computers & Education, 52*(3), 543-553.

Simonson, M., Schlosser, C., & Orellana, A. (2011). Distance education research: A review of the literature. *Journal of Computing in Higher Education, 23*(2-3), 124-142.

Skaalvik, S., & Skaalvik, E. M. (2005). Self-concept, motivational orientation, and help-seeking behavior in mathematics: A study of adults returning to high school. *Social Psychology of Education, 8*(3), 285-302.

Skinner, B. F. (2011). *About behaviorism*: Vintage.

Sleeman, D., & Brown, J. S. (1982). Intelligent tutoring systems.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly, 35*(4), 989-1016.

Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*: Yale University Press.

Steeves, V. (2009). Reclaiming the Social Value of Privacy [Press release]

Suizzo, M. A. (2000). The Social-Emotional and Cultural Contexts of Cognitive Development: Neo-Piagetian Perspectives. *Child development, 71*(4), 846-849.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(05), 557-570.

Tabachnick, B. G., Fidell, L. S., & Osterlind, S. J. (2001). Using multivariate statistics.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821-826.

Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online, 64*, 63.

Tierney, M., & Subramanian, L. (2014). *Realizing privacy by definition in social networks.* Paper presented at the Proceedings of 5th Asia-Pacific Workshop on Systems.

Tisseron, S. (2011). Intimité et extimité. *Communications, 88*(1), 83-91.

Troncy, R., Huet, B., & Schenk, S. (2011). *Multimedia semantics: metadata, analysis and interaction*: John Wiley & Sons.

Tubaro, P., Casilli, A. A., & Sarabi, Y. (2014). *Against the hypothesis of the end of privacy : an agent-based modelling approach to social media*. Cham: Springer.

Turban, E., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2015). E-Commerce: Regulatory, Ethical, and Social Environments *Electronic Commerce* (pp. 691-732): Springer.

Vallet, C. (2012). Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs. *Droit et société*(1), 163-188.

Van der Meij, H. (1990). Question asking: To know that you do not know is not enough. *Journal of Educational Psychology, 82*(3), 505.

Vassileva, J. (2008). Toward social learning environments. *Learning Technologies, IEEE Transactions on, 1*(4), 199-214.

Vivolo-Kantor, A. M., Martell, B. N., Holland, K. M., & Westby, R. (2014). A systematic review and content analysis of bullying and cyber-bullying measurement strategies. *Aggression and violent behavior, 19*(4), 423-434.

Volckrick, E., & Deliège, I. (2001). *Savoirs formels et savoirs informels, une approche pragmatique*. Retrieved from

von Marées, N., & Petermann, F. (2012). Cyberbullying: An increasing challenge for schools. *School Psychology International, 33*(5), 467-476.

Vuorikari, R., Manouselis, N., & Duval, E. (2009). Special issue on social information retrieval for technology enhanced learning. *Journal of Digital Information, 10*(2).

Vygotsky, L. (1987). Zone of proximal development. *Mind in society: The development of higher psychological processes, 5291*.

Walker, C. M., Sockman, B. R., & Koehn, S. (2011). An exploratory study of cyberbullying with undergraduate university students. *TechTrends, 55*(2), 31-38.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Weinberger, A., & Fischer, F. (2006). A framework to analyze argumentative knowledge construction in computer-supported collaborative learning. *Computers & Education, 46*(1), 71-95.

West, D. (2015). An investigation into the prevalence of cyberbullying among students aged 16–19 in post-compulsory education. *Research in Post-Compulsory Education, 20*(1), 96-112.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166.

Whitley, E. A. (2009). Informational privacy, consent and the "control" of personal data. *Information security technical report, 14*(3), 154-159.

Wingate, V. S., Minney, J. A., & Guadagno, R. E. (2013). Sticks and stones may break your bones, but words will always hurt you: A review of cyberbullying. *Social Influence, 8*(2-3), 87-106.

Xu, J.-M., Jun, K.-S., Zhu, X., & Bellmore, A. (2012). *Learning from bullying traces in social media.* Paper presented at the Proceedings of the 2012 conference of the North American chapter of the association for computational linguistics: Human language technologies.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500.

Zheng, B., & Warschauer, M. (2015). Participation, interaction, and academic achievement in an online discussion environment. *Computers & Education, 84*, 78-89.

Zimmerman, B. J. (1990). Self-regulated learning and academic achievement: An overview. *Educational psychologist, 25*(1), 3-17.

Publications

Journal

- **Mouna Selmi**, Hicham Hage, Esma Aïmeur: Predictive role of personality, self-disclosure and self-presentation in cyberbullying. *International Journal of Technology Enhanced Learning* [Soumis].

Conférences avec comité de lecture

- **Mouna Selmi**, Hicham Hage, Esma Aïmeur: Evaluating LSA Sensibility to Disclosure in Learners' Interactions. *In 10th International Conference on Intelligent Systems: Theories and Applications (SITA 2015)*. IEEE.
- **Mouna Selmi**, Hicham Hage, Esma Aïmeur: Opinion Mining for Predicting Peer Affective Feedback Helpfulness. *In Proceedings of the International Conference on Knowledge Management and Information Sharing (KMIS 2014)*, 419-425.
- **Mouna Selmi**, Hicham Hage, Esma Aïmeur: Latent Semantic Analysis for Privacy Preserving Peer Feedback. *Risks and Security of Internet and Systems* (pp. 100-115): Springer.
- **Mouna Selmi**, Esma Aïmeur, Hicham Hage: Privacy Framework for Peer Affective Feedback. *In Proceedings of the 2013 International Conference on Signal-Image Technology & Internet-Based Systems (SITIS 2013)*: 1049-1056.
- Fodé Touré, **Mouna Selmi**, Esma Aïmeur: A2MO and ETREOSys - Analyzing, Modeling and Validation of Enterprise Training Programs. *In Proceedings of the 15th International Conference on Enterprise Information Systems*, ICEIS (2) 2013: 310-316.