Sensibilisation à la Protection de la Vie Privée dans un Contexte d'Utilisation de Dispositifs Portables Intelligents

Par : Jean-François Fortin

Département d'Informatique et de Recherche Opérationnelle

Faculté des Arts et des Sciences

Mémoire présenté en vue de l'obtention du grade de M.Sc. en Informatique

Mars 2019

Résumé

Les DPI (*Dispositifs Portables Intelligents*) sont de plus en plus populaires dans les activités de sport, de loisirs, ainsi que pour la gestion du temps et du calendrier. Leur potentiel est reconnu dans plusieurs scénarios. Plus précisément, leur capacité à collecter une grande quantité de données au sujet de leur propriétaire et de son entourage par le biais des divers senseurs, peut éventuellement porter atteinte à sa vie privée.

Avec l'arrivée des montres intelligentes (*smartwatches*) ou de bracelets électroniques (*fitness trackers*) sur le marché, nous nous retrouvons face à de véritables petits ordinateurs. Lorsque combinés à l'utilisation d'une application propriétaire résidant sur un téléphone intelligent ou un ordinateur et à l'utilisation d'une connexion directe (ou indirecte) à l'Internet, celles-ci ouvrent la porte à une agrégation importante de données.

Le but de cette recherche est donc dans un premier temps d'explorer les risques de sécurité relatifs aux dispositifs portables, dans le but d'en inférer les impacts sur la vie privée.

Nous présentons ensuite une approche de formation adaptée (CLEOPATRA), fondée sur un STI (*Système de Tutorat Intelligent*) tenant compte du style d'apprentissage des individus selon leur cohorte générationnelle. Cette approche utilise une application web avec un modèle de recouvrement des connaissances obtenu à la suite d'un test d'évaluation ainsi qu'un modèle expert, sous-ensemble d'un curriculum de formation élaboré par notre groupe de recherche. Les modules de formation sont extraits de documents disponibles librement sur l'Internet, et d'un *genre* approprié pour la génération à laquelle ils s'appliquent. La formation utilise le PLE (*Personal Learning Environment*) ainsi que l'approche du *microlearning*. A la fin de la formation, les participants sont appelés à repasser le test d'évaluation afin de valider leur rétention des connaissances acquises.

Mots clés

Dispositif portable intelligent, Sécurité, Vie Privée, Système de Tutorat Intelligent, Curriculum, Environnement d'Apprentissage Personnel, Microlearning, Andragogie, Heutagogie, Générations.

Abstract

Smart wearable devices are becoming increasingly popular in sports, leisure, time management and calendar activities. Their potential is recognized in several scenarios. Specifically, their ability to collect a wealth of information about their owner and his entourage through the various sensors, can potentially undermine his privacy.

With the arrival of smartwatches and fitness trackers on the market, we are faced with real small computers. When combined with the use of a proprietary application residing on a smartphone / computer and the use of a direct (or indirect) connection to the Internet, these open the door to a large aggregation of data.

The purpose of this research is therefore to explore the security risks related to portable devices, with the aim of inferring the impacts on privacy.

We then present an adaptive training approach (CLEOPATRA), based on a ITS (*Intelligent Tutoring System*) that considers the learning style of individuals according to their generational cohort. It is a web application using a knowledge overlay model obtained using an assessment test, as well as an expert model, subset of a training curriculum developed by our research group. The training modules are extracted from documents freely available on the Internet, and of an appropriate *genre* for the generation that it applies to. The training uses a PLE (*Personal Learning Environment*) along with a *microlearning* approach. At the end of the training, participants are invited to pass the assessment test again, in order to validate the retention of their recently acquired knowledge.

Keywords

Smart wearable, Security, Privacy, Intelligent Tutoring System, Curriculum, Personal Learning Environment, Microlearning, Andragogy, Heutagogy, Generations.

Table des matières

Liste des tableaux

Liste des figures

Liste des acronymes

AFEC	Analog Front-End Controller
ANT+	Adaptive Network Technology
BAN	Body Area Network
BYOD	Bring Your Own Device
CEPD	Contrôleur Européen de la Protection des Données
CLEOPATRA	Cloud-based Learning Environment On Privacy Awareness Training for Adults
CLUF	Contrat de Licence Utilisateur Final
CPVP	Commissariat à la Protection de la Vie Privée
DPI	Dispositif Portable Intelligent (*Smart Wearable*)
FTC	Federal Trade Commission
GPS	Global Positioning System
GSMA	Global System for Mobile Association
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hyper Text Transfer Protocol Secure
I2C	Inter-Integrated Circuit
IoT	Internet of Things
ISO	International Standards Organization
LE	Low-Energy
LPRPDE	Loi sur la Protection des Renseignements Personnels et des Documents Électroniques
LTE	Long Term Evolution
MAC	Media Access Control
MITM	Man-In-The-Middle
NFC	Near Field Contact
NIST	National Institute of Standards and Technology
OAUTH	Open Web Authorization protocol
OCDE	Organisation de Coopération et de Développement Économiques

PIPEDA	Personal Information Protection and Electronic Documents Act
PLE	Personal Learning Environment
QOS	Quality of Service
RFID	Radio Frequency Identification
RGPD	Règlement Général sur la Protection des Données
SIM	Subscriber Identity Module
STI	Système de Tutorat Intelligent
UE	Union Européenne
USB	Universal Serial Bus
UUID	Universal Unique Identifier
WPAN	Wireless Personal Area Network

Remerciements

Je voudrais premièrement remercier ma directrice de recherche Esma Aïmeur qui a eu confiance en moi et qui m'a pris sous son aile avec les autres membres de son équipe, malgré ma différence générationnelle et mon cheminement atypique. Elle m'a donné la chance et les encouragements nécessaires pour réaliser ce défi personnel.

Je voudrais aussi remercier mon fils, Louis-Philippe, pour toutes les discussions technologiques enrichissantes ainsi que son aide technique pour le développement et l'implantation de CLEOPATRA.

Mes remerciements vont aussi à Rita Yusri, une collègue du laboratoire Héron avec qui j'ai travaillé à l'élaboration du curriculum de formation et de son ontologie. A maintes occasions, elle m'a fourni des idées et conseils pertinents.

Enfin, merci à mon épouse Suzanne, pour son encouragement tout au long de ce travail.

Introduction

Selon CCS Insight[1], une entreprise internationale de recherche qui s'intéresse au futur des technologies connectées, l'industrie des DPI atteindra le nombre de 233 millions d'unités vendues d'ici 2022. Cette croissance est principalement redevable aux ventes de montres intelligentes et de bracelets électroniques (*fitness trackers*).

Ces nouvelles technologies font partie de la catégorie des objets connectés[2] et leur capacité d'accès à l'Internet (direct ou indirect) ouvre un monde de possibilités. Ces DPI sont de véritables ordinateurs qui travaillent conjointement avec des capteurs mesurant certains paramètres de santé tels que le rythme cardiaque ou la qualité du sommeil. Ils peuvent aussi bien aider à gérer l'agenda personnel, recevoir et envoyer des messages-texte ou même faire connaître leur emplacement par le biais d'une puce GPS intégrée.

Les DPI offrent une variété de composants tiers et de logiciels [Kamišalić *et al*, 2018]. Leurs systèmes d'exploitation sont hétéroclites et présentent de nombreux défis à l'utilisation, rendant la tâche plus ardue pour les développeurs d'applications. Par surcroît, une application disponible sur un dispositif ne fonctionne pas nécessairement sur un autre [Jiang *et al*., 2015].

De plus, en raison des informations que ces dispositifs peuvent collecter, stocker et même partager, ils deviennent une cible de choix pour les attaquants cherchant à obtenir ces données. En outre, compte tenu de la connectivité réseau permanente de certains de ces dispositifs et de leurs utilisations différentes, ces derniers pourraient être ciblés par des programmes malveillants, ce qui augmente le risque d'utilisation préjudiciable [Arias *et al*., 2015].

Ce qui nous amène ici à parler des impacts qu'ils peuvent causer à la vie privée. Il existe en effet plusieurs raisons[3] valables de protéger la vie privée et parmi celles-ci il y en a une qui s'impose, soit celle qui fait que :

[1] https://www.ccsinsight.com/ consulté le 2018-11-16
[2] https://www.mouser.ca/applications/article-iot-wearable-devices/ accédé le 2019-01-11
[3] https://teachprivacy.com/10-reasons-privacy-matters/ consulté le 2019-01-11

> *Plus quelqu'un détient d'informations à notre sujet, plus cet individu a un pouvoir sur notre personne*.
>
> *(Daniel J. Solove, 2014, professeur en droit à l'Université George Washington)*

Une protection efficace des informations personnelles permet de gérer adéquatement notre réputation, sans oublier qu'elle apporte un aspect important dans la construction de relations de confiance avec d'autres individus ou entités sociales [Sartor, 2006].

Dans cette recherche, nous nous intéressons principalement au besoin de sensibiliser les personnes adultes aux risques de sécurité et d'atteintes à la vie privée, gravitant autour des DPI. Pour ce faire, nous présentons, en premier lieu, l'environnement technologique dans lequel ces dispositifs évoluent. Nous nous intéressons ensuite à une approche adaptée pour sensibiliser une clientèle non-académique aux enjeux de sécurité à leur utilisation. Cette approche de formation est construite à partir d'un STI (*système de tutorat intelligent*) auquel nous ajoutons un aspect innovateur au style de l'apprenant, à l'effet qu'il tient compte des expériences sociales et du vécu de sa cohorte générationnelle. Nous utilisons aussi la technologie du web et des outils technologiques modernes. A notre avis, bien qu'il existe plusieurs adaptations de systèmes de formation basés sur les STI, dont nous ne remettons pas la pertinence en question, nous n'avons pas trouvé d'approche de formation de groupe basé sur l'appartenance à une cohorte générationnelle, dans la littérature académique ou scientifique que nous avons consultée jusqu'à maintenant.

Le reste de ce document est organisé comme suit : le Chapitre 1 présente le concept de *l'Internet of Things* dans le contexte de la vie privée. Le Chapitre 2 canalise notre approche vers les dispositifs portables connectés. Le Chapitre 3 aborde la question de la sensibilisation sous la forme d'une formation adaptée, prélude à l'arrivée du Chapitre 4 où nous présentons notre système de e-Learning *CLEOPATRA* qui est utilisé afin de promouvoir les connaissances requises à l'atteinte des buts de cette recherche. Un dernier Chapitre 5, portera sur l'évaluation (*preuve de concept*) du système *CLEOPATRA* après qu'un nombre d'utilisateurs l'aient testé et nous en confirment son efficacité. Ceci fera également office de conclusion à notre recherche.

Chapitre 1. *Internet of Things* et vie privée

L'Internet des Objets (IoT) (en anglais : *Internet of Things*), est un paradigme dans le monde des télécommunications sans-fil. L'idée de base de ce concept est l'omniprésence autour de nous d'une variété d'objets tels que balises, capteurs, téléphones mobiles etc. qui sont capables d'interagir et coopérer entre eux dans l'atteinte d'un objectif commun. [Giusto *et al.*, 2010]

1.1 Objets Connectés (en anglais : *Smart Objects*)

Les objets connectés envahissent nos foyers. Ils font partie intégrante de notre vie au quotidien et leur utilité est indissociable à leur côté pratique, ludique et technologique. Selon le site web d'information et de dissémination de connaissances IGI-Global[4], les objets connectés sont des objets électroniques bénéficiant généralement d'une connexion sans fil, partageant des informations avec un ordinateur, une tablette ou un téléphone intelligent et capables de percevoir, d'analyser et d'agir selon les contextes de notre environnement.

Le concept des objets connectés est apparu à la toute fin du vingtième siècle [Madakam *et al.*, 2015]. C'est un technologue anglais, Kevin Ashton, qui en a proposé l'appellation[5] « *Internet of Things* » (*IoT*). [Tripathy et Anuradha, 2017] définissent ce vocable comme « *une troisième vague de l'Internet ayant le potentiel de connecter plus de 28 milliards d'objets de toutes sortes d'ici 2020* ». Ces objets connectés, munis de senseurs, sont non seulement capables d'amasser une foule d'informations, mais ils sont aussi capables de prendre certaines décisions ne nécessitant pas l'intervention d'un humain.

L'augmentation considérable d'objets connectés soulève beaucoup d'inquiétudes[6] en rapport au transit de données de toutes sortes, de leur utilisation de la bande passante ou de la capacité à être véhiculées dans de bonnes conditions (qualité de service ou *QoS*). Selon un article[7] du New York Times du 11 Février 2012 (*The Age of Big Data*), cette croissance de *l'IoT* alimente des dépôts de grandes quantités de données pour lesquels sont requis d'imposantes ressources de

[4] https://www.igi-global.com/dictionary/digital-object-memory/27190 accédé le 2019-01-11
[5] http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf accédé le 2019-01-11
[6] https://internetofthingsagenda.techtarget.com/opinion/Internet-of-Things-marks-dawn-of-smart-objects-more-network-pressures accédé le 2019-01-11
[7] https://s3.amazonaws.com/academia.edu.documents/34393761/2_The_New_York_Times_on_The_Age_of_Big_Data.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1547236399&Signature=3RWdIdq%2FlDmyTz2he1BD32dzf3Q%3D&response-content-disposition=inline%3B%20filename%3D2_The_New_York_Times_on_The_Age_of_Big_D.pdf accédé le 2019-01-11

stockage, de calcul et de communication. Un aspect important de la croissance de ces données, qui est celui de la présente étude, concerne le niveau de sécurité et le respect de la vie privée.

1.2 Big Data

Le terme *Big Data* fait référence à de grands ensembles de données en croissance sous des formats hétérogènes. Le *Big Data* a une nature complexe qui nécessite des technologies puissantes et des algorithmes avancés [Oussous *et al*, 2018]. Il représente entre autres, les vastes ensembles de données produites par les objets connectés. Leur quantité dépasse notre imagination et nos capacités humaines d'analyse, et même celles d'outils informatiques classiques de gestion de base de données ou de l'information.

Dans quelques cas l'accès à certaines de ces informations pourrait représenter une menace à la vie privée. En contrepartie, pour plusieurs entreprises, le *Big Data* représente une opportunité leur permettant d'obtenir, par l'utilisation d'outils analytiques spécialisés, de nouveaux contenus pour les rendre plus agiles. Ce sont de très belles occasions à saisir afin de demeurer compétitifs.

Nous vivons aujourd'hui dans une époque où tout est documenté. Les entreprises et les gouvernements prennent des décisions en fonction des *empreintes numériques*[8] laissées par les gens. Ces traces ne sont pas sans conséquences et ce n'est pas parce qu'on a été d'accord à un moment donné de notre vie de partager des données personnelles avec une entreprise, que le besoin de modifier cette décision ne se présentera jamais. Nous n'avons d'ailleurs aucune garantie qu'une entreprise avec qui nous avons échangé certaines de nos données sera toujours en affaire dans les années à venir et nous ne pouvons aucunement présumer de ce qui arrivera aux données qui sont en leur possession. Il est même possible que de nouvelles lois, par exemple le RGPD[9], amènent avec elles des changements de protection à certaines données pour lesquelles nous voulions que l'accès soit restreint, et ceci pourrait nous être potentiellement désavantageux.

Profitant de l'existence et de l'essor grandissant du *Big Data*, arrivent les « *courtiers en données* » ou « *data brokers* ». Ce sont des entreprises qui se spécialisent dans l'acquisition et la revente des données de consommateurs. Ils les revendent à d'autres entreprises qui pourront, à leur tour, offrir des services personnalisés [Yu-li et Yuntsai, 2018].

[8] https://www.internetsociety.org/fr/tutorials/your-digital-footprint-matters/ accédé le 2019-01-11
[9] https://gdpr.eu/tag/gdpr/ accédé le 2019-01-12

Selon le rapport[10] sur les « *courtiers en données* » du Commissaire à la protection de la vie privée (CPVP) du Canada, la cueillette de données est faite de différentes sources: en ligne et hors ligne et souvent à l'insu des individus. N'ayant aucune limite de temps établie à propos de la période de conservation, ces données sont ensuite agrégées et combinées dans le but d'inférer des éléments de vie privée. Elles peuvent ensuite être partagées ou utilisées à des fins non prévues, cause directe du manque de transparence concernant le processus de cueillette. De nos jours, des techniques évoluées permettent d'établir un profil extrêmement détaillé d'une personne.

A titre d'exemple, il existe aujourd'hui plus de 4 000[11] sociétés de courtage de données dans le monde. Acxiom[12], l'un des plus importants, compte 23 000 serveurs qui collectent et analysent des données de consommation pour plus de 500 millions de consommateurs dans le monde et jusqu'à 1 500 points[13] de données par personne.

1.3 Data Mining et Identification des Données

Les méthodes d'exploration et d'extraction d'informations du *Big Data* sont variées mais elles sont regroupées sous une appellation commune : Le *data mining* [14]. Une définition intéressante du *data mining* est disponible dans un récent article du magazine français en ligne « Le Big Data »

> *…l'analyse de données depuis différentes perspectives et la transformation de ces données en informations utiles, en établissant des relations entre les données ou en repérant des patterns.*

À la base, le *data mining* (Figure 1) est composé d'algorithmes complexes et sophistiqués permettant de segmenter les données. Il fait ensuite des associations et relations entre toutes ces données, permettant ainsi d'obtenir des informations plus précises. Ces informations peuvent être

[10] https://www.priv.gc.ca/media/1779/db_201409_f.pdf accédé le 2018-05-19
[11] https://www.webfx.com/blog/general/what-are-data-brokers-and-what-is-your-data-worth-infographic/ accédé le 2019-01-12
[12] https://www.acxiom.com/ accédé le 2019-01-19
[13] Un point de données est une unité d'information discrète. https://whatis.techtarget.com/definition/data-point accédé le 2019-01-30
[14] https://www.lebigdata.fr/data-mining-definition-exemples accédé le 2018-05-20

ensuite converties en « savoir » à propos de *patterns* historiques ou des tendances futures. On vise à identifier le comportement des utilisateurs à l'aide de vastes quantités de données rassemblées.

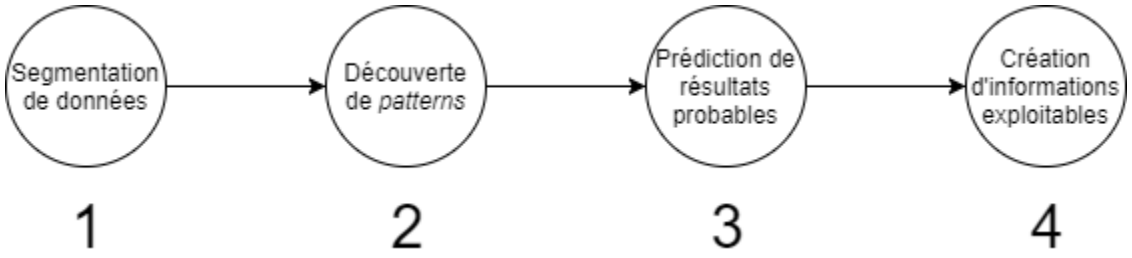


FIGURE 1 LE DATA MINING

Par exemple, des compagnies d'assurance[15] sont en mesure d'amasser les données qui ont rapport à l'activité physique d'une personne et utilisent celles-ci comme intrant dans un algorithme qui détermine si elles maintiennent un niveau de santé adéquat. Certains outils analytiques peuvent même aller jusqu'à informer à propos de problèmes de santé. La prime d'assurance à payer est calculée en fonction du résultat obtenu.

Un article[16] paru dans le journal universitaire américain *The Dartmouth* de Janvier 2019 rapporte les faits suivants :

> *L'Université Oral Roberts, en Oklahoma, demande aux étudiants d'acheter un Fitbit*^{mc} *et de franchir au moins 10 000 pas par jour pour être noté. (…)*

[15] https://www.capgemini.com/wp-content/uploads/2017/07/wearable_devices_and_their_applicability_in_the_life_insurance_industry.pdf accédé le 2018-05-20

[16] http://www.thedartmouth.com/article/2019/01/shah-10000-or-else (accédé le 2019-01-12) et https://www.cnbc.com/2016/02/01/oral-roberts-university-to-track-students-fitness-through-fitbits.html (accédé le 2019-01-25)

Un autre exemple[17] :

> *Depuis septembre 2018, la compagnie d'assurances John Hancock fournit désormais des primes à prix réduits aux personnes inscrites à leur programme d'assurance vie Vitality, qui utilisent un tracker d'activités et décident de communiquer ces données à la société. Les participants au programme bénéficient automatiquement de 20 à 40% de réduction sur ces dispositifs. (...)*

Tous ces renseignements collectés peuvent constituer la clé donnant accès à des renseignements délicats et de nature privée. De ce fait, les organisations doivent être en mesure de montrer comment elles gèrent l'information à partir de la collecte jusqu'à son utilisation.

En Juin 2014, le Commissariat à la Protection de la Vie Privée du Canada[18] qui est l'organisme gouvernemental canadien chargé de protéger et promouvoir le droit à la vie privée des citoyens, a accueilli favorablement un jugement de la Cour Suprême[19], où cette dernière […] *reconnait que l'anonymat sur Internet constitue un élément essentiel du caractère privé des renseignements personnels*.

L'anonymisation et la protection contre l'identification des données sont des sujets sur lesquels les chercheurs mettent beaucoup d'efforts mais ces approches sont difficiles à appliquer dans le contexte de *l'IoT* parce que la plupart des techniques peuvent être brisées en utilisant des données auxiliaires qui peuvent devenir disponibles à tout moment au cours de l'évolution de ce dernier. Quant aux solutions de protection contre l'identification, elles reposent sur des opérations cryptographiques coûteuses et elles aussi difficiles à appliquer à des environnements distribués et hétérogènes comme *l'IoT* [Ziegeldorf *et al*., 2015].

Des données sont considérées anonymisées lorsqu'elles sont épurées d'une (ou plusieurs) catégorie(s) d'informations pouvant servir à identifier une personne. En revanche, avec la

[17] https://www.johnhancockinsurance.com/vitality-program.html (accédé le 2019-01-25)
[18] https://www.priv.gc.ca/fr/ accédé le 2018/05/13
[19] https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2014/s-d_140613/ accédé le 2018/05/12

prolifération importante de données en ligne, il est souvent possible grâce à la technologie informatique, de procéder à la réidentification de données qui avaient été anonymisées.

Par exemple, dans le Tableau 1, il est possible de retirer la colonne « Nom » sans pour autant compromettre l'utilité des données dans une future activité de recherche.

TABLEAU 1 ANONYMISATION PAR RETRAIT D'UNE COLONNE.
SOURCE: [LUBARSKY, 2017]

Nom	Date Naissance		Code Postal	Genre	Origine ethnique	Diagnostic
~~*Adam Smith*~~	1970-01-01		20002	M	Caucasien	Insuffisance cardiaque
~~*Betty Davis*~~	1980-02-02		20001	F	Afro-américain	Pneumonie
~~*Carlos Hernandez*~~	1990-03-03		20007	M	Hispanique	Maladie d'Addison

L'information personnelle apparaît sous forme d'un escalier dont la marche du haut représente ce qui permet l'identification directe jusqu'à la marche du bas où elle ne peut être reliée à aucun individu (Figure 2).

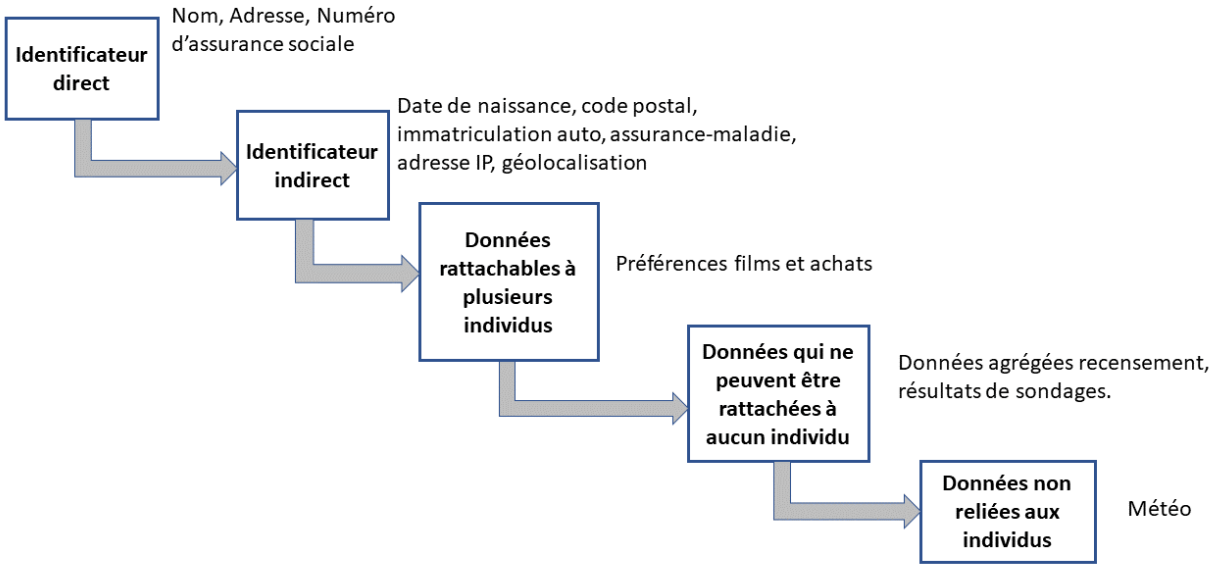


FIGURE 2 INFORMATIONS PERSONNELLES
[LUBARSKY 2017]

[Lubarsky, 2017] décrit quatre techniques d'anonymisation des données :

(1) Effacer la donnée

(2) Remplacer la donnée avec un pseudonyme

(3) Ajouter du bruit statistique : **Généralisation** (par exemple : utiliser un intervalle de valeurs numériques pour représenter l'année de naissance), **Perturbation** (par exemple : systématiquement soustraire/additionner une valeur) et **Échange** (par exemple : échanger les valeurs d'enregistrements dans un même *dataset*)

(4) Agréger les données : produire sommaire statistique ou sous-ensemble des données

En contrepartie, la réidentification des données est possible lorsque :

- L'anonymisation est insuffisante
- On peut découvrir la signification des pseudonymes
- On peut combiner différents *datasets*

1.4 Paradoxe Vie Privée - Personnalisation

Aux États-Unis, un rapport[20] de la FTC (*Federal Trade Commission*) datant de Mai 2014, nous apprenait que l'industrie du courtage de données, profitant des avantages du *Big Data*, amasse et stocke des quantités phénoménales de données sur les ménages américains. En particulier, une de ces entreprises de courtage se targuait de posséder près de 3000 points de données sur chaque consommateur! Suite au CES[21] de 2015, le magazine ZDnet[22] rapportait dans un article[23] daté du mois de février de la même année que Jeffrey Jenkins, co-fondateur et CTO de APX Labs[24] (aujourd'hui Upskill[25]) croit que « *la vie privée dépend fortement de la proposition de valeur que les gens en obtiennent* ».

La littérature sur le sujet nomme ce concept, le « *paradoxe vie privée - personnalisation* » (*personalization-privacy paradox*[26]) [Kokolakis, 2017] : il représente ce qu'un consommateur est prêt à partager comme information personnelle afin d'obtenir des services personnalisés. La personnalisation est perçue comme une composante essentielle permettant de fournir une meilleure expérience au consommateur mais en revanche peut être intrusive et peut impacter sa vie privée. Cette personnalisation est perçue comme une habileté à utiliser l'information personnelle afin de livrer le meilleur service « sur mesure ».

Le programme [27] de fidélité *Amazon Prime* illustre bien le concept « vie privée-personnalisation » : On croit à tort qu'il offre seulement certains avantages tels que la livraison gratuite mais l'entreprise cherche plutôt à bâtir la confiance en soutirant une foule d'informations personnelles qui permettent d'obtenir des recommandations personnalisées et surtout mieux vous connaître personnellement.

[20] https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf accédé le 2018-05-18
[21] https://www.ces.tech/ accédé le 2018-05-19
[22] https://www.zdnet.com/ accédé le 2018-05-18
[23] https://www.zdnet.com/article/wearables-open-new-avenues-for-security-and-privacy-invasions/ accédé le 2018-05-18
[24] https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=262438042 accédé le 2018-05-18
[25] https://upskill.io/ accédé le 2018-05-19
[26] https://itnext.io/personalization-and-privacy-a-paradox-8e06a5701fb3 accédé le 2018-05-20
[27] https://www.entrepreneur.com/article/314611 accédé le 2019-01-12

1.5 Règlementation

La capacité des objets connectés à capturer des informations et des images en temps réel dans la vie d'un individu et de ceux l'entourant, créent de nombreuses nouvelles questions juridiques en matière de confidentialité, vie privée et de responsabilité. La législation entre en jeu lorsque des données personnelles sont impliquées. Rappelons que les données personnelles désignent en général, tout élément permettant d'identifier directement ou indirectement une personne physique (Définition du CNIL[28]).

Alors que les fabricants de ces technologies, font face à plusieurs accusations mettant en cause leurs politiques de confidentialité interdisant la vente de données d'utilisateurs, il en existe d'autres qui autorisent le partage de données sous forme agrégée et anonymisée. Par conséquent, les problèmes reliés à l'utilisation et au partage des données sont compliqués à résoudre parce que les données se présentent sous une panoplie de formats : identifiées ou non identifiées, structurées ou non structurées, sous forme d'image ou de texte verbal, ou agrégées.

Il est donc très pertinent de savoir qu'il existe des organismes de gouvernance en matière de gestion, diffusion, partage ainsi que de normalisation.

1.5.1 Organismes de normalisation

Les normes visent à protéger les données des personnes face à l'innovation numérique qui prend de plus en plus de place dans nos sociétés. En affaires, la normalisation est définie[29] comme suit:

> *« La formulation, publication et mise en œuvre de directives, règles et spécifications pour un usage commun et répété, visant à atteindre le degré optimal d'ordre ou d'uniformité dans un contexte, une discipline ou un domaine donné »*

[28] https://www.cnil.fr/fr/definition/donnee-personnelle accédé le 2019-01-12
[29] http://www.businessdictionary.com/definition/standardization.html accédé le 2018-10-24

L'absence de normalisation peut entraîner des manques d'efficacité et aboutir à des conclusions divergentes sur les données au sein des différents services. La normalisation peut donner une plus grande transparence à une entreprise et une flexibilité accrue.

Les personnes et les entreprises ont intérêt à ce que certains organismes chapeautent et produisent une normalisation pour la gestion et le partage des données personnelles privées et sensibles. Les quatre prochains paragraphes présentent les principaux organismes de normalisation à retenir.

1.5.1.1 OCDE (Organisation de Coopération et de Développement Économiques)

L'OCDE joue un rôle important dans la promotion du respect de la vie privée en tant que valeur fondamentale et condition de la libre circulation des données à caractère personnel à travers les frontières. En 2013, l'OCDE a publié[30] le premier ensemble internationalement reconnu de principes de confidentialité (mise-à-jour de la première version publiée en 1980).

L'Organisation de Coopération et de Développement Économiques (OCDE[31]) a été fondé en 1960 par 18 pays européens auxquels se sont ajoutés les États-Unis et le Canada. Il est aujourd'hui composé d'un groupe de 34 pays-membres qui travaillent à élaborer et échanger à propos de politiques de développement social et économique.

1.5.1.2 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

A l'instar des Nations Unies, les états membres du Conseil de l'Europe ont élaboré plusieurs accords visant à promouvoir le droit des citoyens à la vie privée. En particulier on peut souligner : La « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » (1980) et le « Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel des autorités de contrôle et des flux de données transfrontaliers » (2001).

A l'article 1er de cette convention, on y définit le but[32] suivant :

[30] http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm accédé le 2018-10-23
[31] https://www.investopedia.com/terms/o/oecd.asp accédé le 2018-10-23
[32] https://rm.coe.int/1680078b39 accédé le 2018-11-07

> *Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données »).*

1.5.1.3 National Institute of Standards and Technology (NIST)

Fondé en 1901 et faisant partie du département du commerce des États-Unis, le *NIST* s'est engagé à protéger la vie privée puisque la confiance individuelle dans la confidentialité et la sécurité des informations personnellement identifiables sont un fondement de la confiance dans le gouvernement et le commerce au vingt-et-unième siècle.

Le besoin de normes et de meilleures pratiques en matière de cybersécurité qui traitent de l'interopérabilité, de la convivialité et de la confidentialité des données reste essentiel. Les programmes de cybersécurité du NIST visent à permettre le développement et l'application de technologies et de méthodologies de sécurité pratiques et novatrices qui renforcent la capacité des États-Unis à faire face aux défis actuels et futurs en matière de sécurité des ordinateurs et de l'information.

1.5.1.4 ISO/IEC 27000

L'ISO (Organisation internationale de normalisation) est une organisation internationale non gouvernementale, indépendante, dont les membres sont les organismes nationaux de normalisation. La famille de normes *ISO/IEC 27000* [33] aide les organisations à gérer et assurer la sécurité des informations qu'elles détiennent. On y retrouve plus précisément les normes *ISO/IEC 27001,* qui est un SMSI (*Système de Management de la Sécurité des Informations*) et *ISO/IEC 27002* qui est un code de bonnes pratiques pour le management de la sécurité de l'information. On y présente des approches systémiques par lesquelles une organisation veille à la sécurité des informations sensibles. On y gère aussi le risque.

[33] https://www.iso.org/fr/isoiec-27001-information-security.html accédé le 2019-01-12

La certification d'une entreprise sous ces normes permet d'avoir un système bien encadré, sécurisé et évolutif. Le respect de ces normes permet de réduire les coûts de sécurité, puisqu'elles permettent la mise en place d'actions adaptées aux besoins. Elles constituent également un élément marketing indéniable en rassurant les clients et les partenaires. Cet élément de réassurance peut constituer un avantage concurrentiel, et deviendra un élément indispensable pour ne pas prendre de retard dans l'écosystème informatique.

1.5.2 Organismes de gouvernance

Quand on parle de gouvernance[34], on parle de règles d'imputabilité et de principes de fonctionnement mis en place par un conseil d'administration pour arrêter les orientations stratégiques d'une organisation, assurer la supervision de la direction, apprécier la performance économique et sociale et favoriser l'émergence de valeurs de probité et d'excellence.

Dans un contexte de sensibilisation aux impacts à la vie privée, certains organismes rattachés à la protection de la vie privée prennent tous les moyens afin d'atteindre les buts pour lesquelles ils ont été créés, de façon transparente, efficiente et respectueuse des attentes.

1.5.2.1 FTC (Federal Trade Commission)

Aux États-Unis, le *Federal Trade Commission* (FTC) protège les consommateurs en mettant fin aux pratiques déloyales, trompeuses ou frauduleuses sur le marché. Il mène des enquêtes, poursuit en justice les entreprises et les personnes qui enfreignent la loi, élabore des règles pour assurer un marché dynamique et informe les consommateurs et les entreprises de leurs droits et responsabilités.

Du point de vue de la vie privée, le FTC fournit les ressources[35] aux entreprises qui conservent des données personnelles sensibles sur leur réseau, afin de garantir qu'elles ont un plan sécuritaire en place en cas de difficultés, qu'elles ne colligent que ce qui est nécessaire et se départissent de ces informations de la bonne façon.

[34] https://igopp.org/ligopp/la-gouvernance/ consulté le 2018-11-07
[35] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business accédé le 2019-01-19

1.5.2.2 *Commissariat à la Protection de la Vie Privée du Canada* (CPVP)

Au Canada, la gouvernance est assurée par « Le Commissariat à la Protection de la Vie Privée » (*CPVP*), un organisme fédéral qui guide les personnes sur la façon de protéger leurs renseignements personnels et veille aussi à appliquer la « Loi sur la Protection des Renseignements Personnels et des Documents Électroniques » (*LPRPDE*), connue aussi en anglais sous « *Personal Information Protection and Electronic Documents Act » (PIPEDA).* Cette loi régit les entreprises privées au niveau du traitement des renseignements personnels dans le cadre de leurs activités commerciales.

Le CPVP mène des enquêtes suivant des plaintes de non-respect de la vie privée; il joue un rôle d'éducation et d'information envers le public et effectue des recherches sur les enjeux reliés à la protection de la vie privée.

1.5.2.3 CEPD [36](Contrôleur Européen de la Protection des Données)

Dans l'Union Européenne (UE), on retrouve le « *Contrôleur européen de la protection des données* » (CEPD) qui est l'autorité indépendante chargée de la protection des données. Il est dirigé par un contrôleur et un adjoint, soutenus par une équipe de juristes, administrateurs et informaticiens.

Un peu à la manière du CVPV du Canada, le CEPD contrôle les activités de traitement des informations personnelles par l'administration européenne, il joue un rôle conseil au niveau des institutions de l'UE, il gère les plaintes et mène des enquêtes.

1.5.3 Lois

Au Canada, le droit à la vie privée est enraciné dans la *Charte canadienne des droits et libertés*[37]; aux États-Unis, il est mentionné dans le quatrième amendement[38] à la constitution américaine tandis qu'en Europe, le respect de la vie privée est un domaine pour lequel « l'Agence des droits fondamentaux de l'Union Européenne » (*FRA*[39] ou *Fundamental Rights Agency*) en tant qu'agence européenne, consacre ses activités.

[36] https://edps.europa.eu/about-edps_fr accédé le 2018-10-23
[37] https://laws-lois.justice.gc.ca/fra/Const/page-15.html accédé le 2019-01-12
[38] https://www.law.cornell.edu/constitution/fourth_amendment accédé le 2019-01-12
[39] https://fra.europa.eu/fr accédé le 2018-12-18

Sur ces prémices, il est important que des lois puissent être appliquées afin de faire respecter ce droit et punir les contrevenants.

1.5.3.1 "Health Insurance Portability and Accountability Act" (HIPAA)

La loi *HIPAA*[40] du gouvernement des États-Unis oblige le secrétaire du Département américain de la santé et des services sociaux à élaborer des réglementations protégeant la confidentialité et la sécurité de certaines informations de santé. La règle de sécurité *HIPAA* établit des normes nationales visant à protéger les informations de santé personnelles électroniques créées, reçues, utilisées ou conservées par une entité couverte. La règle de sécurité requiert des sauvegardes administratives, physiques et techniques appropriées pour assurer la confidentialité, l'intégrité et la sécurité des informations de santé protégées de manière électronique.

Aux États-Unis, la *FDA* (*Food and Drugs Administration*) a publié un projet de directive intitulé : « *Bien-être général: Politique relative aux dispositifs à faibles risques* [41]». La *FDA* y précise que les produits de bien-être généraux, y compris les produits liés à la gestion du poids, à la forme physique ou au sommeil, ne relèvent pas du régime réglementaire de la loi de 1938 sur les aliments, les médicaments et les cosmétiques[42]. De plus, la loi *HIPAA*, qui définit les normes américaines pour la gestion électronique de l'assurance-maladie ne protège pas les données collectées par les DPI; elle couvre uniquement les données de santé recueillies par les médecins et hôpitaux[43]. Les données recueillies par les DPI ne sont donc pas sous la couverture d'aucune loi aux États-Unis.

Jusqu'à présent, le long processus d'approbation de la *FDA* a découragé les entreprises de technologies d'essayer d'intégrer une technologie de qualité médicale dans les appareils grand public. Cependant les choses sont appelées à changer car la *FDA* a annoncé le 26 septembre 2017 un projet de programme pilote[44] de pré-certification : L'objectif étant que la *FDA*, après avoir examiné les systèmes de conception, de validation et de maintenance du logiciel, détermine si l'entreprise respecte les normes de qualité et, le cas échéant, lui accorde une pré-certification. Grâce

[40] https://www.hhs.gov/hipaa/index.html accédé le 2018-10-24
[41] https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM518760.pdf accédé le 2018-12-18
[42] https://www.healthlawgurus.com/2015/12/are-wearable-devices-a-privacy-nightmare/ Consulté le 2018-10-22
[43] https://www.pcworld.com/article/3150801/security/privacy-protections-for-wearable-devices-are-weak-study-says.html
[44] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm577480.htm accédé le 2019-01-12

aux informations recueillies dans le cadre du programme pilote, l'agence espère déterminer les paramètres clés et les indicateurs de performance pour cette pré-certification et identifier les moyens par lesquels les entreprises qui se qualifient pourraient potentiellement soumettre à la *FDA* moins d'informations que ce qui est actuellement demandé. Apple, Fitbit, Samsung et d'autres entreprises pourraient tirer avantage de ce projet-pilote. En Janvier 2019, ce pilote en était à sa phase de tests.

1.5.3.2 Loi sur la Protection des Renseignements Personnels et des Documents Électroniques (LPRPDE)

La LPRPDE est une loi fédérale canadienne sur la protection des renseignements personnels. Elle régit les organismes du secteur privé et établit les règles de base concernant le traitement des renseignements personnels par les entreprises dans le cadre de leurs activités commerciales (Extrait du site web du CPVP[45])

Cette loi repose sur dix principes relatifs à l'équité dans le traitement de l'information que les entreprises doivent respecter :

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte
5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte

[45] https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/ accédé le 2019-01-12

Un exemple [46] récent (2018) tiré du site web du CPVP :

Le fabricant VTech Holdings Limited, dont le siège social est situé à Hong Kong, a avisé le CPVP d'une atteinte mondiale à la protection des données qui a potentiellement compromis les renseignements personnels de plus de 316 000 enfants canadiens et de plus de 237 000 adultes, qui sont pour la plupart les parents des enfants. Les personnes touchées avaient acheté ou utilisé des produits ou services Web de l'entreprise qui sont destinés aux enfants (...)

L'enquête du CPVP a révélé d'importantes lacunes liées aux mesures de sécurité dans le cadre du processus de gestion de l'information de VTech (...)

Les mesures de sécurité en place chez VTech ne correspondaient pas au volume et à la sensibilité potentielle des renseignements en cause et auraient pu exposer les enfants à des risques inutiles de préjudice si ceux-ci étaient tombés entre les mains de personnes malintentionnées (...)

VTech a pris, en temps opportun, toutes les mesures nécessaires pour circonscrire la portée de l'incident, réduire le risque pour les personnes touchées et atténuer le risque d'un incident similaire à l'avenir en réglant les problèmes relatifs à la sécurité (...)

De notre côté de la frontière, le fait que de nombreux appareils intelligents utilisés par les Canadiens soient fabriqués par des sociétés américaines complique encore plus les choses; leurs produits obligent souvent les consommateurs canadiens à renoncer[47] efficacement à leur droit à la vie privée. Bien que cela soit juridiquement douteux, les lois en vigueur sur la protection de la vie privée ne sont pas assez claires et fortes, ce qui encourage les fournisseurs américains de technologies à continuer leur pratique.

1.5.3.3 RGPD (Règlement Général sur la Protection des Données)

En Europe, depuis le 25 mai 2018, le *RGPD* vise à adapter la législation en matière de protection des données à l'évolution des technologies. Il clarifie les droits des personnes concernées

[46] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-001/ accédé le 2019-01-13
[47] https://globalnews.ca/news/3791571/canada-privacy-laws-internet-of-things/ accédé le 2019-01-12

et accroît les obligations des responsables du traitement des données à caractère personnel des résidents de l'Union Européenne (UE). Le champ d'application du *RGPD* s'étend au-delà de l'UE en impactant toute organisation qui propose des biens ou des services aux résidents de l'UE ou qui surveille le comportement de personnes dans l'UE.

Le *RGPD* impose des obligations supplémentaires et plus strictes au niveau du *Big Data* et du profilage, qui représente un aspect important de l'industrie des objets connectés. Cette nouvelle loi oblige les manufacturiers à mettre la vie privée à l'avant-plan, dès la conception de leurs produits afin de garantir un maximum d'intimité au consommateur.

Aucun partage des données personnelles n'est possible sans un consentement explicite individuel, et le *RGPD* oblige les entreprises à informer les individus de ce qui arrivera à leurs données.

Des sanctions importantes (

Tableau 2) sont prévues en cas de fuites et de non-respect à cette loi et ce sont les autorités de contrôle[48] [49] (par exemple : le CNIL[50] en France, l'APD[51] en Belgique etc.) qui imposent les sanctions administratives.

[48] https://www.legalplace.fr/guides/rgpd-sanction/ accédé le 2019-01-13
[49] https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde accédé le 2019-01-13
[50] https://www.cnil.fr/professionnel accédé le 2019-01-13
[51] https://www.autoriteprotectiondonnees.be/

TABLEAU 2 TROIS EXEMPLES RÉCENTS DE SANCTIONS EN VERTU DU RGPD

Pays	Autorité de Contrôle	Mois / Année	Nature du délit	Sanction
France 	CNIL	Décembre 2018	Bouygues Télécom : Existence d'une vulnérabilité[52] permettant d'accéder à des contrats et factures de clients	Sanction pécuniaire d'un montant de 250 000 euros
Allemagne 	Baden-Württemberg Data Protection Authority	Novembre 2018	Site de réseau social Knuddels : Piratage [53] de plus de de 2,6 millions d'informations privées	Condamné à 20 000 euros d'amende
Portugal 	CNPD (Comissão Nacional de Proteção de Dados)	Novembre 2018	Centre Hospitalier Barreiro-Montijo [54] : Plusieurs personnels administratifs avaient des accès réservés aux médecins. 985 médecins avaient des habilitations pour accéder au dossier médical des patients, alors que l'établissement ne comprend que 296 médecins (Les comptes de médecins temporaires demeurent tout le temps actifs)	Sanction financière de 400 000 euros

1.5.4 Contrat de licence de l'Utilisateur Final

Les contrats de licence de l'utilisateur final (CLUF), mieux connus sous l'acronyme anglais EULA (*End-User License Agreement*) sont des accords qui sont généralement rattachés à un logiciel distribué par des éditeurs indépendants. Avant que les utilisateurs finaux soient autorisés à installer ou à utiliser un logiciel qu'un éditeur veut rendre disponible à une large communauté d'utilisateurs, ces derniers devront accepter tous les termes du CLUF. [Muttik, 2016]

Les CLUFs conviennent des actions et droits qui peuvent être exécutés par un tiers. Ils peuvent renfermer une foule de renseignements, pouvant aller de la décision de mesurer de la

[52] https://www.cnil.fr/fr/bouygues-telecom-sanction-pecuniaire-pour-manquement-la-securite-des-donnees-clients accédé le 2019-01-13
[53] https://www.welivesecurity.com/2018/11/27/german-chat-site-faces-fine-gdpr/ accédé le 2019-01-13
[54] https://www.itgovernance.eu/blog/en/portuguese-hospital-appeals-gdpr-fine accédé le 2019-01-13

fréquence cardiaque aux minutes, jusqu'au partage des données de l'objet connecté utilisé à une entreprise filiale.

Quand on parle de la protection des renseignements personnels, le Rapport final du projet de recherche[55] présenté au Bureau de la consommation d'Industrie Canada cite :

> *(...) On trouve dans les CLUF des clauses qui autorisent, par exemple, les entreprises à collecter et à utiliser des données personnelles sans que la finalité précise de cette collecte ou de cette communication ne soit indiquée au consommateur. Les politiques de confidentialité que certaines entreprises s'engagent à respecter ne sont souvent accessibles qu'à la suite d'efforts et de détours considérables, les compagnies ignorant de ce fait leur obligation de faire des efforts raisonnables pour s'assurer que l'utilisateur est bien informé.*

En cas de litige, même si le consommateur croit qu'il peut se référer à ces contrats, la difficulté réside dans le fait que les CLUFs ne sont pas exécutoires et par conséquent il est difficile d'obtenir dédommagement face à une instance judiciaire en cas de besoin. Ces CLUFs n'apportent donc qu'une protection très limitée aux consommateurs de DPI.

La mesure dans laquelle les utilisateurs d'objets connectés pourront prendre des décisions éclairées en matière de protection de la vie privée dépendra en fin de compte de l'efficacité des politiques gouvernementales et d'autoréglementation.

1.5.5 Politiques de Confidentialité

Une politique de confidentialité[56] est un document à caractère légal qui explique comment une organisation traite les informations d'un client qui ont été collectées dans le cadre de ses opérations. Cette politique devrait habituellement :

[55] https://uniondesconsommateurs.ca/docu/rapports2009-2010/03-R10-CLUF-f.pdf accédé le 2018-05-22
[56] https://whatis.techtarget.com/definition/privacy-policy accédé le 2018-10-24

- Préciser quelles sont les informations personnelles collectées ainsi que toute autre information par rapport aux habitudes de navigation, téléchargements, historique de commandes, etc.
- Préciser si des informations (*cookies*) seront sauvegardées sur l'ordinateur utilisé
- Avec qui seront peut-être partagées les informations collectées.

La politique de confidentialité est gouvernée par des lois propres à chaque pays.

Des outils peuvent aider les entreprises et individus dans ce domaine. En particulier, il existe un générateur de politique de confidentialité[57] réalisé dans le cadre d'une recherche post-doctorale sur les mécanismes de production de la confiance dans les environnements électroniques. Ce générateur a été financé par la *Chaire L.R. Wilson*[58] *sur le droit des technologies de l'information et du commerce électronique* de l'Université de Montréal. Ce générateur permet à toute personne qui collecte des renseignements personnels via son site web, d'élaborer une politique de confidentialité retraçant ses engagements dans ce domaine.

[57] http://www.politiquedeconfidentialite.ca/questionnaire.php?action=commencer# accédé le 2018-12-18
[58] https://www.chairelrwilson.ca/a-propos/mission/ accédé le 2018-12-18

Chapitre 2. Les Dispositifs Portables Intelligents

Les dispositifs retrouvés dans l'IoT sont répartis en deux principales classes[59] :

La première classe (contrainte), celle qui nous intéresse dans le cadre de cette recherche, contient les appareils avec senseurs et transducteurs[60] qui ont besoin d'une passerelle pour communiquer leurs données. Ils requièrent une source d'alimentation électrique (batterie) et ont besoin de technologies sans fil à faible consommation, tel le *Bluetooth LE* (voir section 2.5.2.2), pour communiquer. On retrouve les DPI dans cette classe.

La seconde classe (non-contrainte), pour sa part, est une classe d'objets qui peuvent communiquer directement avec des serveurs centraux pour le stockage des données recueillies. Ils n'ont pas de contrainte d'alimentation électrique et peuvent supporter de multiples senseurs. Nous n'élaborerons pas plus sur cette dernière.

2.1 Introduction

Les DPI représentent tout objet connecté (de la classe des objets contraints) pouvant être porté sur le corps, tel un accessoire ou un vêtement. Les plus populaires sont les montres intelligentes et les bracelets électroniques, deux types d'objets connectés qui nous intéressent dans le cadre de cette recherche. Ces objets ont des senseurs qui capturent et émettent certaines données physiques ou environnementales de leur porteur. L'intérêt[61] commercial pour les DPI s'est accru avec l'arrivée de la récente version de la norme de communications sans fil *Bluetooth*[62] en 2010, et avec la disponibilité à grande échelle des téléphones intelligents[63].

[59] http://www.rfwireless-world.com/IoT/IoT-devices.html accédé le 2019-01-13
http://www.cisoplatform.com/profiles/blogs/classification-of-iot-devices accédé le 2019-01-13
[60] Dispositif assurant une conversion ou un transfert de signaux et dans lequel un signal au moins est de nature électrique (https://www.larousse.fr/dictionnaires/francais/transducteur/79088) accédé le 2019-01-13
[61] http://www.businessinsider.com/consumer-interest-in-wearables-is-picking-up-2017-12 accédé le 2018/05/11
[62] https://www.bluetooth.com/ accédé le 2018/05/11
[63] https://www.statista.com/statistics/203713/smartphone-penetration-per-capita-in-north-america-since-2000/ accédé le 2018/05/11

FIGURE 3 BRACELET ÉLECTRONIQUE (GAUCHE); MONTRE INTELLIGENTE (DROITE)
SOURCE: GETTYIMAGES.CA

La montre intelligente et le bracelet électronique (Figure 3) se portent toutes deux au poignet et mesurent des signes reliés à l'activité physique (par exemple la fréquence cardiaque, la distance parcourue, etc.) La montre intelligente offre en plus des applications pratiques telles un appareil photo, un agenda, un GPS et plusieurs autres. Bien que plus limité en termes de fonctionnalités, le bracelet électronique cible donc une clientèle plutôt axée sur le sport et l'activité physique[64].

L'intérêt général pour les montres et bracelets électroniques est indéniable et est en croissance. *International Data Corporation* [65] (IDC), une entreprise d'étude de marché en technologie, confirme une augmentation de plus de 10% du nombre d'unités vendues des DPI en 2017 par rapport au nombre vendu en 2016. Les goûts des utilisateurs pour ces objets sont de plus en plus sophistiqués et ces derniers orientent généralement leurs achats vers des marques reconnues telles que Apple[mc66], Fitbit[mc 67], Garmin[mc 68], ou Huawei[mc 69] pour n'en nommer que quelques-unes.

2.2 Avantages et Inconvénients

Autant ces dispositifs intelligents peuvent-ils avoir des caractéristiques intéressantes, autant peuvent-ils soulever de sérieuses inquiétudes : La quantité de données recueillies est sans précédent. Les biosenseurs capturent la fréquence cardiaque, la température corporelle, et même les mouvements. Ils peuvent aussi collecter des informations en rapport avec l'humeur, la qualité du sommeil et les émotions. Toutes ces données, lorsque qu'elles sont croisées avec des données

[64] https://www.wareable.com/wearable-tech/who-is-actually-buying-wearable-tech-887 accédé le 2018/05/12
[65] https://www.idc.com/getdoc.jsp?containerId=prUS43598218 accédé le 2018/05/11
[66] https://www.apple.com/ca/fr/watch/ accédé le 2018-12-18
[67] https://www.fitbit.com/fr-ca/home accédé le 2018-12-18
[68] https://www.garmin.com/fr-CA accédé le 2018-12-18
[69] https://consumer.huawei.com/ca-fr/wearables/watch2/ accédé le 2018-12-18

personnelles provenant d'autres sources ont un potentiel élevé d'inférences, de profilage et d'atteinte à la vie privée.

On est en droit de se poser plusieurs questions à propos de la nature des données collectées et transmises via l'application d'un DPI et si ces données sont protégées adéquatement de tiers ayant de mauvaises intentions. Plus encore, quel est le niveau de transparence du manufacturier ? Avons-nous accès à des cadres législatifs ou gouvernementaux pour nous protéger en cas de divulgation d'informations ou d'identification d'une personne ? Quelles seraient les conséquences dans une telle situation ?

Selon les principes de protection de la vie privée[70] retrouvés dans un rapport de recherche du CPVP les utilisateurs de DPI devraient pouvoir

> […] *exercer un contrôle sur leurs données et choisir de se soustraire à l'environnement « intelligent » sans pour autant subir de conséquences négatives*.

Selon [Talebi *et al.*, 2016] l'intrusion à la vie privée est devenue une menace potentielle majeure associée à la collecte, au suivi, au stockage et au partage de l'information. Pour tenter de contrer de telles menaces, on met beaucoup d'emphase sur les politiques de confidentialité de la vie privée surtout depuis que l'omniprésence de la technologie sème beaucoup de doute à propos de l'accès à l'information et comment cette dernière est utilisée. Malheureusement ces politiques varient grandement d'un fabricant à l'autre.

Dans certains cas, l'information provenant des DPI pourrait même servir à faire du profilage et de la discrimination au niveau de l'emploi, de l'éducation, des assurances, de la finance et des services sociaux [Montgomery *et al.*, 2016]. Un article de la revue *UndercoverRecruiter*[71] explique qu'un employeur peut utiliser efficacement les données extraites d'un DPI lors d'un processus de recrutement. L'employeur peut ainsi analyser rétroactivement la gestuelle du corps ainsi que les

[70] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/iot_201602/ accédé le 2018/05/12
[71] https://theundercoverrecruiter.com/wearable-tech-work/ accédé le 2019-01-13

réponses aux questions. Ceci aide à déterminer si le candidat a le profil recherché pour le poste convoité.

Bien que les DPI soient des produits innovateurs, ils ne sont pas développés avec la « sécurité-par-conception[72] » en tête (mieux connu dans le jargon technologique sous le nom de *secure-by-design*). En fait, il n'existe pas encore de règles et normes à propos de la sécurité dans l'*IoT*. Ceci rend donc les dispositifs vulnérables. Les vecteurs d'attaques se situent principalement au niveau:

- Des informations d'identification courantes par défaut
- De la configuration très basique des dispositifs
- Des mises à jour et rustines insécures qui doivent être appliquées manuellement
- Des vulnérabilités au niveau des applications web ou mobiles du dispositif

Chez Intel, dans le groupe de recherche sur la sécurité, on rapporte qu'un dispositif portable intelligent est habituellement développé en seulement six mois[73], de la planification jusqu'à sa mise en marché ce qui ne laisse que très peu ou pas de temps pour les évaluations de sécurité.

Quant au concept de « Protection de la vie privée dès la conception[74] » (*privacy-by-design*) il doit tenir compte des impacts à la vie privée tout au long du processus de développement du dispositif. C'est une notion au cœur du RGPD et elle implique beaucoup plus que d'assurer l'accès sécurisé aux données. En un mot, la vie privée est une question de contrôle i.e. permettre aux individus de garder un contrôle personnel sur leurs informations personnellement identifiables en ce qui concerne sa collecte, son utilisation et sa divulgation. Dans le cas des DPI, ce n'est pas simplement une bonne idée mais une intention très souhaitable pour toute organisation qui veut conserver la confiance de ses clients. [Cavoukian et Dixon, 2013]

Dans un contexte d'entreprise *BYOD* (*Bring Your Own Device*) , par exemple si vous désirez utiliser votre DPI personnel pour votre travail, ceci implique des risques de sécurité et ils sont similaires à ceux rencontrés par l'utilisation de téléphones intelligents personnels. Par exemple le jumelage d'une montre intelligente personnelle avec un téléphone intelligent administré par

[72] https://duo.com/decipher/uk-government-proposes-secure-by-design-guidelines-for-iot accédé le 2018-05-21
[73] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/are-your-wearables-fit-to-secure-you-researchers-outline-3-attack-surfaces accédé le 2018-05-21
[74] https://www.dpms.eu/rgpd/explication-privacy-by-design/ accédé le 2019-01-13

l'entreprise sera perçu comme un risque. Un voleur peut intercepter le flux Bluetooth entre la montre intelligente et sa passerelle, dérobant plusieurs informations sensibles stockées sur le téléphone intelligent et peut aller jusqu'à dérober des informations d'identité de connexion du client aux ressources d'affaires dans l'infonuagique (*cloud)*.

Une entreprise peut suivre un employé, savoir combien d'heures il a travaillé, combien de pauses ont été prises ainsi que beaucoup d'autres informations. En revanche, les employés qui refuseraient de se plier à ce genre de surveillance pourraient être perçus comme s'ils voulaient cacher quelque chose.

Les entreprises elles-mêmes sont sujettes à des violations des données qu'elles auraient collectées. Ces données contiennent énormément de détails de toutes sortes incluant le déplacement des employés, leurs habitudes, intérêts et même leurs informations de santé.

En 2016, Price-Waterhouse-Cooper[75] a sondé en ligne, 1000 résidents des États-Unis au sujet de la sécurité des DPI. Paradoxalement, ce rapport a révélé que les inquiétudes des consommateurs en lien avec la vie privée ont diminué (surtout en ce qui a trait aux montres intelligentes). Il est donc urgent de proposer une sensibilisation afin d'améliorer le niveau d'éducation des individus sur ce sujet essentiel.

En Novembre 2017, la BBC annonçait dans un article de presse [76] la décision de l'Allemagne de bannir les montres intelligentes pour les enfants. Ces montres, munies d'un GPS, donc capables de retourner la position de leur propriétaire, ont été perçues comme des cibles à l'espionnage parce que les données qui étaient transmises par la majorité d'entre elles, n'étaient même pas chiffrées.

Il y a cependant des bons côtés aux DPI: La revue ITPRO rapportait dans un article du 30 avril 2018[77] qu'il y a une tendance importante des DPI liée aux programmes de forme physique de certaines grandes entreprises. Ces entreprises prennent des ententes avec des compagnies d'assurances et préparent des programmes d'entrainement appropriés dans le but de maintenir une bonne santé chez les employés, réduisant les coûts pour l'employeur.

[75] https://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-cis-wearables.pdf accédé le 2018-05-21
[76] http://www.bbc.com/news/technology-42030109 accédé le 2018-05-20
[77] http://www.itpro.co.uk/business-strategy/31017/how-wearable-tech-is-helping-to-save-lives accédé le 2018-05-21

En Angleterre, le consortium [78] « myCareCentric Epilepsy » en collaboration avec le « *Public Health England* » (PHE) a rapporté une augmentation de 70% du nombre de décès de patients épileptiques entre 2001 et 2014. C'est pourquoi, en collaboration avec la plateforme *Azure* de *Microsoft*, ce consortium fournit aux patients atteints d'épilepsie une technologie permettant la collecte de données sur la santé afin d'alerter le personnel médical de toute complication et tendances lors de crises.

Même si l'utilisation de technologie avec les enfants demeure un sujet controversé, l'entreprise américaine *Good Parents Inc*. propose un DPI avec capteurs spécifiquement construit pour les enfants de 3 à 10 ans d'âge. Le dispositif : *Kiddo*^{mc} [79] monitore les principaux signes vitaux (température corporelle, fréquence cardiaque, sommeil, activité, transpiration et nutrition) et détecte les *patterns* inhabituels de telle sorte que les parents puissent utiliser ces informations pour prendre des actions appropriées. L'application utilise l'apprentissage-machine (*machine-learning)* afin d'être en mesure de représenter l'état « normal » pour l'enfant. En situation anormale, les parents reçoivent un avertissement par le biais d'un message. L'application peut aussi faire des suggestions.

2.3 Fonctionnement

Dans le but de bien comprendre les enjeux de sécurité, il est important d'avoir une certaine connaissance de l'architecture informatique matérielle[80] des DPI (Figure 4). En plus de représenter le dispositif en blocs communicants, celle-ci nous permet de visualiser les endroits où l'information est échangée avec l'extérieur.

[78] https://www.poole.nhs.uk/about-us/latest-news/2018-news/new-tech-could-save-nhs-%C2%A3250m.aspx accédé le 2019-01-13
[79] http://www.kiddowear.com/ accédé le 2018-05-21
[80] https://www.embedded.com/design/real-world-applications/4431259/2/The-basics-of-designing-wearable-electronics-with-microcontrollers accédé le 2018-05-14

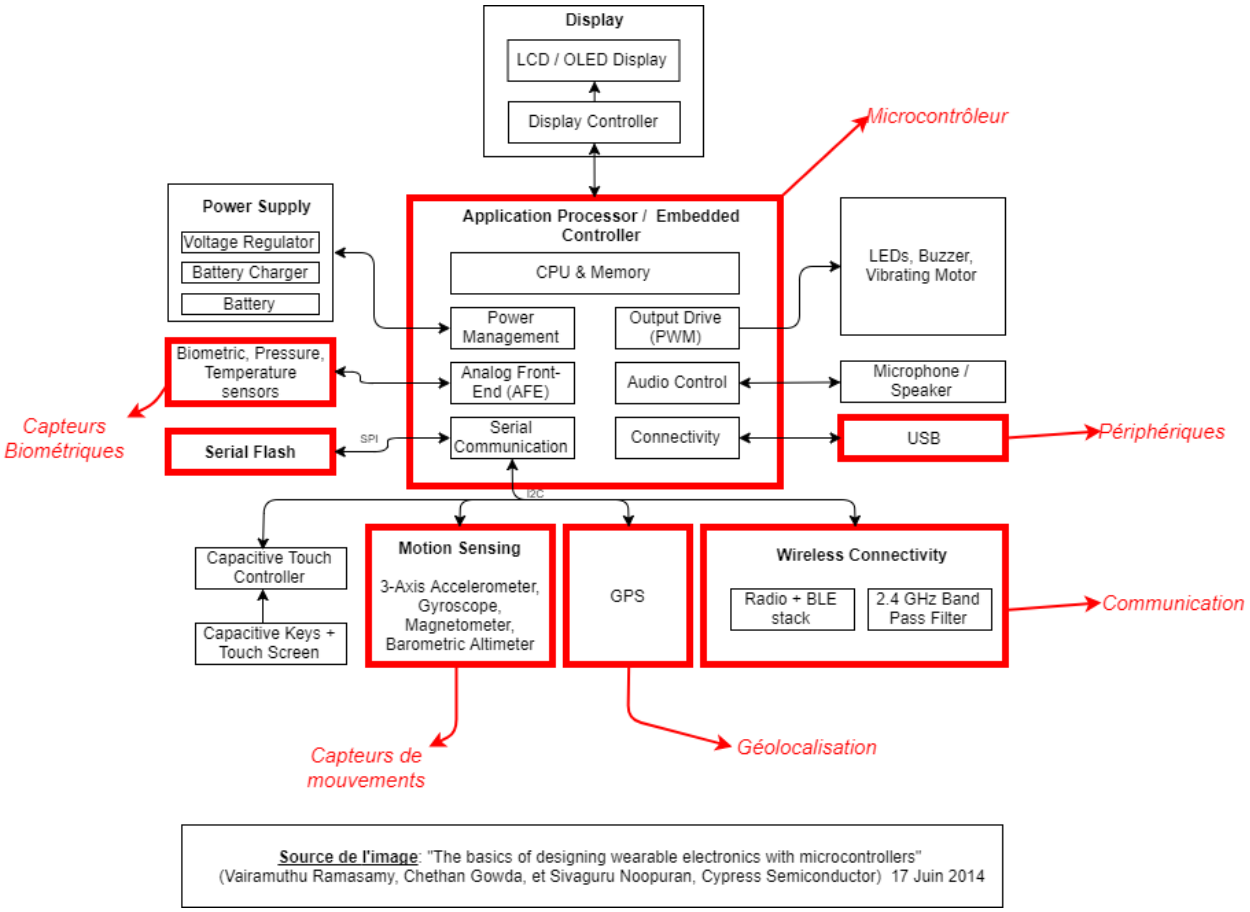


FIGURE 4 ARCHITECTURE MATÉRIELLE (DISPOSITIF PORTABLE INTELLIGENT)

Le microcontrôleur [81] est le cœur du DPI. Il combine l'unité centrale de traitement, la mémoire et autres interfaces donnant accès en entrée/sortie aux différents capteurs et périphériques tels que décrits au Tableau 3.

[81] https://internetofthingsagenda.techtarget.com/definition/microcontroller accédé le 2018-05-15

TABLEAU 3 CAPTEURS ET PÉRIPHÉRIQUES D'UN DISPOSITIF PORTABLE INTELLIGENT

Fonctionnalité	Interface	Détails
Capteurs biométriques	Signaux analogiques envoyés au microcontrôleur via un AFEC (*Analog Front-End Controller* ou contrôleur frontal analogique).	Fréquence cardiaque, Fréquence respiratoire, Pression sanguine, Température corporelle, Sueur
Capteurs de mouvements	Signaux reçus via un bus I^2C (bus série et synchrone). Permet d'attacher des circuits intégrés à faible vitesse à des microcontrôleurs sur de courtes distances.	**Accéléromètre** (enregistre l'accélération linéaire et dynamique dans un environnement 3D) **Gyroscope** (capteur de position angulaire) **Magnétomètre** **Vibrateur** (*linear motion*)
Géolocalisation		**GPS** **Magnétomètre** (mesure du champ magnétique ex : boussole)
Communication		**Bluetooth LE** (*low-energy*) **WiFi** **Carte SIM** (Téléphone 3G/4G) **NFC** (*Near Field Contact* ex : Paiement mobile) **RFID**
Périphériques	USB (Universal Serial Bus) : permet le branchement de périphériques externes au microcontrôleur.	Caméra Transfert de données

La présence de nombreux capteurs exige que les données convergent vers un concentrateur de données (*data hub*), rôle habituellement joué par un téléphone intelligent. Elles sont ensuite acheminées par Internet à un centre de données (*data center*) dans l'infonuagique (*cloud*). A cet endroit, les données peuvent faire l'objet de recherches et calculs statistiques ou de forage de données (*data mining)* sans compter la possibilité qu'elles soient partagées, moyennant une autorisation du propriétaire.

2.4 Connectivité / Communication

Il y a une grande variété de dispositifs qui peuvent être considérés comme portables mais il est aussi important de savoir à quel réseau ils appartiennent [Mishra, 2015]

Le réseau le plus près de l'humain est le « *Body Area Network* » ou *BAN* qui est un réseau sans fil peuplé par les dispositifs portables portés en surface ou même potentiellement implantés à l'intérieur du corps. Ces dispositifs font la collecte de données biométriques pour les envoyer à un DPI avec accès à des capacités en calcul et stockage sur Internet, généralement par le biais d'un téléphone intelligent qui en reçoit les données par la technologie *Bluetooth*[82]. En l'absence de téléphone intelligent, il est possible, pour certains bracelets électroniques par exemple, d'être jumelé par *Bluetooth* à un ordinateur portable.

Certaines montres intelligentes plus récentes bénéficient de la technologie 4G LTE[83]. Ceci signifie que la montre a une connexion en continu à un réseau de téléphonie mobile sans passer par un téléphone intelligent. Les applications sont donc fonctionnelles là où le WiFi n'est pas disponible et ont un accès direct à l'Internet avec un débit de crête de quelques centaines de mégabits par seconde.

En général, la communication entre les dispositifs du BAN et le DPI (montre ou bracelet) utilise le protocole *Bluetooth LE (Low-Energy)* qui est une version récente de *Bluetooth* ayant dans sa visée, de nouvelles applications en santé, la mesure de l'activité physique, la sécurité et la domotique. Certains dispositifs de collecte de données de DPI communiquent par le protocole ANT+[84]; c'est le cas pour les dispositifs intelligents des compagnies Garmin^{mc} (compagnie parent de ANT), Adidas^{mc}, Fitbit^{mc}, Nike^{mc} pour ne nommer que les plus connus.

Le réseau créé et centré sur la personne utilisant un *DPI* est connu sous le nom de PAN ou WPAN[85] (*Wireless Personal Area Network*) où on y utilise habituellement les technologies de

[82] https://www.bluetooth.com/ accédé le 2018/05/15
[83] https://www.futura-sciences.com/tech/definitions/technologie-4g-14703/ accédé le 2018-05-25
[84] https://www.thisisant.com/ accédé le 2018-05-25
[85] https://www.computerworld.com/article/2483791/emerging-technology/what-wearable-computing-is-really-all-about.html accédé le 2018-05-15

communication Bluetooth, Wi-Fi[86], NFC[87] et 3G/4G LTE. Le BAN est un sous-ensemble du WPAN (Figure 5).

Le GSMA[88], organisation qui représente les intérêts des opérateurs de réseaux mobiles partout dans le monde (près de 800 opérateurs et 300 entreprises) travaille actuellement à l'élaboration de la technologie 5G[89] qui devrait être déployée d'ici 2020. Le réseau 5G permettra aux DPI de communiquer en moins d'une milliseconde soit cinquante fois plus rapidement qu'avec une technologie 4G. On parle donc ici d'une connectivité en temps réel, permanente. Les DPI pourront ainsi faire l'acquisition des données d'une plus grande quantité de senseurs. C'est pourquoi on dit que c'est la technologie d'avenir de l'*IoT* parce qu'on l'utilisera pour déployer en masse une quantité phénoménale d'objets connectés.

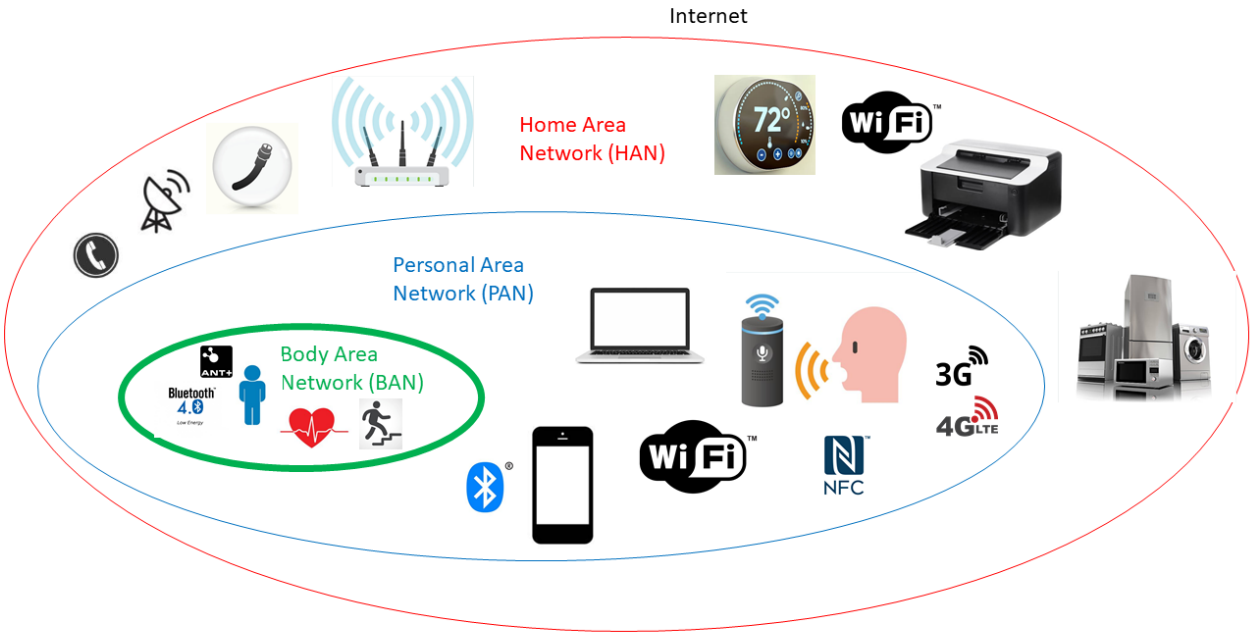


FIGURE 5 REPRÉSENTATION SPATIALE DES RÉSEAUX
IMAGES ISTOCKPHOTO.COM

[86] https://standards.ieee.org/findstds/standard/802.11-2016.html accédé le 2018-05-15
[87] http://nearfieldcommunication.org/ accédé le 2018-05-15
[88] https://www.gsma.com/ accédé le 2018-05-25
[89] https://www.gsma.com/futurenetworks/technology/understanding-5g/ accédé le 2018-05-25

Le Bluetooth au niveau du WPAN lie le DPI au téléphone intelligent (Figure 6). Les technologies WiFi et 3G/4G sont plutôt utilisées comme des moyens directs ou indirects de joindre l'Internet, là où les ressources de l'infonuagique (*cloud* [90]) sont disponibles. Enfin, quand la technologie NFC est présente, celle-ci permet le paiement par contact.

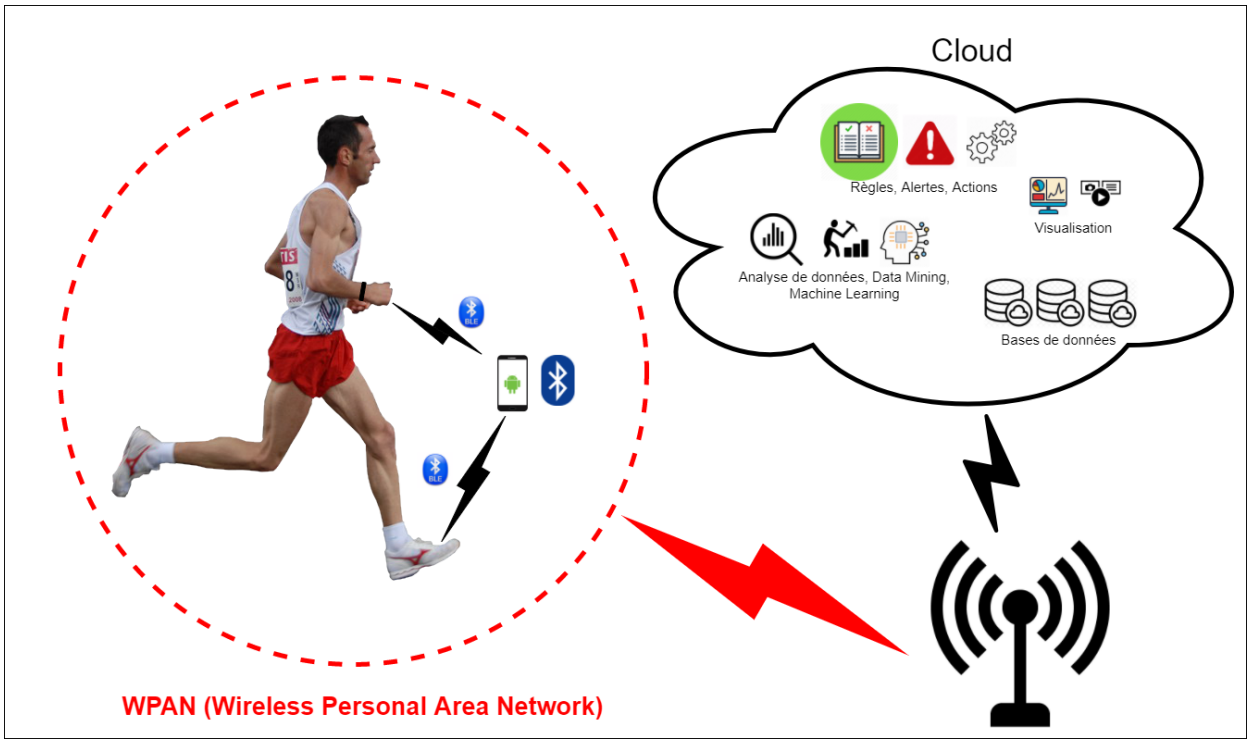


FIGURE 6 « CLOUD » PERSONNEL D'UN DISPOSITIF PORTABLE INTELLIGENT

2.5 Sécurité

2.5.1 Généralités

Un article de [Karakaya *et al*., 2016] nous brosse un tableau des enjeux de sécurité des DPI. Les montres et bracelets, qui viennent habituellement avec une application résidant sur un téléphone intelligent, ont un accès direct au monde extérieur via l'Internet. En conséquence, ceci ouvre une porte aux pirates (*hackers*) qui recherchent par exemple les données de positionnement,

[90] https://azure.microsoft.com/fr-ca/overview/what-is-cloud-computing/ accédé le 2018-05-25

messages et autres informations sensibles. Ces dispositifs deviennent aussi de plus en plus intéressants à pirater à mesure que leurs capacités de stockage et de communication augmentent.

Une étude[91] de l'entreprise Hewlett-Packard complétée en Juillet 2015 démontre que la totalité (100%) d'une dizaine de montres testées présentent des faiblesses marquées au niveau de l'authentification, du manque de chiffrement, de l'interface-utilisateur, de la protection des mises-à-jour du *firmware* et de la protection de la vie privée.

L'accès aux différents capteurs (ex : accéléromètre et gyroscope) d'un DPI est possible et ce, sans privilèges, permettant une identification assez précise des activités [Perez et Zeadally, 2018]. Mais la principale vulnérabilité émerge de la communication Bluetooth qui est utilisée pour la transmission et la réception de données au téléphone intelligent. Dans l'industrie, les enjeux de sécurité avec la technologie Bluetooth sont bien connus [Hassan *et al.*, 2017]. Un attaquant qui est en mesure d'avoir accès au téléphone intelligent par ce lien a conséquemment accès à une quantité considérable de données personnelles.

Exemple particulier : Il existe un phénomène connu associé au Bluetooth : « Transfusion de données » [Lee *et al.*, 2017]. Il survient au moment du jumelage Bluetooth alors que l'hôte (téléphone intelligent) envoie une copie de données secrètes/privées de l'utilisateur au dispositif jumelé dans le but d'effectuer d'éventuelles actions. La nature de ces données et la quantité transmise ne sont pas clairement connues [Lee *et al.*, 2018] mais on sait qu'elles servent éventuellement à des fins d'initialisation et de personnalisation. Ainsi, un adversaire qui vole le DPI d'une personne serait en mesure d'accéder à ces données secrètes.

Les attaques peuvent être résumées comme suit (Tableau 4) :

[91] http://www8.hp.com/us/en/hp-news/press-release.html?id=2037386#.WwgZs0jt5nI accédé le 2018-05-25

TABLEAU 4 PRINCIPALES ATTAQUES "INTELLIGENTES" SUR LES DPI
[LIU ET SUN, 2016]

Attaque	Spécialité
MITM (man-in-the-middle)	Modification des données en transit entre le DPI et le téléphone intelligent.
Injection de code malicieux	Prise de contrôle de certains capteurs
Attaque de firmware	Contrôle complet du DPI
Attaque « mule »	Les activités enregistrées ne sont pas réellement effectuées par le propriétaire. De telles attaques permettent au DPI de pouvoir enregistrer une mesure correcte à partir de faits fabriqués (par exemple : attacher un bracelet à un équipement motorisé)
Attaque « MoLe » (*Motion Leaks*)	Reconnaissance d'informations sensibles entrées au clavier par le mouvement de frappe de la personne.
Injection du compte de l'utilisateur	La protection par mot de passe n'est possible seulement que si le DPI n'est pas jumelé (Bluetooth) avec le téléphone intelligent. Quand il est jumelé, les données peuvent être accédées par le port micro-USB.

2.5.2 Protocoles de communication du BAN (Body Area Network)

Le BAN présente une topologie réseau en étoile: les capteurs sont répartis sur le corps et envoient leurs données à un collecteur centralisé (DPI). Les nœuds du BAN ont une taille plus petite et sont contraintes en termes de ressources. Pour cette raison, les systèmes d'échanges de clés pour les réseaux BAN doivent être légers et consommer encore moins d'énergie que ceux conçus pour les réseaux de senseurs sans fil. [Kompara et Hölbl, 2017]

Il existe donc deux protocoles de communication largement répandus qui servent à cette fin et nous les présentons ici.

2.5.2.1 ANT+ :

ANT+ est un protocole de communication sans fils opérant sur la bande de fréquence de 2.4 GHz. Il est utilisé par le DPI pour communiquer avec les différents capteurs. ANT+ est petit et

ne demande que très peu d'énergie. Il a cependant plusieurs faiblesses au niveau de la sécurité : il n'est pas chiffré et bien qu'il en offre la possibilité (AES[92] sur 128 bits) il devient alors limité à un seul canal de communication car il exige alors une plus grande consommation électrique. ANT+ n'offre aucune authentification des messages, ce qui est crucial pour l'intégrité des données sur les réseaux sans fils. Ce protocole est vulnérable aux attaques pseudo-MITM[93]. [Camelo *et al.*, 2015]

2.5.2.2 Bluetooth LE [94] (Low-Energy) :

Bluetooth LE (BLE) est un protocole de communication sans fils opérant lui aussi sur la bande de fréquence de 2.4 GHz. Comme toute technologie sans fil, BLE ne fait pas exception aux menaces de sécurité telles que le suivi des périphériques, l'espionnage et les attaques *Man-In-The-Middle* (MITM). En effet, les périphériques BLE diffusent l'adresse *Media Access Control* (MAC[95]), le *Universal Unique IDentifier* (UUID[96]) et de l'information de service à intervalle régulier. En raison de cette diffusion, les adversaires peuvent facilement suivre l'appareil et décoder les informations de diffusion en utilisant un renifleur ou même un téléphone intelligent. BLE ne requiert pas d'authentification pour le jumelage d'un capteur à un DPI.

Si un attaquant MITM actif écoute la clé publique partagée pendant le processus de jumelage initial et décide plutôt de partager sa propre clé publique au lieu de la clé publique réelle, alors le périphérique qui a reçu la clé publique de l'attaquant n'a aucune connaissance de la source de la clé et va chiffrer et envoyer le message en utilisant la clé publique partagée par l'attaquant. L'adversaire peut alors déchiffrer les messages et les interpréter. En outre, il peut éventuellement décider de chiffrer le message à l'aide de la clé publique d'origine et ensuite le remettre à l'initiateur pour maintenir la communication intacte.

La version 4.2 de BLE introduit un nouveau modèle de sécurité avec le jumelage sécuritaire. Les techniques de sécurité telles que le masquage des adresses MAC, l'échange de clés basé sur les courbes elliptiques Diffie-Hellman [Vasundhara, 2017] et les connexions sécurisées garantissent

---

[92] https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard accédé le 2019-01-14

[93] Un adversaire est capable de forger la communication dans le but de stopper une synchronisation (capteur vs DPI) et ensuite initier une nouvelle synchronisation entre les deux cibles. Ceci a le même effet qu'une attaque MITM traditionnelle à l'exception qu'elle serait perceptible par les cibles.

[94] https://www.design-reuse.com/articles/39779/security-considerations-for-bluetooth-smart-devices.html accédé le 2018-05-25

[95] https://www.lemagit.fr/definition/Adresse-MAC accédé le 2019-01-14

[96] https://searchmicroservices.techtarget.com/definition/UUID-Universal-Unique-Identifier accédé le 2019-01-14

la sécurité. Ainsi, ces nouvelles spécifications ont permis d'adopter des approches plus intelligentes en matière de confidentialité pour ces appareils. A présent, BLE est considéré comme sûr.

2.5.3 Le WPAN (Wireless Personal Area Network)

Un WPAN ou « réseau personnel sans fil » est un type de réseau personnel qui utilise les technologies de communication sans fil pour communiquer et transférer des données entre les périphériques connectés de l'utilisateur. Il permet à une personne de connecter ensemble la plupart de ses appareils et d'accéder à Internet ou à un réseau local à l'aide de l'une des techniques de communication sans fil natives / prises en charge.

En règle générale, les périphériques du WPAN comprennent des périphériques et des appareils portatifs tels que des assistants personnels, des téléphones intelligents et des tablettes.

2.5.3.1 NFC :

Near Field Communication (NFC[97]) est une technologie sans fil permettant le transfert de données entre dispositifs sur une très courte distance (une dizaine de centimètres au maximum). On l'utilise en général pour effectuer des paiements. La communication a lieu quand les deux dispositifs, tous deux compatibles avec la norme RFID (opération à 13,56 MHz), sont tout près l'un de l'autre. Parce que la distance de transmission est petite, on peut présumer que NFC est une technologie sécuritaire. L'échange de données est chiffré, donc l'espionnage, l'interception et la manipulation ne sont donc pas des options viables. [Kennedy et Hunt, 2008]

2.5.3.2 Technologie 4G LTE :

Les DPI utilisant la technologie 4G LTE (pas besoin de jumelage avec un téléphone intelligent) ont un niveau de sécurité[98] qui est bâti à partir des caractéristiques qu'on retrouve dans les technologies de connexion 2G et 3G. Les fournisseurs de service y ajoutent des options de chiffrement multiple ainsi que des schèmes d'authentification (pour l'utilisateur et le DPI). Ce ne sont que quelques éléments et la liste est loin d'être exhaustive, alors on peut aisément conclure que la technologie 4G LTE est sécuritaire. Comme elle sera encore présente pour quelque temps, les fournisseurs continueront potentiellement d'y ajouter d'autres éléments de sécurité. Il existe

[97] http://nearfieldcommunication.org/ accédé le 2019-01-14
[98] https://opengear.com/articles/just-how-secure-4g accédé le 2018-05-25

bien sûr des menaces[99] connues telles que les attaques de renégociation, le « *tracking* » d'identité, l'interception d'appels, le brouillage mais ce sont des attaques qui sont valides aussi pour les téléphones intelligents et pour lesquelles les DPI n'y peuvent rien de plus.

2.5.3.3 WiFi :

Les DPI qui ont un accès direct à un réseau WiFi (sans passer par un téléphone intelligent) sont dépendants de la sécurité appliquée à cette technologie. Aujourd'hui les communications WiFi utilisent la norme WPA (WiFi Protected Access) et préférablement WPA2. Cette norme utilise un chiffrement symétrique basé sur AES[100] utilisant une clef de 256 bits.

Les accès non-autorisés sont possibles. Parmi ceux-ci on peut citer les associations malicieuses, le *spoofing* de l'adresse MAC[101], les attaques MITM[102], ou le déni de service (DoS[103]).

WPA2 était jusqu'à récemment amplement suffisant afin de garantir une confidentialité maximale, mais en octobre 2017, le chercheur Mathy Vanhoef a dévoilé l'attaque Krack[104] (*Key Reinstallation Attacks*), réduisant à néant la sécurité pour tous les terminaux WiFi protégés par le protocole de chiffrement WPA2. Concrètement, les attaquants peuvent utiliser cette nouvelle technique d'attaque pour lire des informations qui étaient auparavant supposées être chiffrées en toute sécurité. Ils peuvent ainsi voler des informations sensibles telles que des numéros de carte de crédit, des mots de passe, des messages de discussion en ligne, des courriels, des photos, etc.

Le consortium WiFi Alliance[105] vient cependant de lever le voile sur le nouveau protocole WPA3 qui permet d'améliorer la sécurité offerte par WPA2 et qui adresse directement les problèmes soulevés par l'attaque Krack. Il protège contre les attaques par force brute et offre une confidentialité persistante (*forward-secrecy*[106]).

---

[99] https://www.rsaconference.com/writable/presentations/file_upload/tech-r03_lte-security-how-good-is-it.pdf accédé le 2018-05-25

[100] https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard accédé le 2018-05-25
[101] https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-le-mac-spoofing/ accédé le 2018-12-19
[102] https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html accédé le 2019-01-15
[103] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos accédé le 2018-12-19
[104] https://www.krackattacks.com/ accédé le 2018-12-19
[105] https://www.wi-fi.org/ accédé le 2018-12-19
[106] http://fracademic.com/dic.nsf/frwiki/1889739 accédé le 2018-12-19

2.5.4 Cloud

L'infonuagique (*cloud*) est une évolution majeure de l'informatique. Cette technologie permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels. Les données, au lieu d'être stockées sur vos disques durs ou mémoires, sont disponibles sur des serveurs distants et accessibles par Internet.

Le stockage dans le *cloud* permet une plus grande accessibilité des fichiers étant donné que l'information peut être accédée n'importe quand, à partir de n'importe où, tant qu'on a un accès à l'Internet. C'est probablement à cause de cette caractéristique qu'on peut penser que le *cloud* est un secteur où la sécurité revêt le plus d'importance. On peut y retrouver de l'information dont la valeur est importante et qui nous identifie personnellement.

La synchronisation des données dans le *cloud* présente des risques. Parmi ceux-ci on y retrouve les *DDoS*[107] [Deshmukh et Devadkar, 2015], les injections SQL[108] et les attaques « back-door »[109]. Ce sont des attaques qui finissent en fuites importantes de données pour les individus et les entreprises.

2.5.5 Intégrité des Données

Même si les DPI sont souvent des objets destinés aux loisirs, il est louable de se questionner sur la nécessité de garantir l'intégrité des données. Pour démontrer certains faits, il peut être fortement souhaitable d'avoir des données intègres. La littérature sur le sujet fait même état de cas où certaines données ont été amenées comme preuves dans une cour de justice.

Dans un article [110]de la revue *Wired* de Décembre 2014, on rapporte un cas réel à propos d'une femme de Calgary qui a fait une réclamation pour blessure corporelle à la suite d'un accident de voiture, quatre ans auparavant (i.e. vers 2010). A l'époque elle était entraîneure personnelle. Ses avocats ont soumis les données de son bracelet Fitbit pour montrer que son mode de vie avait

[107] https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack accédé le 2018-05-27
[108] https://www.techopedia.com/definition/29781/sql-injection-attack accédé le 2018-05-27
[109] https://searchsecurity.techtarget.com/definition/back-door accédé le 2018-05-27
[110] https://www.wired.com/2014/12/wearables-in-court/ accédé le 2019-01-15

radicalement tombé au-dessous de la moyenne pour les femmes d'un groupe démographique similaire.

Citons en exemple les DPI de la compagnie Garmin[mc] (Figure 7) qui n'utilisent pas[111] le protocole HTTPS[112] dans la majorité de leurs applications et qui, en plus, utilisent OAuth 1.0[113] pour l'authentification de l'utilisateur. Le fait d'utiliser OAuth 1.0 sans HTTPS donne la possibilité à des tiers de capturer les requêtes d'utilisateurs et de les trafiquer.

Bien qu'ils utilisent HTTPS, certains bracelets et trackers (ex : Bellabeat LEAF, Jawbone UP), (Figure 7) sont vulnérables aux données forgées par un tiers trompant ainsi le serveur sur l'origine exacte du DPI. HTTPS n'assure qu'une communication sécurisée et n'offre aucune protection en rapport à l'abus sur les données.

FIGURE 7 LA SÉRIE GARMIN VIVO, LE BELLABEAT LEAF, ET LE JAWBONE UP

2.5.6 Vol – Perte

La petite taille des DPI fait que ce sont des objets qui peuvent être facilement égarés ou même volés ajoutant au risque supplémentaire de perte d'informations personnelles contenues à l'intérieur du dispositif lui-même. Cette situation est aggravée par le fait que ces DPI n'ont pas tous prévu de mécanisme d'identification (*login*) et que les données ne sont pas chiffrées, ce qui représente un réel danger et parce que la qualité des technologies vidéo et audio des montres intelligentes d'aujourd'hui surpassent celles des outils professionnels d'espionnages d'il y a

[111] https://openeffect.ca/reports/Every_Step_You_Fake.pdf à la page 27 accédé le 2018-12-19
[112] https://www.techopedia.com/definition/5361/hypertext-transport-protocol-secure-https accédé le 2018-05-27
[113] https://oauth.net/core/1.0/ accédé le 2018-05-27

quelques années, la possibilité qu'un dispositif contienne des images et vidéos pouvant porter atteinte à la vie privée est aussi une réelle possibilité. Plus un DPI contient des données d'informations personnelles, sur l'entourage, par rapport à l'état de santé, le numéro de carte de crédit et la localisation, plus les gens devront se préoccuper de leur sécurité.

2.6 Divulgation d'Informations

Une cause inhérente d'atteinte à la vie privée des DPI est expliquée par leur connexion au *cloud* ou à l'Internet. Cela fait partie de la nature-même des objets connectés et ouvre grand la porte aux fuites de données.

Comme il a été déjà mentionné, l'absence généralisée d'authentification des dispositifs fait que l'accès aux données stockées localement est d'autant facilité et soulève de sérieuses préoccupations par rapport à l'abus d'individus malicieux. Selon [Shrestha et Saxena, 2017] les menaces à la vie privée se retrouvent généralement dans les catégories suivantes :

- Accès sans entrave : facilité d'accès au dispositif (accès physique), et aussi causé par l'absence d'authentification.
- Reniflage des données de capteurs : les données émanant des capteurs ne sont pas chiffrées.
- Attaques par canal latéral : habileté à prendre le contrôle des capteurs.
- Spectateurs : Visualiser les mouvements ou les informations entrées dans l'intention de les répéter.
- Fuite d'informations : du site web du fabricant ou sur les réseaux sociaux, par exemple.

Afin de pouvoir atteindre leur plein potentiel opérationnel, les DPI requièrent qu'une portion de leur utilisation soit réalisée en ligne. Pour ce faire, leur propriétaire doit auparavant accepter la totalité du contenu des politiques de service et de confidentialité. Il peut arriver que ce dernier oublie qu'il avait donné des permissions d'accès à certaines applications qui synchronisent les données reçues avec des services tiers dans le *cloud*, ce qui potentiellement pourrait attenter à sa vie privée.

La vie privée est effectivement une préoccupation grandissante pour beaucoup de personnes et elle se traduit souvent en craintes au niveau du stockage et du partage d'informations personnelles. Le fait de divulguer des informations personnelles rend les utilisateurs de DPI vulnérables à de multiples variétés d'atteintes à la vie privée. Quoiqu'il en soit, les gens continuent

à utiliser leur DPI (montre, bracelet ou autre) et à en partager les données sur les sites du fabricant, dans le *cloud* ou sur les réseaux sociaux. Cette contradiction entre la préoccupation et le partage de l'information est appelée le « *paradoxe de la vie privée* »[114].

Afin de mieux comprendre les intentions derrière la divulgation d'informations personnelles, [Talebi et al, 2016] ont élaboré un modèle (Figure 8) basé sur cinq hypothèses fondamentales en vie privée et qui sont applicables dans un contexte d'utilisation de DPI :

H1 : Il y a une relation négative entre la préoccupation par rapport à la vie privée et la divulgation d'informations personnelles. Les utilisateurs qui sont soucieux de leur vie privée révèlent moins d'informations personnelles que les non-initiés dans le domaine.

H2 : Il y a une relation négative entre la perception de possession d'informations personnelles et la volonté de les divulguer. Plus les utilisateurs croient posséder d'informations personnelles, moins ils vont vouloir les divulguer.

H3 : Il y a une relation positive entre les normes subjectives et la divulgation d'informations personnelles. Dû à la croissance d'utilisation des DPI et de leurs applications, et à cause des bénéfices découlant de leur utilisation, les utilisateurs se motivent mutuellement entre eux pour faire de même.

H4a : Il y a une relation négative entre l'énoncé de confidentialité et la préoccupation des utilisateurs par rapport à la vie privée. Plus les utilisateurs perçoivent que l'énoncé de confidentialité de l'entreprise les protège, moins ils ressentiront de préoccupations à divulguer des informations personnelles.

H4b: Il y a une relation négative entre la possibilité de personnalisation des éléments de la vie privée et les préoccupations des utilisateurs par rapport à la vie privée. Plus une application permet de personnalisation à ce niveau, plus la préoccupation de l'utilisateur sera réduite.

[114] Le paradoxe de la vie privée est une conséquence de la demande concurrente d'utiliser les technologies de l'information (y compris les technologies sociales et les logiciels sociaux) et de se protéger des menaces potentielles à la sécurité personnelle et à la vie privée résultant de l'utilisation abusive des informations disponibles. https://www.igi-global.com/dictionary/privacy-paradox/37939 accédé le 2018-05-30

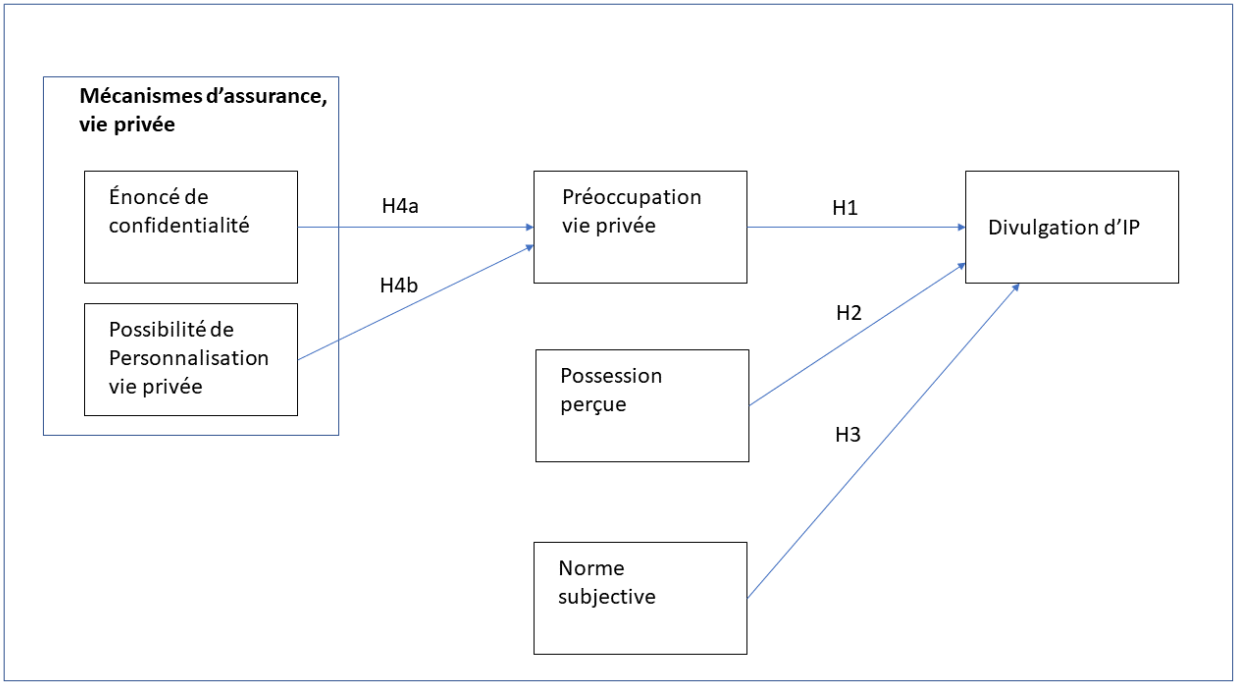


FIGURE 8 MODÈLE DE RECHERCHE SUR LA VIE PRIVÉE [TALEBI ET AL, 2016]

Il est essentiel que les données recueillies par les DPI soient chiffrées et anonymisées avant leur partage. Les données non anonymisées, stockées dans l'infonuagique, pourraient révéler des informations personnelles sensibles. Ces données sont prisées à un point tel que le risque qu'elles soient dérobées est élevé. Par conséquent les entreprises vont jusqu'à se procurer des assurances en cas d'incident de violation de données [Vijayaraghavan et Agarwal, 2018].

Tout comme la détermination de l'emplacement est devenue un élément essentiel des communications personnelles, la détection de présence et les technologies tenant compte de la localisation sont la clé du succès[115] à long terme de *l'IoT*. La localisation d'un objet peut aussi être vue comme un aspect important à considérer pour l'anonymat dans le contexte de *l'IoT*.

Cette localisation est normalement rendue possible par le moyen du GPS[116] mais il existe beaucoup d'autres méthodes qui n'ont pas besoin du GPS : elles sont basées sur un ensemble de technologies disponibles partout dans *l'IoT*. On parle ici de BlueTooth LE, WiFi, capteurs géomagnétiques et capteurs à bande ultra-large. Certaines techniques comme la micro-localisation

[115] https://www.iotforall.com/future-geolocation-multi-technology/ accédé le 2019-01-15
[116] https://www.futura-sciences.com/tech/definitions/technologie-gps-1897/ accédé le 2018-05-19

[Zatari et al., 2016], technologie sans fil, utilisant un émetteur-récepteur (*transceiver*) à basse consommation électrique, peut retourner la position basée sur la détection d'objets tagués, avec une précision de l'ordre du centimètre.

Dans un rapport[117] du *« Center for digital democracy - School of Communications American University – Washington DC »* on cite que les DPI envoient constamment des signaux qui permettent aux entreprises de publicité (ou autres) de saisir l'opportunité de géolocaliser une personne, par le biais du GPS intégré dans son téléphone intelligent, le Wifi et les communications Bluetooth. Conséquence de ceci, des firmes spécialisées en marketing de données ont misé sur cette fonctionnalité. Elles utilisent les technologies d'apprentissage machine afin de rendre possible le « *on-the-go targeting »* ou *« geo-fencing »*[118]

Le bracelet Jawbone[mc], par exemple, transmet la latitude et la longitude de son propriétaire pendant que l'application mobile associée est ouverte i.e. lors d'événements préconfigurés ou lors d'une synchronisation du dispositif. Cette géolocalisation est produite avec une précision de 14 décimales, ce qui retourne une position à quelques millimètres près [Hilts *et al.*, 2016].

Le secret étant la base de la vie privée, les manufacturiers travaillent très fort pour en savoir le plus possible sur chaque personne [Cellary, 2013]. Cette connaissance est requise afin de mieux servir les individus mais aussi pour en tirer des avantages et profits. Les atteintes à la vie privée visent à identifier la susceptibilité d'une personne à différentes propositions. En ce sens, dans ce que nous avons vu jusqu'à maintenant, le simple cas de vendre des données personnelles à un tiers, serait un cas de trahison. Il est donc très raisonnable de se questionner dans quelle mesure une personne devrait faire confiance à un manufacturier de DPI, compte tenu du risque potentiel de trahison.

Un premier moyen d'en savoir plus sur un individu est d'identifier de la manière la plus précise et la plus opportune possible ses besoins, mais le manufacturier peut aussi chercher à identifier ses faiblesses. Bien que toutes ces informations soient acquises dans un cadre légal, ceci peut être perçu comme une trahison car l'individu est convaincu qu'il bénéficiera d'un meilleur service reposant sur l'identification de ses besoins.

---

[117] https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf accédé le 2018-05-22

[118] https://www.cio.com/article/2383123/mobile/geofencing-explained.html accédé le 2018-05-28

Connaissant les faiblesses de son client, un fournisseur de services peut évaluer sa susceptibilité à accepter une proposition pire que celle proposée à d'autres clients (pouvant générer un profit supérieur). Le client peut alors accepter ou refuser cette offre.

Par conséquent, des règlementations additionnelles sont nécessaires pour protéger la vie privée non seulement contre l'acquisition illégale de données privées, mais également contre leur traitement illégal. Encore pire, serait de vendre à un tiers les conclusions tirées de données personnelles analysées.

Tant et aussi longtemps qu'un manufacturier prétend offrir un service personnalisé, la question de trahison se posera toujours. Ce type de discrimination personnalisée sera particulièrement difficile à combattre, car le client est sans défense.

Encore aujourd'hui [Yeoh, 2017] croit que les efforts déployés pour identifier les risques à la vie privée provenant de l'agrégation et l'analyse de données d'objets connectés par des tiers parties, sont insuffisants. Les personnes utilisant la technologie *IoT* croient que ceux qui amassent ces données devraient être tenus responsables de leurs actes. Elles voudraient aussi avoir les moyens d'en permettre l'utilisation et être munies d'outils qui les aideraient à fournir un consentement éclairé.

2.7 Vol d'Identité[119]

La stratégie première du vol d'identité est d'amasser le plus de données possibles. Avec un peu d'efforts, de recherches sur la toile, en combinant avec l'information obtenue des réseaux sociaux et maintenant celle des DPI, il est maintenant possible d'obtenir un portrait assez complet d'une personne et ainsi planifier une attaque pour en voler l'identité. Si en plus, on acquiert les données relatives au travail de cette personne, cette attaque devient rapidement très lucrative.

A maintes occasions dans la littérature parle-t-on de la gestion de l'identité dans l'IoT [Caviglione et Coccoli, 2011], [Vidalis et Angelopoulou, 2014]. Cette identité personnelle est de plus en plus stockée et utilisée sous différentes formes numériques laissant la porte ouverte à de possibles menaces. L'IoT est basé sur des services liés à l'identité [Lee et Kim, 2010] alors que les données transmises par les objets connectés sont basées sur l'identité.

[119] https://www.globalsign.com/en/blog/identity-theft-in-the-iot/ accédé le 2018-05-27

L'attaque du Salami [120] [Rustad, 2001] est un bon exemple d'une attaque largement documentée : Elle est principalement reliée à des crimes financiers et d'identité, où l'auteur détecte les paquets d'un réseau, les modifie et les réinsère dans le réseau sans en perturber la disponibilité. La principale caractéristique de l'attaque du Salami est sa faible importance par rapport à l'ampleur de l'attaque globale. Comme son nom l'indique, cette attaque rappelle une tranche de salami. Il ne s'agit que d'une stratégie visant à obtenir un avantage dans le temps en accumulant des informations par petits incréments, de façon qu'elle puisse également être utilisée de manière parfaitement légale. L'attaquant utilise une base de données en ligne pour saisir les informations des clients, et les accumule graduellement sur une période donnée. Les clients ne sont pas au courant et aucune plainte n'est donc déposée.

2.8 Conclusion

En se basant sur tout ce qui a été dit jusqu'à présent dans cette section, on peut conclure qu'un DPI contient et permet l'accès à ce qu'il y a de plus privé comme information, i.e. le nom, l'adresse, la date de naissance, le numéro de carte de crédit et des données sur la santé. Le téléphone intelligent ouvre aussi grandes les portes à certaines applications comme le courriel, les identificateurs d'accès aux ressources du travail et des réseaux sociaux, les applications pour les transactions bancaires et beaucoup plus. Il est étonnant qu'on s'en préoccupe si peu alors qu'autant de données se retrouvant dans ces appareils puissent porter de graves atteintes à la vie privée. La tendance récente BYOD encourage aussi le risque de fuite d'informations tant personnelles que d'affaires.

Plus une personne possède de dispositifs connectés, plus les données deviennent disponibles pour le vol d'identité. Un *hacker* a donc plus de chances de mettre la main sur une information qui lui donnera accès à un ordinateur ou espace de stockage privé.

Chapitre 3. Sensibilisation des individus aux risques

La problématique étant exposée, il est donc important de :

[120] https://ajmaurya.wordpress.com/2014/03/27/what-is-a-salami-attack/ accédé le 2019-01-16

- Savoir reconnaître une donnée sensible.
- Savoir qu'un DPI collecte et diffuse des données sensibles.
- Savoir que des précautions adéquates peuvent être prises pour protéger, anonymiser ou chiffrer des données.
- Savoir que les utilisateurs de DPI doivent être conscients des fuites potentielles ou du piratage de leurs données, et par conséquent en subir des impacts dans leur vie privée.

Dans un premier temps il est primordial de conscientiser le lecteur à propos des risques de sécurité et des atteintes à la vie privée dans *l'IoT*, et en particulier des DPI. Par la suite, nous proposons de sonder un échantillon d'individus adultes d'âges variés utilisant des DPI (pour le sport, les loisirs ou la gestion du temps) et d'enquêter sur leur niveau d'éveil aux atteintes à la vie privée par le moyen d'un test d'évaluation avec questions à choix multiples, basées des situations réelles de la vie courante. Ceci nous permettra de déceler les points faibles des connaissances.

Nous proposons ensuite une session d'apprentissage et de sensibilisation, du genre application web. Nous demanderons aux participants volontaires de suivre cette formation. Les participants y acquerront les connaissances et notions manquantes dans les sujets où ils n'auront pas obtenu la note de passage des sujets du test d'évaluation.

La dernière étape suggérée est de demander aux participants de repasser le test d'évaluation. Ceci nous confirmera la capacité d'apprentissage et de rétention du public-cible. Les apprenants seront en mesure de voir sur-le-champ leur progrès et apprécieront la différence de connaissances qu'ils auront acquises.

3.1 Curriculum

Le Grand Dictionnaire de l'Office Québécois de la Langue Française [121] définit un curriculum comme suit :

[121] http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8350041 accédé le 2018-10-21

> *C'est l'ensemble intégré des éléments qui définissent le contenu de la formation en fonction d'objectifs à atteindre et de compétences à acquérir, mis en œuvre selon un ordre de progression déterminé et construit dans le cadre d'un système d'éducation.*

Dans le cadre de ses travaux académiques, l'équipe d'étudiants gradués dirigée par le professeur Esma Aïmeur du DIRO (département d'informatique et de recherche opérationnelle) à l'Université de Montréal, a élaboré un curriculum représentant les sujets importants à connaître dans le domaine de la sensibilisation à la vie privée. Nous l'utilisons dans cette recherche afin de sélectionner les domaines de connaissances qui devront faire partie de notre test d'évaluation ainsi que pour définir les sujets à étudier.

Ce curriculum ressemble à une ontologie mais n'en est pas une à proprement dit, à cause de son organisation plutôt hiérarchique et l'absence de liens et de raisonnements. Il couvre (voir la Figure 9) plusieurs aspects de la sensibilisation à la vie privée, bien plus que ce dont nous aurons besoin dans le cadre de notre recherche. Par exemple, certains volets tels que le « développement logiciel » ou l'aspect « transactionnel » dans le *big data*, pour n'en nommer que deux, ne sont pas pertinents. Nous avons donc retiré ces composants du curriculum que nous avons jugé moins pertinents. Pour le bénéfice du lecteur de ce document, le curriculum complet a été mis en annexe.

Afin d'être plus clairs dans notre démarche, dans la Figure 9 les cercles représentent des « domaines de connaissances » alors que les rectangles blancs représentent des « sujets » (faisant partie de ces domaines). Les rectangles gris ou bleu pâle doivent être compris comme des « ensembles de sujets ».

Par exemple :

- « *Security Knowledge* » : est un domaine de connaissance à propos de la sécurité informatique en général.
- « *Self-Awareness* » et « *Safe Behaviours* » : sont des ensembles de sujets relatifs aux comportements sécuritaires dans le cadre d'une sensibilisation personnelle.
- « *Personal Information Disclosure* » et « *Password Protection* » : sont deux sujets faisant partie de ces ensembles et pour lesquels nous devrons sensibiliser / former les apprenants.

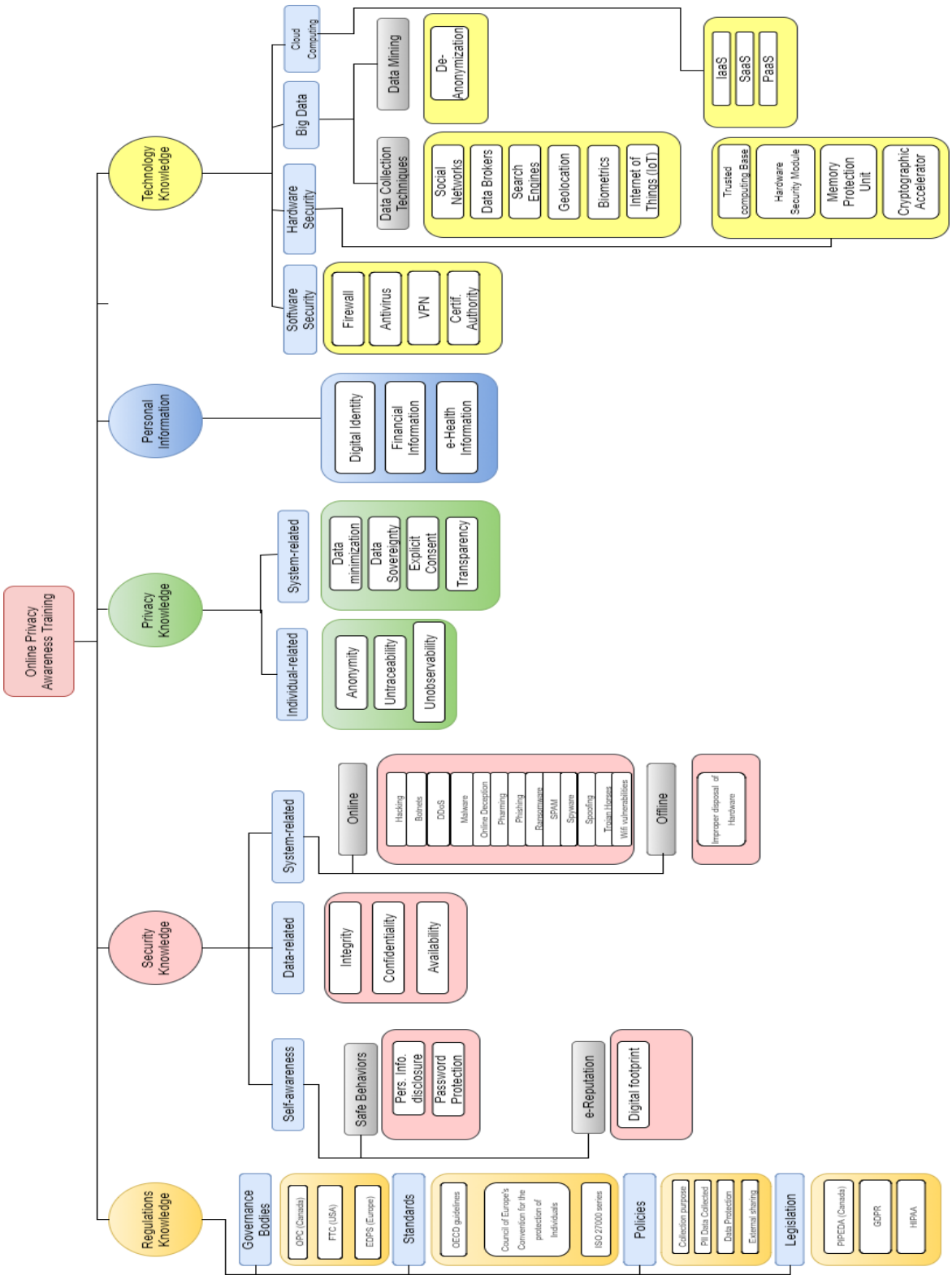


FIGURE 9 CURRICULUM DE FORMATION SUR LA VIE PRIVÉE

La pédagogie évolue et les moyens de l'inculquer doivent suivre. Parce que nous ciblons la formation d'une clientèle adulte, hors du contexte scolaire : nous choisissons d'utiliser une approche de *e-Learning*.

Le *e-Learning* permet aux apprenants de bénéficier d'une bonne rétention des connaissances parce qu'il se fait à une cadence et selon des conditions personnalisées. Il est compatible avec tous les horaires, n'interfère pas avec les occupations personnelles et ne requiert pas de se déplacer. Il facilite enfin l'habilitation (*enpowerment*) [Hur et Im, 2013].

3.2 Formation Adaptée pour une Meilleure Rétention

Prochaine étape suite au choix du e-Learning, nous proposons l'adaptation. Pourquoi adapter la formation? Parce qu'on y met en œuvre un apprentissage qui répond aux besoins d'un apprenant. Parmi les avantages[122] à en tirer, on retrouve :

- La formation un-à-un
- Le gain de temps
- La confiance et la compréhension chez les apprenants
- L'individualisation des parcours d'apprentissages
- Le focus sur les sujets où l'attention est requise

L'apprentissage adaptatif [123]existe depuis plusieurs années, il origine de la psychologie cognitive, qui a commencé avec le travail du comportementaliste B.F. Skinner dans les années 1950 et s'est poursuivi dans le mouvement de l'intelligence artificielle des années 1970. C'est une modalité d'apprentissage éprouvée qui est utilisée dans de nombreux environnements pour former plus efficacement. Dans l'apprentissage adaptatif, le principe de base est que l'outil ou le système sera capable de s'adapter à la méthode d'apprentissage de l'apprenant.

3.3 Système de Tutorat Intelligent (STI)

La compréhension du système de tutorat intelligent (*Intelligent Tutoring System*) est une bonne base de départ pour bien expliquer les éléments composant un système d'apprentissage tel que le e-Learning. [Phobun et Vicheanpanya, 2010] présentent un modèle sur lequel nous baserons la suite de cette recherche. Ce modèle est représenté à la Figure 10.

[122] https://elearningindustry.com/adaptive-learning-in-corporate-training-benefits-know accédé le 2018-11-09
[123] https://adaptivelearninginelt.wordpress.com/tag/skinner/ 2019-01-16

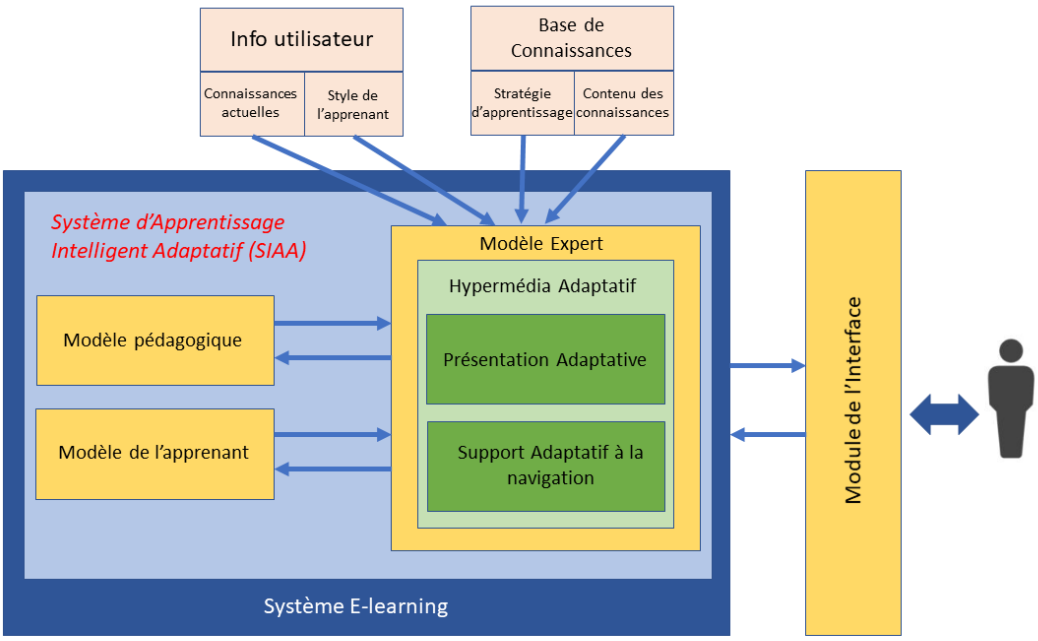


FIGURE 10 SYSTÈME DE TUTORAT INTELLIGENT
[PHOBUN ET VICHEANPANYA, 2010]

3.3.1 Modèle de l'Apprenant

Commençons par le modèle de l'apprenant, c'est-à-dire la composante du STI qui représente le niveau de connaissances de l'apprenant. [Herder, 2016] définit ce modèle comme une structure de données qui caractérise un utilisateur à un certain moment dans le temps. Il va se définir par l'écart entre les connaissances propres de l'apprenant et les connaissances de l'expert telles qu'elles sont représentées dans le système. Il permet de découvrir ce que l'étudiant connait (ou pas) ou ce qu'il connait peut-être, mais de façon incorrecte.

Il existe quelques classifications connues de modèles d'apprenant dans le monde de l'éducation. On parle par exemple de :

- Prédictif (exécute différents modèles et tente de trouver celui qui sied l'apprenant de façon optimale)
- Analytique (analyse l'input de l'apprenant dans le but de proposer la meilleure méthode en tenant compte aussi du contexte)

- Recouvrement (*Overlay*): il représente les connaissances de l'utilisateur, ses intérêts et ses objectifs en tant que sous-ensemble du modèle expert

Le modèle de recouvrement (*Overlay model*) est le plus populaire : On attribue un « poids » servant à chiffrer le niveau de connaissances de l'individu. Ce poids est représenté sur une échelle de 0 à 100.

3.3.2 Base de Connaissances

La base de connaissances contient les concepts, règles, et stratégies de résolution de problèmes du domaine à apprendre. C'est la source de l'expertise ainsi que la norme d'évaluation d'expertise et d'évaluation de performances de l'élève. On l'organise ici en un curriculum comprenant tous les éléments de connaissance auquel on ajoute un quiz (avec pointage) référant aux connaissances acquises dans chacun des domaines.

3.3.3 Modèle Expert

Le modèle expert reçoit des informations de la base de connaissances et du modèle de l'apprenant, et prend les décisions appropriées afin de choisir une stratégie d'apprentissage appropriée. Ces décisions devraient refléter les formes d'interactions avec les étudiants.

3.3.4 Modèle Pédagogique

D'après [Al-Nakhal et Abu Naser, 2017] :

> *« Le modèle pédagogique agit comme instructeur virtuel : il expose le matériel dans un ordre approprié, selon le style d'apprentissage et compétences des élèves. Ce processus est interactif et le travail du modèle est d'illustrer les concepts à l'étudiant et soutenir tous les processus d'apprentissage* »

3.3.4.1 Notre proposition : PLE *(Personal Learning Environment)*

Notre proposition de modèle pédagogique va donc du côté de « l'Environnement d'Apprentissage Personnel » mieux connu dans la littérature sous PLE (*Personal Learning Environment*). C'est un modèle qui se marie très bien avec l'omniprésence de l'internet et de ses ressources vouées à la formation. Il offre une combinaison d'outils et de services individualisés et une approche moderne de l'apprentissage. Il est centré sur les efforts de l'individu pour apprendre. Le PLE réfère aux efforts visant à adapter l'éducation aux différents besoins des étudiants.

Le concept du PLE a beaucoup été vanté par Graham Atwell[124], un membre associé de l'Institut de recherche sur l'emploi de l'Université de Warwick. L'idée d'un PLE reconnaît que l'apprentissage est continu et on doit chercher à fournir des outils pour soutenir cet apprentissage. Il reconnaît également le rôle de l'individu dans l'organisation de son propre apprentissage. De plus, les pressions en faveur d'un PLE reposent sur l'idée que l'apprentissage se déroulera dans des contextes et des situations différents et ne sera pas fourni par un seul prestataire d'apprentissage. À cela s'ajoute une reconnaissance croissante de l'importance de l'apprentissage informel. Le PLE est donc un outil approprié au e-Learning et cadre très bien dans l'optique d'une formation à la sensibilisation aux impacts à la vie privée.

3.3.4.2 Microlearning

Parce que la technologie continue à être intégrée dans les tâches quotidiennes des employés, on se doit de développer des approches plus mixtes en matière de formation et de développement. Le *microlearning* [Emerson & Berge, 2018] permet de livrer des morceaux d'informations en peu de temps, souvent via les médias sociaux. C'est une stratégie qui complète bien des formations classiques ou virtuelles et qui renforce les concepts entre les tâches.

Dans un monde caractérisé par des changements réguliers au sein de la main-d'œuvre, par de nouvelles technologies et par une diminution rapide de l'attention, le *microlearning* occupe une place centrale dans l'industrie de l'apprentissage. Le *microlearning* se définit donc comme « *la livraison de pépites de contenu de petite taille* »[125]. L'industrie du e-Learning déclare qu'un module

[124] http://www.pontydysgu.org/pontydysgu-and-people/graham-attwell/ (consulté le 2018-10-08) et https://www.researchgate.net/profile/Graham_Attwell2 (consulté le 2018-10-08)
[125] https://elearningindustry.com/most-important-microlearning-features consulté le 2018-10-08

de *microlearning* est axé sur l'atteinte d'un résultat d'apprentissage spécifique, en fragmentant un vaste sujet et en permettant à l'apprenant de suivre ces parties dans l'ordre de son choix.

Grâce au *microlearning*, on peut se concentrer sur des objectifs très précis d'un sujet donné. Les apprenants peuvent ainsi choisir ce qui correspond le mieux à leurs besoins et utiliser ce matériel de formation d'une manière spécifique. En fournissant uniquement les informations les plus critiques dans un package court et succinct permet aussi aux apprenants de mieux assimiler les informations et de les utiliser ensuite. Avec un contenu plus long, les instructeurs peuvent être confrontés à une perte d'engagement, ce qui donnera inévitablement de mauvais résultats à l'évaluation. La rétention est également plus importante en raison de l'accessibilité des informations et de la quantité de contenu partagé. Il est finalement possible grâce au *microlearning* de proposer un apprentissage personnalisé, ce qui contribue également à accroître l'engagement et le succès.

Dans un but d'efficacité[126] du *microlearning* il faut…

- Définir les objectifs et suivre les besoins de l'apprenant
- Choisir le type de contenu approprié
- Offrir des parcours d'apprentissage
- Évaluer le succès de l'apprentissage

Une firme américaine, ATD Research [127], a sondé plusieurs professionnels du développement des talents dans le but d'établir une norme dans l'industrie du *microlearning*. Ils ont constaté que la durée moyenne maximale d'une activité de *microlearning* devrait être d'environ treize minutes. Cependant, le temps moyen du *microlearning* devrait idéalement être aux alentours de dix minutes mais beaucoup s'entendent pour dire que toute activité de trois à quinze minutes peut être qualifiée de *microlearning* à l'opposé d'une formation plus classique qui peut durer une heure ou plus.

[126] https://trainingindustry.com/articles/content-development/microlearning-how-to-ensure-that-small-is-effective/ consulté le 2018-10-18

[127] Cole, M. (mars 2017) "Just how micro is microlearning?" https://www.td.org/insights/just-how-micro-is-microlearning consulté le 2018-10-18

3.3.5 Style de l'Apprenant

Les styles d'apprentissage de chaque individu sont à la base de l'apprentissage lui-même. Ils sont définis comme « *un ensemble de caractéristiques cognitives, affectives et facteurs physiologiques servant d'indicateurs relativement stables de la perception, de l'interaction et de la réponse de l'apprenant* » [Keefe, 1979]. Ils peuvent aussi être des « *conditions éducatives dans lesquelles un élève est le plus susceptible d'apprendre* » [Stewart et Felicetti, 1992].

Il existe dans le monde de l'éducation quatre styles prédominants pour l'apprentissage:

- Les apprenants visuels où les individus apprennent en regardant.
- Les apprenants auditifs où les individus apprennent en écoutant.
- Les apprenants Lecture-Écriture où les individus apprennent par le biais de la lecture et de l'écriture.
- Les apprenants kinesthésiques où les individus apprennent par la pratique.

Les gens essaient de traiter les tâches conformément à leur style d'apprentissage, mais cela ne les aide pas toujours. Il y a des raisons de penser que les gens voient les théories sur les styles d'apprentissage au sens large mais en fait, le soutien scientifique à ces théories fait défaut [Willingham *et al.*, 2015].

Il est bien sûr possible de connaître le style d'un apprenant par le biais d'un questionnaire[128]. Le résultat final identifiera alors les traits dominants de l'apprenant. Bien qu'un style puisse s'appliquer à un individu dans le but de lui procurer une formation adaptée, on très difficilement utiliser cette approche lorsqu'on doit travailler avec un groupe de personnes participant, par exemple, à du e-Learning. Dans ce cas, il faudrait avoir autant de modules d'apprentissage qu'il y a de styles différents d'individus.

Un examen approfondi de la littérature à propos des styles d'apprentissage jette un sérieux doute sur la validité et l'utilité de l'utilisation des styles classiques d'apprentissage comme base pour accommoder les individus de toute génération [Coffield, Moseley, Hall et Ecclestone, 2004]. Les critiques n'ont trouvé que peu de preuves à propos de l'existence-même des 70 (et plus)

[128] http://vark-learn.com/the-vark-questionnaire/ (consulté le 2018-10-08)

modèles de styles d'apprentissage rapportés dans des centaines d'études publiées dans la littérature de recherche pédagogique et psychologique.

Notre proposition : Andragogie et Heutagogie

Que faire alors ? Afin de répondre aux attentes de formation d'une clientèle adulte dans un milieu non-académique, nous proposons une référence à l'andragogie. C'est une théorie élaborée par un américain du nom de Malcom Knowles. Selon cet éducateur, l'andragogie est l'art et la science de l'éducation des adultes [Kearsley, 2010]. Knowles présente quatre principes de base pour l'éducation des adultes :

1. Les adultes doivent être impliqués dans la planification et l'évaluation de leur instruction.
2. L'expérience (incluant les erreurs passées) forment la base des activités d'apprentissage.
3. Les adultes sont intéressés à apprendre des sujets en lien direct avec leur travail ou leur vie personnelle.
4. L'apprentissage adulte est centré sur un problème existant plutôt que sur le contenu.

Alors que l'andragogie (Figure 11) fournit de nombreuses approches utiles pour améliorer la méthodologie éducative, cette dernière a toujours une connotation de relation enseignant-apprenant. A cause du rythme rapide du changement dans la société, et à cause de l'explosion de l'information, on suggère maintenant d'examiner une approche éducative où c'est l'apprenant lui-même qui détermine quoi et comment il doit apprendre.

L'heutagogie (aussi dans la Figure 11), répond à ce besoin : C'est l'étude de l'autodétermination dans l'apprentissage (*self-determined learning*), et elle peut être considérée comme une progression naturelle par rapport aux méthodologies éducatives antérieures - en particulier du développement des capacités - et pourrait bien constituer l'approche optimale de l'apprentissage au XXIe siècle. Un changement de mentalité vers l'heutagogie permet de mieux maîtriser l'apprentissage pour l'apprenant. De plus, cela permet une approche beaucoup plus créative de l'apprentissage, quel que soit le contexte.

L'apprenant adulte apporte avec lui un large éventail d'expériences dans le monde de l'éducation continue. Celles-ci affecteront les styles d'apprentissage et l'assimilation des connaissances. Les apprenants adultes doivent pouvoir appliquer les connaissances dans leurs situations de vie.

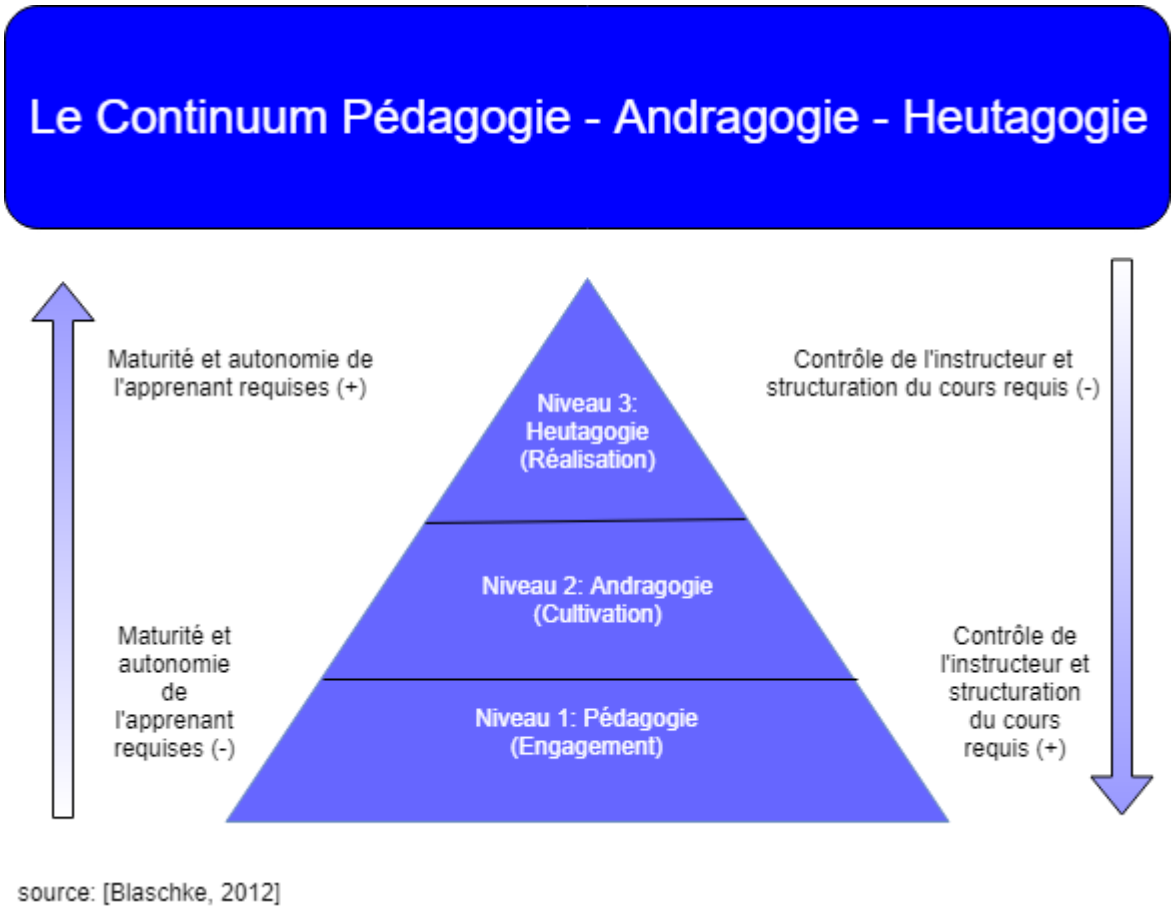


FIGURE 11 LE CONTINUUM PÉDAGOGIE - ANDRAGOGIE - HEUTAGOGIE[129]

3.4 Générations

Puisque nous devons travailler avec un groupe de personnes adultes participant à du e-Learning, et que l'heutagogie apparaît être une approche méritoire, intéressons-nous donc particulièrement à décrire ces trois générations d'adultes [Dimock, 2018] :

- Les Baby-boomers (1946-1964)
- La Génération X (1965-1980)
- Les milléniaux (ou Génération Y) (1981-1996)

[129] http://www.irrodl.org/index.php/irrodl/article/view/1076/2087 consulté le 2018-12-10

Notons qu'en sciences sociales, une génération signifie « *des personnes au sein d'une population délimitée qui vivent les mêmes événements significatifs au cours d'une période donnée* » [Pilcher, 1994].

Dans les prochains paragraphes nous donnons un aperçu des caractéristiques de ces trois générations d'adultes. Il existe une foule de références en recherche qui décrivent ces caractéristiques et celles qui sont présentées dans notre travail font l'unanimité [Shepherd, 2017] [Knight, 2016] [Kriegel, 2013] [Longenecker, 2012] [O'Neill, 2010].

3.4.1 Baby-boomers

Les baby-boomers sont caractérisés par leur souci de sécurité d'emploi et d'un environnement de travail stable, par la fidélité à leur organisation, par leur dynamisme et par leurs perspectives idéalistes et optimistes. Cette génération ne figure plus en nombre sur les lieux de travail. Les organisations ont donc dû s'adapter aux nouvelles valeurs et aux nouvelles orientations professionnelles des employés de la génération X et de la génération Y.

Ce sont des bourreaux de travail, performants et compétitifs. Ils questionnent l'autorité mais veulent bien la respecter. Ils préfèrent un environnement d'apprentissage stable et sans risque représenté par un enseignement magistral avec possibilité d'interaction. Ils perçoivent la technologie comme un moyen et non une fin. C'est pourquoi ils préfèrent la documentation imprimée quand c'est possible.

3.4.2 Génération X

Les membres de la génération X sont considérés comme plus cyniques, pessimistes et individualistes que la génération des baby-boomers qui les ont précédés. Ils sont plus à l'aise avec le changement et la diversité; plus susceptibles de déménager à la recherche de salaires plus élevés et de nouveaux défis (et donc moins engagés envers leur organisation). Ils ont un fort sentiment de nécessité d'équilibre entre vie professionnelle et vie privée.

Ils préfèrent apprendre par l'action, en utilisant l'auto-apprentissage, la recherche ou les projets. Ils aiment la liberté de découvrir des choses par eux-mêmes. Ils sont techniquement compétents alors ils n'hésitent pas à utiliser la technologie quand elle est disponible,

préférablement aux livres. Ils aiment les tâches multiples et la compétition. Ils veulent gérer leur propre horaire.

3.4.3 Milléniaux (ou Génération Y)

Les Milléniaux veulent développer leurs compétences, sont astucieux sur le plan technologique, souhaitent être exposés à de nouveaux défis et ont une orientation internationale / mondiale. Comme les baby-boomers, ils sont très motivés et optimistes, mais contrairement à eux, ils ne valorisent pas particulièrement la sécurité de l'emploi. Ils sont plus favorables à l'action collective que la génération X, sont férus de travail en équipe et des aspects sociaux du travail, valorisent les responsabilités et veulent être impliqués dans les processus de prise de décision. Ils recherchent des rétroactions sur leurs performances.

Multi-tâches et Multi-carriéristes, ils préfèrent l'apprentissage collaboratif avec possibilité d'interaction selon un horaire flexible. Ils préfèrent aussi les activités qui sont courtes et interactives. Ils ont peu de patience pour les séminaires et longues présentations. Leur apprentissage doit être divertissant et ludique, utilisant les technologies et les réseaux sociaux. Ils ont besoin d'avoir un parcours d'apprentissage clair et connaître les attentes.

Un résumé des caractéristiques de chaque génération est présenté au Tableau 5.

TABLEAU 5 RÉSUMÉ DES QUALIFICATIFS ASSOCIÉS AUX GÉNÉRATIONS D'ADULTES

Sources: [Shepherd, 2017], [Knight, 2016], [Kriegel, 2013], [Longenecker, 2012], [O'Neill, 2010]		
Baby-Boomers	**Génération X**	**Milléniaux (Génération Y)**
Dédiés	Actifs	Ambitieux
Loyaux	Ingénieux	Motivés
Compétitifs	Curieux	Collaboratifs
Respectueux	Compétents	Expansifs
Conscientisés	Technophiles	Impatients
Expansifs	Compétitifs	Technophiles
Interactifs	Diversifiés	Flexibles
Technophobes	Autonomes	Insécures
	Équilibrés	Multitâches

3.5 Générations et Événements[130] Sociaux

L'approche générationnelle, où les membres de chacune des cohortes ont été influencés par toutes sortes d'événements sociaux (Tableau 6), aide à mieux comprendre notre choix d'une approche heutagogique, particulièrement dans une situation d'apprentissage à distance (e-Learning) de la sécurité et des atteintes à la vie privée.

[130] Un tableau de ressources disponibles pour chacun des événements est situé dans l'annexe à la section 7.5

TABLEAU 6 LES GÉNÉRATIONS ET LES ÉVÉNEMENTS SOCIAUX MARQUANTS
(SOURCES : [TANNER1, MAI 2018], [TANNER2, MAI 2018], [TANNER, JUILLET 2018] ET [GUAY ET GAUDREAU, 2018])

Baby-Boomers	Génération X	Milléniaux
1954 – Début des auditions de l'affaire McCarthy 1962 – La crise des missiles cubains. 1963 – L'assassinat du président John Kennedy. 1964 - L'Acte des Droits Civils de 1964 est accepté. 1965 – Les États-Unis envoient des troupes au Vietnam. 1968 - Martin Luther King est assassiné. 1968 - Robert Kennedy est assassiné. 1970 – Fusillade à l'Université Kent State. 1970 – La crise d'Octobre 1970 (Canada): kidnappings politiques, Ottawa suspend les droits civils.	1972 – Le scandale du Watergate 1972 - Le Terrorisme aux jeux olympiques de Munich. 1978 – Le suicide collectif de Jonestown 1979 - Effondrement de la centrale de Three Mile Island 1979 - La crise des otages iraniens 1980 – Le referendum du Québec sur la "souveraineté-Association" est perdu 60% contre, 40% pour. 1982 – Le rapatriement de la Constitution Canadienne, accompagné de la Charte des Droits et Libertés. 1986 - Explosion de la navette spatiale Challenger. 1988 - Bombardement du vol de Lockerbie 1987 – La chute de la bourse 1987 – L'échec de l'Accord du Lac Meech (Canada) 1990 - Opération Desert Storm	1992 – L'Accord de Charlottetown (Canada) est rejeté par voie de referendum national. 1995 - Le bombardement d'Oklahoma City 1995 - Le referendum du Québec sur la souveraineté est perdu de justesse. Plusieurs fusillades dans les écoles. Diversité Exposition précoce à des problèmes d'adultes graves. Sensibilisation aux impacts environnementaux.
Droits civils, guerres, événements politiques importants.	Scandales et jeux de pouvoir politiques, terrorisme, événements économiques importants.	Événements de la Génération X plus : diversité culturelle et Environnement.

En conséquence des événements sociaux marquants qui sont présentés ici, il est plausible et peu risqué d'avancer que l'apprentissage en ligne est plus efficace, quand on tient plutôt compte de la diversité générationnelle[131].

[131] https://www.eleapsoftware.com/effective-elearning-multi-generational-workforce/ accédé le 2018-12-19

Notre choix d'utiliser une approche générationnelle pour catégoriser les groupes d'apprenants plutôt que d'utiliser les styles d'apprenants individuels est donc une approche valable, et avec une formation basée sur les principes heutagogiques, on pourra prendre en considération l'aspect d'expérience sociale et familiale des cohortes générationnelles participant au e-Learning. Nous pourrons utiliser ces aspects dans un but d'adapter une formation pour chacune des cohortes générationnelles, ce qui sera beaucoup plus applicable sur une clientèle dont on ne connaît pas le nombre ni le style.

> « *Les organisations qui comprendront mieux les différences générationnelles auront plus de succès à long terme dans la gestion de leurs employés et trouveront des moyens de s'adapter aux différences* ».
>
> [Twenge et Campbell, 2008]

Chapitre 4. CLEOPATRA

Comme nous l'avons mentionné à même l'introduction de ce mémoire, nous désirons donner un moyen aux adultes d'acquérir une formation afin de les sensibiliser aux enjeux de la vie privée. Pour ce faire nous proposons ici un système de e-Learning qui tient compte de leur statut générationnel et qui leur permettra d'atteindre ce but.

4.1 Définition

CLEOPATRA[132] (***C****loud-based* ***L****earning* ***E****nvironment* ***O****n* ***P****rivacy* ***A****wareness* ***TR****aining for* ***A****dults*) est notre proposition de système de *e-Learning* utilisant une approche de *microlearning* [133] dans un contexte de PLE [134](*Personal Learning Environment*). Il a comme but de sensibiliser les participants à la sécurité informatique et aux impacts à la vie privée.

C'est une application web interactive et indépendante de la technologie utilisée pour y accéder, que ce soit un ordinateur, tablette ou téléphone intelligent. Elle ne requiert seulement que l'utilisation d'un fureteur internet.

C'est un environnement d'apprentissage conduisant à la sensibilisation à la vie privée pour une clientèle adulte. On dit aussi qu'il utilise l'infonuagique (*cloud*) parce que sa base de connaissances ne contient qu'une liste de URL[135] (*Uniform Resource Locator*) référant à des documents en lien avec les préférences de formation des apprenants. On parle donc ici d'une « adaptation de la formation ».

CLEOPATRA offre cinq modules de formation, ou « domaines de connaissances » tirés du curriculum décrit à la section 3.1. Le Tableau 7 présente ces modules ainsi que la durée approximative reliée à son apprentissage.

[132] http://www-labs.iro.umontreal.ca/~fortinje/index.php accédé le 2018-11-12
[133] Voir la section 3.3.4.2
[134] Voir la section 3.3.4.1
[135] https://www.larousse.fr/dictionnaires/francais/URL/80723 accédé le 2018-12-14

TABLEAU 7 MODULES DE FORMATION DE CLEOPATRA

Module	Durée approximative[136] de la formation
1 : Connaissances générales à propos de la règlementation (*Regulations knowledge*)	45 minutes
2 : Connaissances générales à propos de la sécurité (*Security knowledge*)	1 heure 15 minutes
3 : Connaissances générales à propos de la vie privée (*Privacy Knowledge*)	30 minutes
4 : Connaissance d'une information personnelle (*Personal Information Knowledge*)	10 minutes
5 : Connaissances générales en technologie (*Technology Knowledge*)	1 heure 30 minutes
Grand Total	**4 heures 10 minutes**

L'apprenant n'a pas besoin de suivre les modules dans un ordre particulier, ni de les suivre tous, bien qu'il puisse le faire s'il le désire. Une évaluation du niveau de connaissances de l'apprenant (test d'évaluation[137]) permettra d'apprécier le niveau des connaissances en sécurité et vie privée avant d'entreprendre un ou plusieurs des cinq modules et orientera l'apprenant vers un plan d'apprentissage qui aidera à combler ses lacunes.

4.2 Architecture logicielle

CLEOPATRA est construit à l'aide du langage de programmation PHP, un des langages de programmation le plus utilisé au monde[138] et conçu spécifiquement pour le web[139]. Il peut être utilisé gratuitement car il possède une licence *open-source*. On y retrouve une communauté très active d'utilisateurs et on trouve facilement une multitude de sources de documentation.

[136] La durée de chaque élément est estimée avec l'aide de l'outil en ligne Read-O-Meter : http://niram.org/read/ accédé le 2018-12-15. Cet outil calcule la durée selon sur une moyenne de temps de lecture de 200 mots/minute.
[137] Voir le test d'évaluation à la section 7.1
[138] https://w3techs.com/technologies/details/pl-php/all/all consulté le 2018-12-14
[139] http://php.net/manual/en/intro-whatis.php consulté le 2018-12-14

La base de connaissances et les différents composants (informations sur les participants, index des modules, quiz etc.) sont rendus disponibles sous MySQL, un système *open-source* de gestion de base de données relationnelles fréquemment utilisé avec PHP. MySQL est utilisable virtuellement sous toutes les plateformes disponibles aujourd'hui; il est donc très portable. L'information qui y est stockée est facilement accessible en utilisant des commandes SQL (*Structured Query Language*). Cette base de données normalisée, évite ainsi redondance et optimise les performances. On peut consulter le modèle relationnel de la base de données à la section 7.3.

Le cœur de notre système de e-Learning a été réalisé suivant une adaptation du progiciel HUGE[140] qu'on décrit comme *une solution simple d'authentification PHP (login), intégrée dans un petit framework MVC*[141].

Un *framework PHP* est une plateforme de base qui nous permet de développer des applications Web. En d'autres termes, il fournit une structure. Ceci permet de gagner du temps, en évitant de produire du code répétitif. En ce qui concerne le motif de conception logicielle MVC (*Model-View-Controller*), celui-ci est utilisé dans plusieurs *frameworks* PHP. Dans le paradigme MVC appliqué à CLEOPATRA, l'input de l'utilisateur, la modélisation et l'output visuel sont explicitement séparés en trois rôles :

- Le « Contrôleur » qui interprète les commandes de l'utilisateur et les envoie au « Modèle ».
- Le « Modèle » qui bâtit la requête SQL, l'envoie au système de gestion de la base de données et gère la réception des résultats.
- La « Vue » qui gère la portion de l'affichage i.e. le résultat du lien externe montrant l'élément de formation.

La « Vue » et le « Contrôleur » sont spécifiquement conçus pour travailler ensemble alors que le « Modèle » fonctionne d'une manière un peu plus détachée. Voir aussi la Figure 12.

[140] https://github.com/panique/huge accédé le 2018-12-14
[141] MVC : motif de conception logicielle *Model – View – Controller*

HUGE a été élaboré à la suite de l'observation et de l'analyse d'applications gigantesques contraignant les développeurs à retourner aux notions de bases en programmation en structurant leur code et en utilisant des constructions plus simples. HUGE est donc un progiciel idéal pour fournir l'essentiel requis au développement de plus petits projets. Enfin, il implémente *out of the box* le hachage/salage du mot de passe, disponible dans les récentes versions de PHP, question de sécurité.

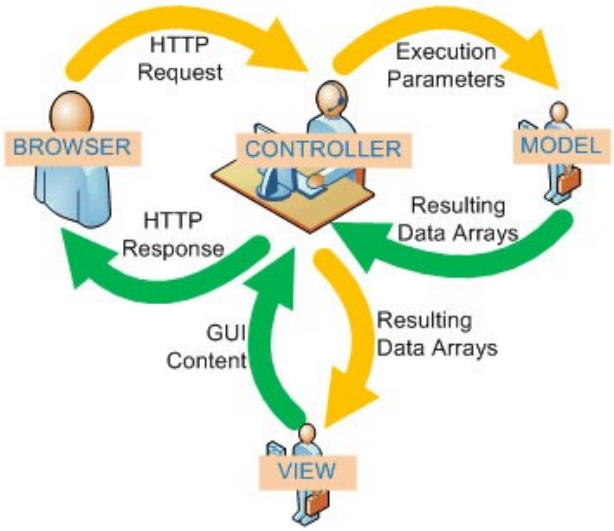


FIGURE 12 REPRÉSENTATION DU FLOT DE COMMUNICATIONS DANS LA TRIADE MVC[142]
SOURCE : ONEXTRAPIXEL.COM

4.3 Le flux logique de la formation

La Figure 13 présente le diagramme du flux logique de la formation que nous proposons et qui offre l'adaptation au style de l'apprenant. Il est basé sur une approche heutagogique, telle que nous l'avons définie à la section 0.

L'étudiant passe par une première évaluation générale de ses connaissances parmi les sujets du curriculum relatifs à la sécurité informatique et à la vie privée. Cette évaluation est composée

[142] Source de l'image: https://onextrapixel.com/an-overview-of-php-framework-guides-for-developers/ consulté le 2018-12-15

de quelques questions à choix multiples et qui confrontent à des situations très réalistes. Les résultats de ce test seront utilisés dans la composition d'une partie du dossier-étudiant et ils nous indiqueront les domaines de connaissances où il a obtenu la note de passage et ceux où il aura besoin d'aller chercher une formation supplémentaire.

La note de passage dans les différents domaines de connaissance n'est pas laissée au hasard : elle est déterminée en utilisant une version simplifiée de la méthode Angoff[143] bien connue dans le monde de l'éducation. Pour chacune des questions du test, nous estimons le pourcentage d'individus minimalement compétents qui seront en mesure de répondre correctement. Ces « difficultés prévues » sont additionnées et divisées par le nombre total d'éléments de l'examen pour obtenir un pourcentage limite qui, une fois arrondi, correspond à la note de passage. En utilisant cette approche, la note de passage de tous les domaines de connaissances de notre test a été fixée comme suit :

Connaissance de la sécurité	6/10
Connaissance de la vie privée	8/10
Informations personnelles	5/10
Connaissance de la technologie	6/10
Règlementation	6/10

Parce que le système CLEOPATRA connait la génération de l'apprenant, ce dernier est en mesure de créer un sous-curriculum de formation où les liens (URL) utilisés sont ceux qui reflètent les préférences de « genres de pages » pour la génération dont il est question.

Après avoir suivi la formation, deux situations peuvent se présenter :

1- L'étudiant n'a pas obtenu la note de passage dans un ou plusieurs domaines de connaissances.
2- L'étudiant a obtenu la note de passage dans tous les domaines de connaissance mais est désireux d'améliorer son score.

[143] https://www.maxinity.co.uk/blog/standard-setting-simplified-angoff accédé le 2019-01-23

Que ce soit pour la situation 1 ou 2, il est invité à repasser le test, ce qui servira à lui démontrer son amélioration provenant d'une formation adaptative.

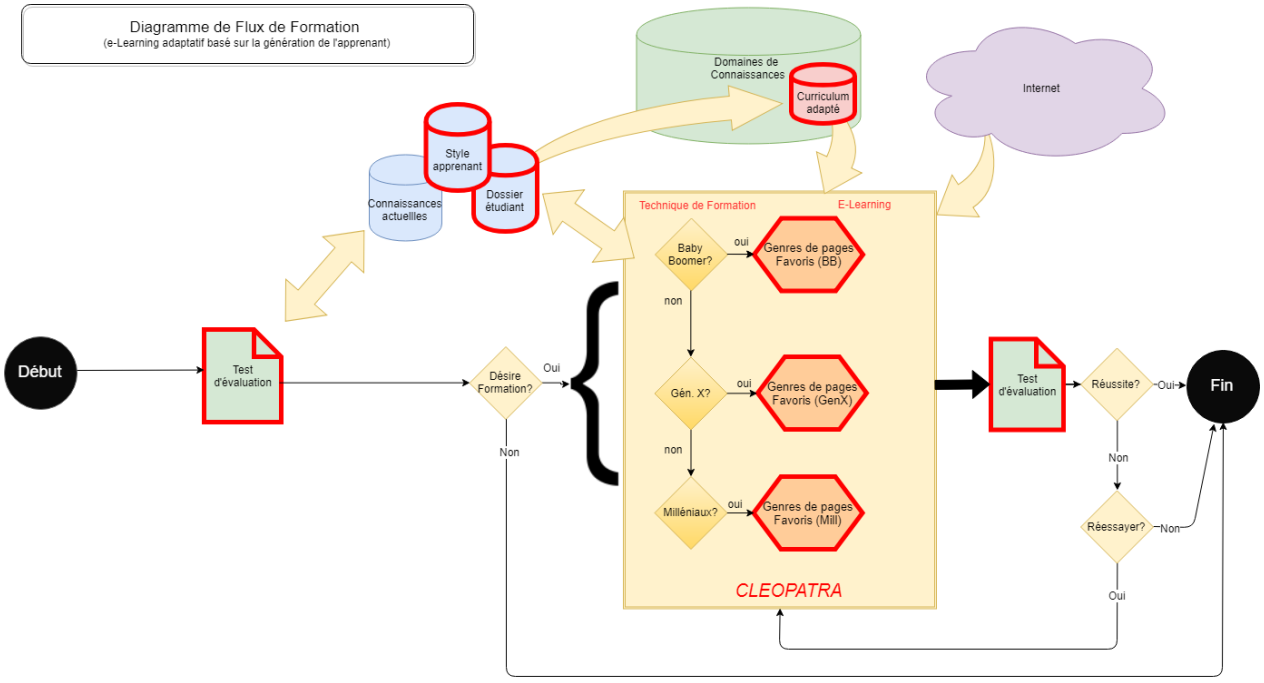


FIGURE 13 FLUX DE FORMATION (E-LEARNING ADAPTATIF GÉNÉRATIONNEL)

4.4 Présentation d'un contenu web convenable

En vue de proposer aux individus un contenu web qui les rejoindra, nous devrons connaître pour chacune des générations, la liste de genres de pages web qui sont en lien direct avec leurs attributs et préférences.

4.4.1 Genres de Pages Web

Les genres de pages web sont difficiles à définir de manière claire en raison de la grande diversité du web. Leur classification est une tâche difficile et elle fait encore partie de beaucoup de sujets de recherche. Il y a beaucoup de méthodes afin de décider qu'une page web appartient à un genre ou un autre : Pour ce faire on peut utiliser, par exemple, des méthodes basées sur des techniques combinées de *Natural Language Processing* (NLP) et de *machine-learning* [Pritsos et Stamatatos, 2013] mais pour les besoins de notre recherche, afin de déterminer si on peut associer

un genre à une génération en particulier, nous les catégoriserons manuellement. En revanche, l'automatisation de cette tâche pourrait faire l'objet d'un futur travail.

Nous avons donc besoin d'une liste initiale de genres de pages web avec laquelle nous pourrons travailler. Il en existe quelques-unes dans la littérature. Ces listes ont généralement été créées avec l'aide de classifieurs entraînés sur des grands ensembles de données (*datasets*). Le *dataset 20-Genre* [Vidulin *et al.*, 2007] a particulièrement retenu notre attention : Il comprend 1539 pages web appartenant à 20 genres, un nombre ni trop grand ni trop petit, chaque page appartenant à un genre ou plus.

Le nombre de *datasets* disponibles à l'entrainement des classifieurs est assez limité et bien que ces derniers datent déjà de quelques années, le *dataset 20-genre* est encore utilisé dans les recherches récentes sur le sujet, par exemple [Jebari, 2016]. Dans notre recherche, ce schème de classification peut servir de base très intéressante pour avoir une liste de genres de pages web suffisant pour notre formation.

Le Tableau 8 présente la liste des genres extraits du *dataset 20-genre*. [Vidulin *et al.*, 2007]

Tableau 8 Genre de pages web - Corpus "20-genre"
[Vidulin *et al.*, 2007]

Blog (*Blog*)	Blogs, journaux intimes, mises à jour horodatées
Enfants (*Children*)	Encyclopédie pour enfants, paroles pour enfants
Commercial (*Commercial*)	Pages d'accueil d'institutions, d'organisations, de partis politiques, d'individus institutionnalisés; descriptions de produits; descriptions de service; communiqué de presse
Communauté (*Community*)	Forums, pages de groupes de discussion, portails avec contenu généré par l'utilisateur. Réseaux sociaux.
Livraison de Contenu (*Content delivery*)	Pages de téléchargements, de galeries d'images et de films, Jeux
Divertissement (*Entertainment*)	Blagues, puzzles, horoscopes, jeux
Message d'Erreur (*Error message*)	Pages d'erreur HTTP personnalisées, erreurs non HTTP
FAQ (*FAQ*)	FAQ (Foire aux questions)
Passerelle (*Gateway*)	Pages d'introduction, pages de redirection, pages de login
Index (*Index*)	Collections de liens, table des matières
Informatif (*Informative*)	Matériel encyclopédique, recettes, manuels d'utilisation, How-tos, notes de cours pour un large public, livres informatifs, biographies, discographies, filmographies
Journalistique (*Journalistic*)	Nouvelles, reportages, éditoriaux, interviews, critiques
Officiel (*Official*)	Documents juridiques, rapports officiels, règlements
Personnel (*Personal*)	Pages d'accueil personnelles, pages avec avis, descriptions d'intérêts et d'activités
Poésie (*Poetry*)	Poèmes, paroles
Pornographie (*Pornography*)	Photos et vidéos, histoires
Prose fiction (*Prose fiction*)	Histoire de fanfiction, nouvelle, roman
Scientifique (*Scientifique*)	Papiers, thèses, notes de cours pour une audience spécialisée, livres scientifiques
Magasinage (*Shopping*)	Magasins en ligne, petites annonces, comparateurs de prix, listes de prix
Entrée utilisateur (*User Input*)	Formulaires, sondages

Nous avons retenu 11 genres (cellules grisées du Tableau 8). Les genres qui n'ont pas été sélectionnés n'ont pas vraiment d'application possible compte tenu du sujet traité ici.

4.4.2 Cohortes Générationnelles et Genres

Nous avons ensuite soumis un court sondage[144] à une population égale de baby-boomers, générations X et milléniaux. On y présentait dix situations touchant la sécurité informatique et la vie privée et on demandait aux participants d'identifier parmi les 11 genres de pages web retenus, celui qui correspondait le mieux à la source d'information d'où ils préfèreraient obtenir leurs éléments de formation. Chaque génération a reçu le même sondage et les résultats sont présentés au Tableau 9.

TABLEAU 9 PROPORTION DES CHOIX DE SOURCES D'INFORMATION SUR LE WEB

	Baby-boomers	**Génération X**	**Milléniaux**
Blog	2%	4%	7%
Commercial	11%	9%	6%
Communauté	17%	29%	22%
Contenu	1%	1%	4%
FAQ	18%	19%	17%
Index	4%	1%	3%
Informatif	6%	5%	9%
Journalistique	21%	14%	12%
Officiel	10%	9%	9%
Personnel	3%	3%	4%
Scientifique	3%	3%	4%
Autre/sait pas	*5%*	*3%*	*3%*

[144] Sondage soumis via Amazon Mechanical Turk (Octobre 2018) sur une population de n=69 individus par cohorte.

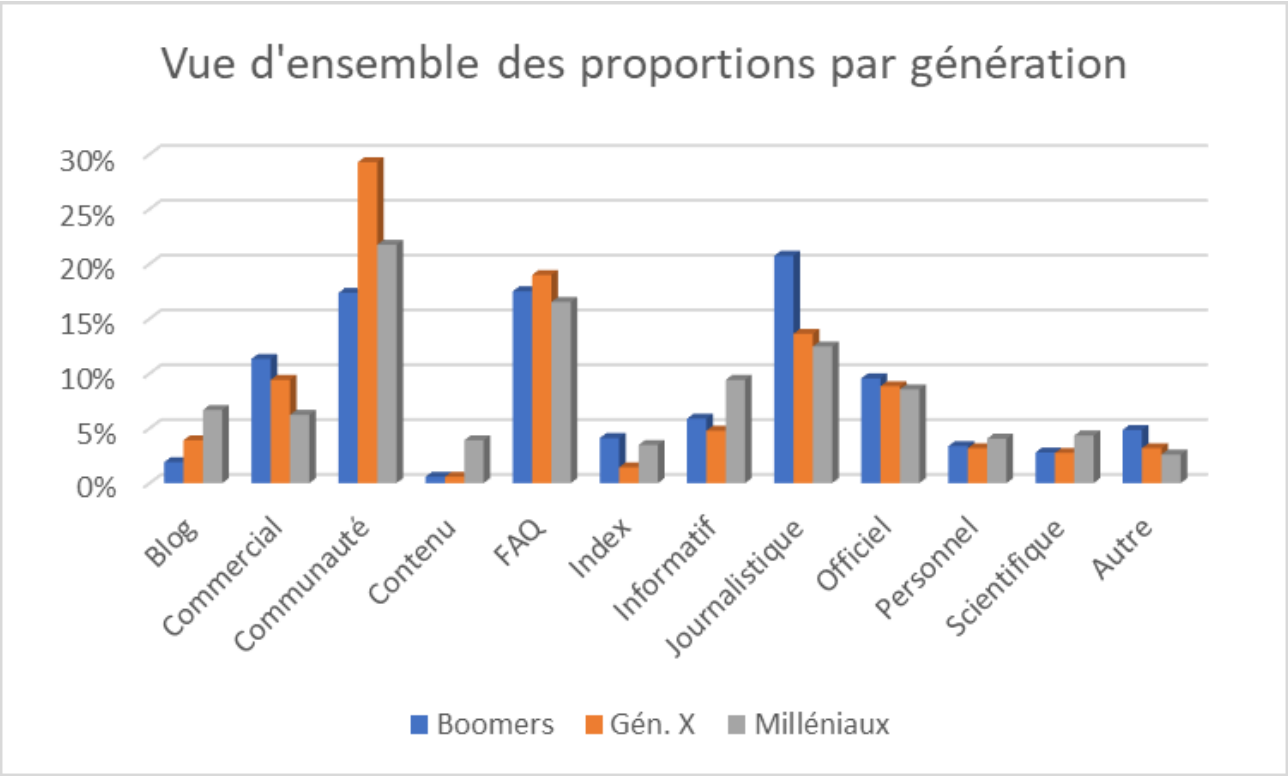


FIGURE 14 REPRÉSENTATION GRAPHIQUE DES RÉSULTATS DU SONDAGE

Interprétation des résultats obtenus (Tableau 9 et Figure 14):

- Alors que le genre « communauté » offre une opportunité d'échanger avec d'autres utilisateurs, le genre « FAQ » permet de prendre connaissance des expériences vécues pour éviter de répéter certaines erreurs ou obtenir des informations sur-le-champ. Ces aspects sont prisés par les individus de la génération X ainsi que les milléniaux. Les baby-boomers n'y sont pas en reste mais préfèrent épuiser les autres ressources avant de s'y référer.

- Le genre « journalistique » offre des ressources généralement recherchées pour la variété de contenus ainsi que le détail et l'harmonie dans la présentation de l'information. De plus, ce genre se prête bien au *microlearning* en offrant des ressources condensées. Ce sont des informations crédibles où les auteurs citent les sources. Les baby-boomers apprécient ce genre de page.

- Le genre « commercial » a un peu plus de crédibilité chez les plus âgés mais semble en perte de vitesse chez les plus jeunes. Ce genre de page offre une possibilité de formation très limitée dans tous les cas.

- Les trois générations se réfèrent de façon très limitée à des ressources « informatives », par exemple des livres ou documents explicatifs.

- Les trois générations voient un certain intérêt à obtenir des informations justes, à partir du genre « officiel ». On peut penser qu'avec la multitude d'informations disponibles sur le web, il est rassurant quand c'est possible, d'avoir la possibilité d'en valider la véracité et l'exactitude avec ce genre de page.

- Les genres « blog » et « personnel » sont généralement peu utilisés. Ceci peut s'expliquer par le fait qu'ils représentent des sources d'information subjectives (opinions d'un auteur) pouvant biaiser un apprentissage. Les générations plus jeunes y montrent cependant un certain intérêt.

- Le genre « index » est généralement peu populaire ne donnant qu'un accès indirect à l'information recherchée.

- Malgré un faible regain chez les milléniaux, le genre « scientifique » est peu populaire possiblement à cause de son aspect aride ou difficile d'approche pour un individu moyen.

- Les ressources provenant du genre « contenu » (ex : sites de téléchargement) sont moins populaires. Les plus jeunes générations présentant des traits axés sur la technologie et le multimédia, préfèrent se tourner vers des bases plus solides avec un contenu mieux rassemblé (par exemple le genre « journalistique »). Les milléniaux y démontrent quand même un intérêt. On doit comprendre ici que le genre « contenu » n'est pas pour autant mis de côté dans une formation avec *microlearning* mais il doit être utilisé avec parcimonie.

- On remarque finalement que la catégorie « Ne sait pas » décroît avec l'arrivée de plus jeunes générations. Ceux-ci sont généralement plus à l'aise avec toutes les ressources disponibles sur le web et sont capables d'arrêter leur choix parmi les genres offerts.

Nous avons donc résumé aux Tableau 10, Tableau 11 et Tableau 12 les **six genres préférés** de chacune des générations. Ce sont ces six choix que nous considèrerons dans la mise en place de notre base de connaissance pour les sources de formation.

TABLEAU 10 LES SIX GENRES PRÉFÉRÉS DES BABY-BOOMERS

	Attributs de cette génération	Contenu web les plus souhaitables à leur présenter, en ordre de priorité
Baby-Boomers	• Préfèrent une formation en face-à-face (quand c'est possible) • Ne sont pas tous adeptes de la technologie • Apprennent en écoutant • Lisent des articles et de livres • Utilisent le multimédia (mais en quantité limité)	**1. Journalistique** **2. FAQ** **3. Communauté** **4. Commercial** **5. Officiel** **6. Informatif**

TABLEAU 11 LES SIX GENRES PRÉFÉRÉS DE LA GÉNÉRATION X

	Attributs de cette génération	Contenu web les plus souhaitables à leur présenter, en ordre de priorité
Génération X	• Formation utilisant les outils web 2.0 • Besoin de questionner, alors possibilité de multiples sources pour confirmer. • Défis reliés à leur réalité. • Matériel bref et facile à lire • Multimédia • Base de connaissances structurée et simple • Aiment bien les graphiques • Période d'attention courte	**1. Communauté** **2. FAQ** **3. Journalistique** **4. Commercial** **5. Officiel** **6. Informatif**

TABLEAU 12 LES SIX GENRES PRÉFÉRÉS DES MILLÉNIAUX

	Attributs de cette génération	Contenu web les plus souhaitables à leur présenter, en ordre de priorité
Milléniaux	• Multimédia • Disponibilité partout / En tout temps • Flexibles • Multi-tâches • Dépendants de la disponibilité des ressources sur internet • Présence sur les réseaux sociaux • Simulations • Apprentissage structuré • Travail en équipe	**1. Communauté** **2. FAQ** **3. Journalistique** **4. Informatif** **5. Officiel** **6. Blog**

4.5 Notre proposition d'une architecture de Modèle Expert

Revenons donc à notre STI (Figure 10) et examinons le modèle expert. Un aspect de notre modèle expert est organisé dans un curriculum c'est-à-dire *une structure regroupant tous les éléments de connaissance liés entre eux selon des séquences pédagogiques* [Nkambou *et al.*, 2010]. La Figure 15 ci-dessous représente alors l'architecture, à plus haut niveau, de notre modèle expert contenant deux étapes importantes identifiées comme suit :

- **Étape A** : L'accès au système d'e-Learning
- **Étape B** : Le processus d'adaptation du système à l'apprenant qui tient compte de ses préférences de pages web. On y génère ici un curriculum adapté.

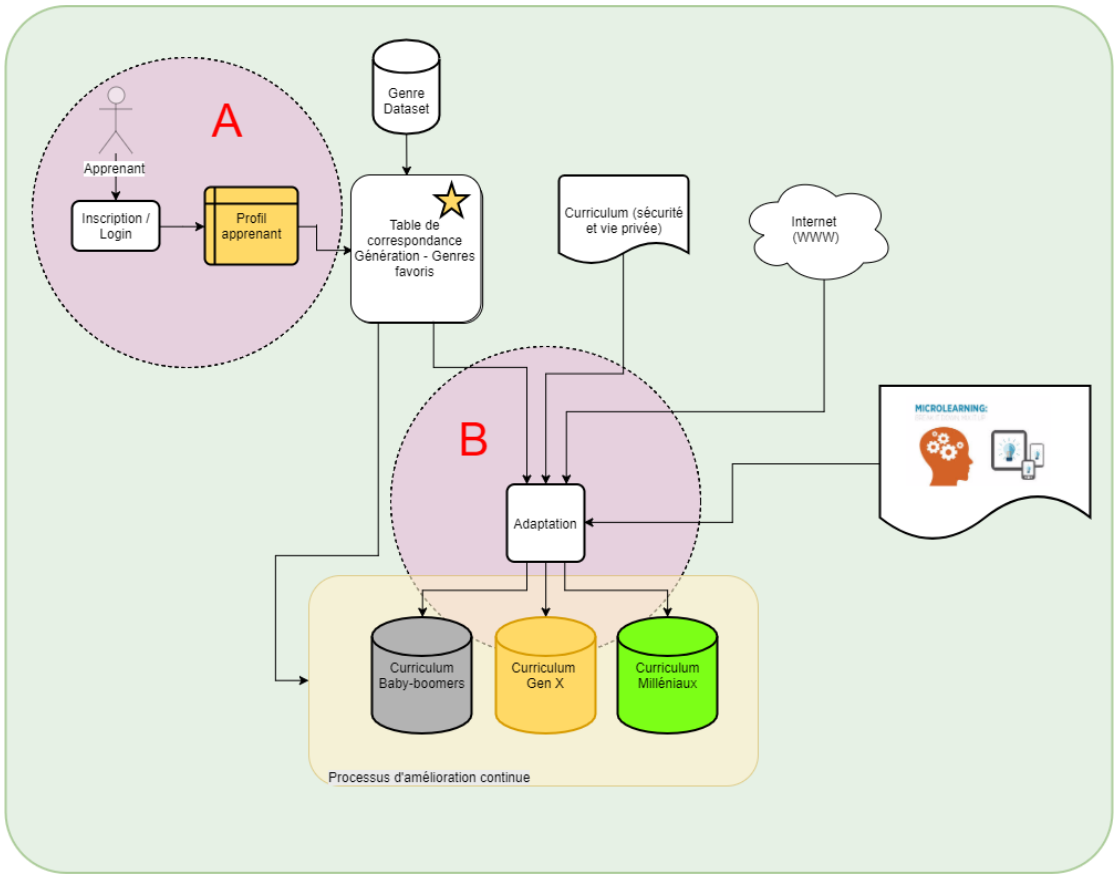


FIGURE 15 REPRÉSENTATION LOGIQUE DU MODÈLE EXPERT

La procédure d'accès (Figure 16 et Figure 17) au système CLEOPATRA requiert minimalement les informations suivantes :

- Un nom d'utilisateur (habituellement un pseudonyme)
- Une adresse de courriel (afin d'être en mesure de donner des rétroactions et instructions aux participants)
- Un mot de passe, que seul le participant connaît.
- Le sexe de la personne (Homme ou Femme, uniquement pour des fins statistiques)
- Dans quel intervalle d'années on retrouve l'année de naissance de l'utilisateur. Ceci nous indiquera à quelle génération l'utilisateur appartient. (On se rappellera ici que c'est une méthode d'anonymisation)

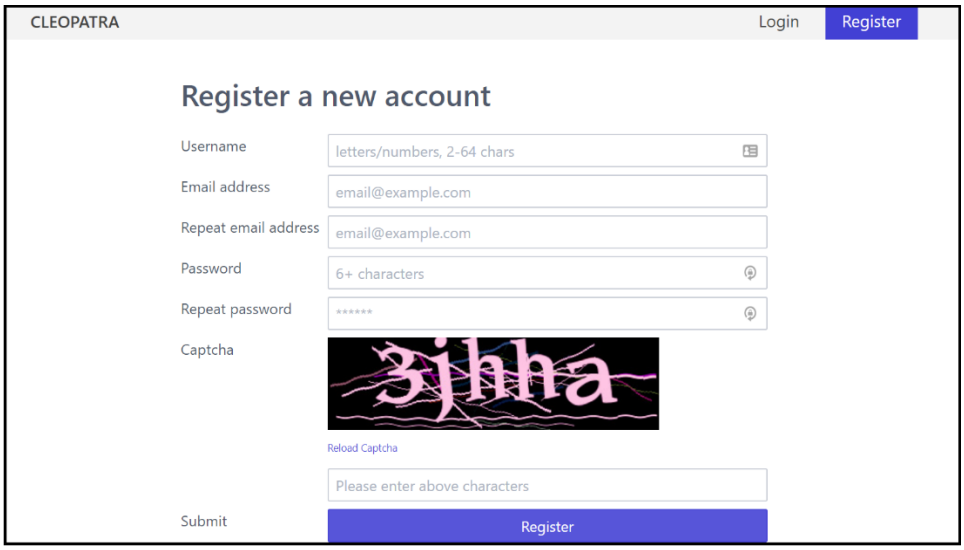


FIGURE 16 ÉCRAN DE CRÉATION D'UN NOUVEAU COMPTE D'APPRENANT

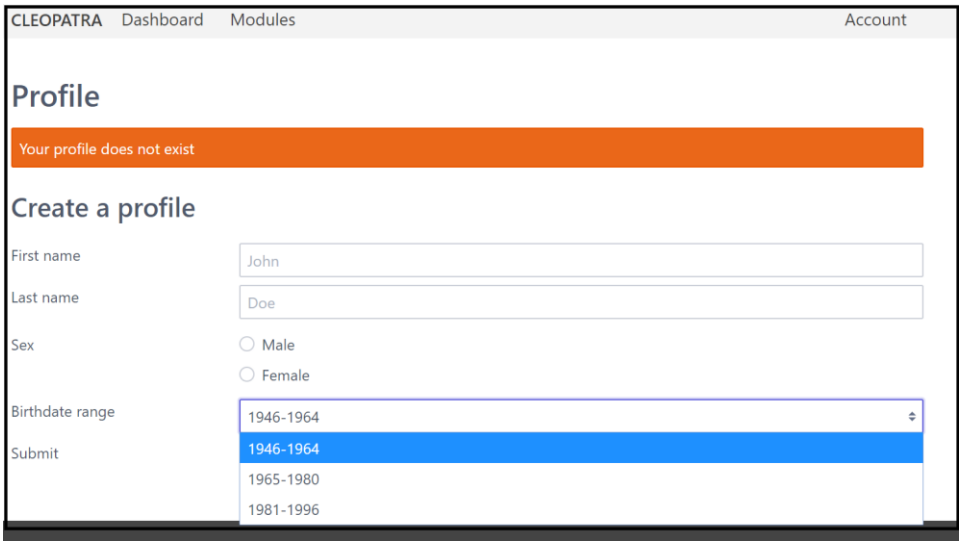


FIGURE 17 ÉCRAN DE CRÉATION D'UN PROFIL D'APPRENANT

La procédure obligatoire d'accès au système permet à l'apprenant de suivre la formation à son rythme, l'interrompre et la reprendre au moment voulu ou même de la resuivre s'il ou elle a besoin de rafraîchir ses connaissances.

Les informations collectées pendant la procédure d'inscription servent à construire un profil de l'utilisateur et à pouvoir s'y référer pour lui présenter un contenu adapté. On y répertorie la note obtenue dans chacun des modules (réf : Modèle de recouvrement – *Overlay model* à la section 3.3.1)

La seconde portion importante de cette architecture gravite autour de la procédure d'adaptation elle-même (Étape B de la Figure 15): elle tire ses informations des « préférences de genres de pages » pour chacune des générations. On se souviendra que ces préférences ont été obtenues à la suite d'un sondage permettant d'identifier en ordre du plus au moins favori, le genre de page web qui sera consulté pour aller chercher de la formation sur un sujet à apprendre.

L'adaptation s'inspire finalement du curriculum de formation en vie privée décrit à la section 3.1. CLEOPATRA présente les modules qui correspondent aux cinq domaines de connaissances identifiés dans ce curriculum.

Les modules adaptés à chaque génération utilisent les règles du *microlearning*[145] sans toutefois négliger la présence du processus d'amélioration continue qui nous permet de converger vers une adaptation optimale de la formation présentée (voir la prochaine section pour les détails à cet effet).

4.6 Présentation et Processus d'Amélioration du Contenu Offert

Le processus d'adaptation à l'apprenant est basé sur l'amélioration continue du contenu à présenter. Il s'agit de commencer avec un URL représentatif [146] du sujet de formation et de vérifier ensuite s'il est possible de remonter la liste de genres favoris de l'apprenant, selon la génération dont il fait partie (voir Tableau 10, Tableau 11 et Tableau 12).

[145] https://www.learnupon.com/blog/microlearning-intro/ Consulté le 2018-11-19

[146] Dans ce cas-ci, « représentatif » veut dire que le genre de page web choisi fait partie de la liste de genres favoris de la génération dont il est question.

Un algorithme (pseudo-code) est présenté ici pour une meilleure compréhension.

```
// Hypothèse : le URL initial pour un sujet donné, est une page dont le
// genre fait partie des six genres favoris de la génération en question.

genrePage ← DéterminerGenrePage (URL);
positionDepart ← PositionDansLaListe(genrePage, Génération);
i ← positionDepart;

Fini ← (i == 1); // vérifie si on est déjà optimal
WHILE NOT Fini // tant qu'on n'est pas rendu au premier (meilleur) genre
de la liste
{
      i ← i-1; // On tente avec un autre genre
      if genrePertinent (sujetFormation,i)
      {
            positionDepart ← i;
            Fini ← (i == 1);
      }
}
Return (positionDepart); // Position optimale
```

Voici un exemple :

On adresse la question à un individu de la génération X :

Qu'est-ce que le « Commissariat à la vie privée du Canada »?

Une recherche rapide sur le web nous donne comme référence initiale, le site web du CPVP i.e. http://www.priv.gc.ca . Selon notre liste de genres au Tableau 8 on pourrait classer ce genre de page web dans la catégorie « Commercial » (i.e. Pages d'accueil d'institutions ou d'organisations).

On pourrait explorer certains genres correspondant aux trois positions précédentes dans la liste des favoris de la génération X (Tableau 11), i.e. « Journalistique », « FAQ » et « Communauté ».

Commençons par le genre « Journalistique ». Un page de ce genre offre un contenu beaucoup plus agréable, bien condensé, moins formel et surtout plus accessible à une communauté d'utilisateurs. Il existe effectivement de très bons articles qui font référence au CPVP. Ce serait donc une première alternative souhaitable à viser. Habituellement les médias publient des informations basées sur des sources fiables, donc crédibles. Pour quelqu'un de la génération X, c'est un choix qui leur est plus approprié que le genre « Commercial ». A titre d'exemple pour ce

genre, on pourrait proposer un article de Radio-Canada du 31 octobre 2018 intitulé : « Les Entreprises devront signaler les atteintes à la vie privée des citoyens[147] ». On peut le retenir en attendant de trouver mieux.

Considérons ensuite le genre « FAQ » : Ce genre de page offre généralement des informations sur des questions pointues ou fréquentes et est limitée au niveau de la couverture des besoins. On peut donc dire que ce genre ne serait pas pertinent ici parce qu'on cherche à avoir une meilleure compréhension et connaissance de l'organisme CPVP.

Certaines pages du genre « Communauté » pourraient représenter un choix intéressant: En effet, plusieurs institutions gouvernementales font de plus en plus d'efforts [148] pour rejoindre les plus jeunes générations, en particulier par le biais des réseaux sociaux (facebook, instagram, twitter et youtube). Ils y proposent des contenus de qualité et divertissants.

Parce que ce genre (Communauté) est le premier choix dans les favoris pour la génération X, nous le retenons donc. La vidéo du CPVP intitulée : « My Privacy, My Choice, My Life[149] » donne un aperçu de l'organisation et de ses buts en quatre minutes. Ceci correspond donc mieux à ce qu'on recherche, surtout dans un contexte de *microlearning*.

On peut donc remplacer le lien initial par ce dernier lien et ainsi nous avons amélioré le contenu de la formation sur ce sujet.

4.7 Module de l'interface et Quiz

En référence à la Figure 10 de la section 3.3, il ne reste qu'à présenter le module de notre interface utilisateur (voir Figure 18). Ce module puise ses sources d'information à partir des curriculums de formation adaptés pour chacune des générations. Il donne la possibilité à l'utilisateur de visualiser le contenu des liens offerts dans chacun des différents domaines de connaissances, à partir du fureteur de son choix. Il faut donc comprendre que bien que les sujets

[147] https://ici.radio-canada.ca/nouvelle/1133131/loi-protection-donnees-personnelles-politique-vie-privee accédé le 2018-12-20
[148] https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/medias-sociaux-politiques-avis/ accédé le 2018-12-17
[149] https://www.youtube.com/watch?time_continue=6&v=eH6t20mlMVE accédé le 2018-12-20

soient les mêmes pour toutes les générations, les URL offerts et par conséquent les pages présentées seront habituellement différentes pour chacune des trois générations.

Il y a cependant deux raisons qui font qu'un genre de page sur une connaissance donnée, soit identique pour plus d'une génération : soit que le genre de page la plus approprié pour ces générations (au moment de la recherche de cette information) soit identique, soit qu'il n'était pas possible de trouver un lien dont le genre était adapté à une génération particulière. Les administrateurs du site de e-Learning pourront revisiter occasionnellement la base de connaissances afin de mettre à jour les liens pour qu'ils reflètent les nouvelles disponibilités d'information du web.

Partie importante de l'approche de *microlearning*, un quiz de quelques questions à choix multiples est présenté à l'apprenant afin de valider son niveau d'absorption et de compréhension des sujets présentés, à la fin de chaque module. La note du quiz obtenue sera inscrite au profil de l'utilisateur. Il est important de savoir que cette note n'est pas modifiée lorsque le participant repasse la formation. Par exemple, si j'ai obtenu 40% à mon premier quiz dans un des domaines de formation, cette note demeurera à 40% dans mon profil même si j'ai les bonnes réponses quand je reprends la formation dans ce domaine. En effet, c'est la note obtenue aux tests d'évaluation (initial et final) qui est importante et qui sert à mesurer les progrès des participants.

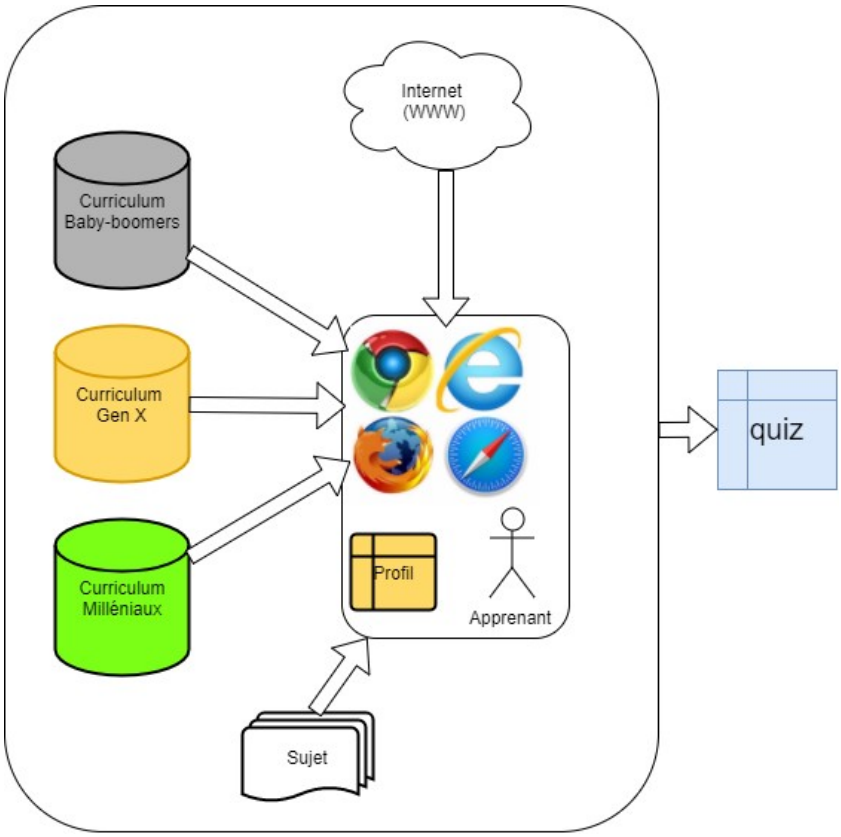


FIGURE 18 REPRÉSENTATION LOGIQUE DU MODULE DE L'INTERFACE

4.8 Le contenu de la base de connaissance

Nous avons déployé une version initiale de la base de connaissances (Figure 10) pour les trois générations. La répartition des genres de page suit notre proposition des favoris (Tableau 10, Tableau 11 et Tableau 12) et dans la mesure du possible offre un genre optimal. Ce qui n'est pas toujours le cas, soit parce que nous n'avons pas trouvé un genre optimal associé au sujet en question ou parce que nous n'avons volontairement pas optimisé certaines ressources afin d'offrir une

variété de genres parmi les favoris. La Figure 19 représente la répartition des genres dans la base de connaissances que nous utiliserons pour l'évaluation initiale de CLEOPATRA.

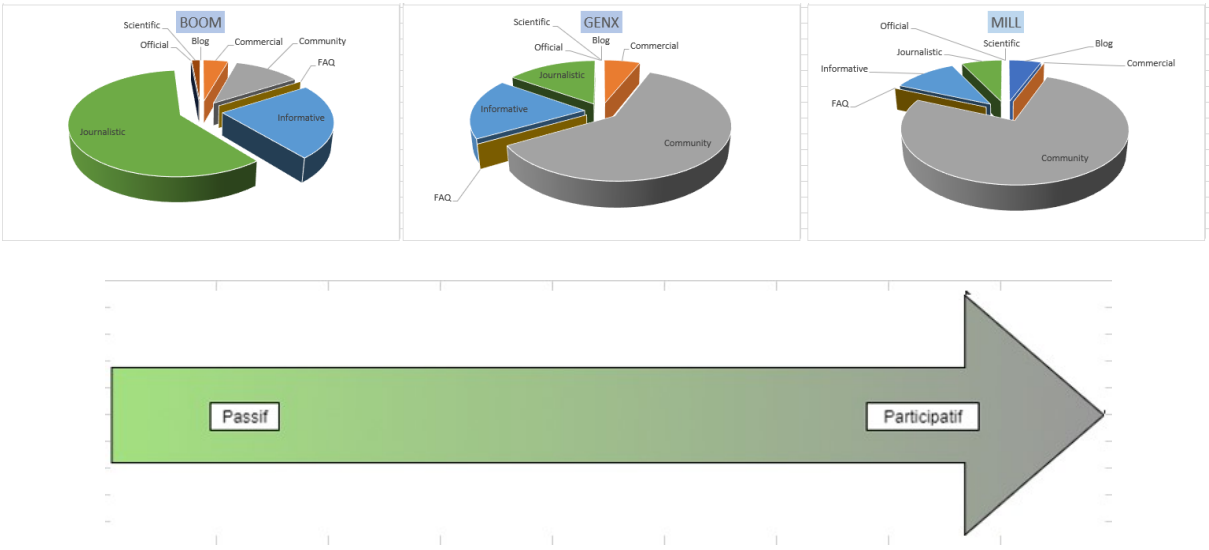


FIGURE 19 RÉPARTITION DES GENRES PAR GÉNÉRATION DANS LA BASE DE CONNAISSANCES

A première vue, on peut remarquer que du point de vue des générations, l'aspect participatif des plus jeunes évolue vers l'utilisation de ressources où il leur est possible de contribuer (ou participer) d'une quelconque façon. A l'opposé, les plus âgés (ex : baby-boomers) semblent préférer utiliser des ressources éducatives d'une manière plus passive. Ces deux observations concordent bien avec les caractéristiques cognitives des générations précédemment décrites.

Il était important pour nous d'assurer que la base de connaissances offrait une proportion majoritaire (plus de 51%) du genre favori optimal pour chaque génération. Ce résultat a été assez facile à obtenir compte tenu du grand nombre de sources disponibles sur le web. On comprendra aisément qu'il est aussi possible de continuer à modeler cette base de connaissances grâce au processus d'amélioration continue et de la disponibilité de nouvelles ressources.

Chapitre 5. Évaluation du système CLEOPATRA

Nous en sommes maintenant arrivés au point où nous souhaitons voir fonctionner notre proposition modélisée du flux de travail tel que représenté à la Figure 13.

Nous suggérons donc d'en valider le fonctionnement avec quelques participants, utilisateurs d'une montre intelligente ou bracelet électronique, et qui ne sont pas des professionnels dans le domaine de l'informatique.

5.1 Critères de succès

Parce que l'internet devient un fournisseur principal de connaissances dans un contexte de e-learning, il est souhaitable que notre système réponde à des critères de qualité minimales. [Jindal, 2018] définit une structure intéressante de critères à considérer dans l'évaluation d'une approche de e-Learning. Ces critères sont représentés au Tableau 13 et nous y avons indiqué comment CLEOPATRA les rencontre.

TABLEAU 13 ÉVALUATION DES CARACTÉRISTIQUES DE CLEOPATRA [JINDAL, 2018]

Critères de sélection du site de e-Learning CLEOPATRA	Facteurs qualitatifs	Fonctionnalité	C'est est un système **adaptable**, qui jouit d'une **interopérabilité** certaine (web-based) et qui utilise une plateforme **sécuritaire** (fureteurs populaires, PHP, MySQL)
		Portabilité	Il est **modelable** à tout type de formation. Il est **simple à installer**.
		Maintenabilité	La **maintenance et les changements sont simples**, généralement limités à une mise à jour des informations dans la base de données en utilisant un outil convivial de gestion de BD.
		Utilisabilité	Son utilisation ne requiert que **peu d'efforts.**
		Fiabilité	Les informations qu'on y trouve se doivent d'être **adéquatement choisies**.

		Efficacité	Le **niveau de performances est amplement suffisant** et en lien avec l'internet.
	Facteurs spécifiques	Interface utilisateur	Il possède une **interface simple et intuitive** présentant les modules reliés aux domaines de connaissances.
		Communauté d'apprentissage	Il **ne possède pas** encore cette fonctionnalité mais cette dernière pourrait être ajoutée **dans un contexte d'amélioration du produit**.
		Contenu	Le contenu doit être **suivi et révisé lorsque jugé nécessaire**, selon les nouveautés disponibles de l'internet.
		Personnalisation	L'utilisation d'un **curriculum adapté** selon la génération permet de **rencontrer les besoins des individus d'une manière efficace.**
		Généralités	Selon **le rythme et la disponibilité** de l'individu. Accès à un **dossier étudiant**.

5.2 Défi

Contribuer à une telle étude requiert un engagement exigeant un certain temps de lecture que certains n'ont pas voulu investir, malgré une rémunération promise. Ce manque d'intérêt est explicable lorsqu'on se réfère aux fondements andragogiques (section 3.3.5). On les traduit par l'absence individuelle d'implication dans la planification, le manque d'intérêt personnel mais surtout l'inexistence d'un problème qui serait une source de motivation pour justifier cet effort.

Nous avons quand même pu récolter quelques résultats dans chacune des trois générations et ainsi démontrer que CLEOPATRA fonctionne et apporte des bénéfices supplémentaires.

5.3 Fonctionnement

Les candidats passent un premier test d'évaluation[150] qu'ils peuvent remplir en ligne. On y pose des questions dans les cinq domaines de connaissances du curriculum de la section 3.1. On mesure ainsi leurs connaissances actuelles.

Lorsque cette première évaluation est complétée, nous procédons à sa correction et nous calculons la note obtenue dans chacun des domaines de connaissances. On envoie par la suite une

[150] https://goo.gl/forms/WGmaTiYaN3OJNifZ2 accédé le 2019-03-01

invitation à utiliser le système CLEOPATRA avec une priorisation de formation dans les domaines de connaissances où le participant n'a pas obtenu la note de passage. Il peut aussi arriver que nous suggérions une formation supplémentaire mais facultative dans les domaines de connaissances où il a obtenu tout juste la note de passage (voir les Figure 22 et Figure 23) car nous croyons qu'il pourrait en tirer profit.

Une fois cette formation terminée, le participant repasse le test d'évaluation, ce qui nous permet de constater les progrès réalisés et démontre que CLEOPATRA les a bien aidés.

5.4 Participants

Il a été possible de trouver des participants dans chacune des générations selon la répartition suivante :

TABLEAU 14 DISTRIBUTION DE LA POPULATION DE L'ÉVALUATION

Génération	Homme / Femme	Nombre total
Milléniaux	1 H / 5 F	6
Génération X	1 H / 1 F	2
Baby-boomers	0 H / 2 F	2

Il a fallu se rendre à l'évidence de la présence marquée de milléniaux (âgés approximativement de 23 à 37 ans) dans cet échantillon, résultat prévisible[151] car ils représentent la clientèle majoritaire de bracelets/montres intelligents.

5.5 Résultats

Les résultats obtenus (Tableau 15) suite à la participation de nos candidats sont assez éloquents. Pour chacun des cinq modules de CLEOPATRA, correspondant à un domaine de connaissances en particulier, nous y avons affiché les notes obtenues, avant et après la formation. Le plan de formation qui y est aussi présenté, inclut les numéros de modules où le participant n'a pas obtenu la note de passage. Ce plan suggère aussi une formation facultative à propos de certains modules où il serait souhaitable, mais non obligatoire, d'aller chercher une amélioration.

[151] Selon une nouvelle de la firme de sondage Ipsos : les DPI sont plus populaires parmi les milléniaux https://www.ipsos.com/en/who-are-worlds-biggest-wearable-tech-buyers accédé le 2019-03-01

Dans tous les cas présentés ici, chaque participant ayant suivi la formation recommandée y a vu ses notes améliorées. Nous avons représenté ces améliorations par un (+). On peut aisément constater cette amélioration en comparant les résultats AVANT et APRÈS. Comme effet secondaire bénéfique, nous avons aussi remarqué que la grande majorité des participants ont amélioré leurs résultats de domaines qui ne leur avaient pas été suggérés et pour lesquels ils avaient déjà obtenu une assez bonne note. Nous les avons représentés dans le tableau par une astérisque (*).

Notre processus d'évaluation aurait cependant bénéficié des commentaires libres des participants au niveau du choix de la documentation sélectionnée et de la pertinence des genres de pages web utilisées. Nous avons demandé cette information d'une façon informelle mais aucun n'a pris le temps de nous répondre sur ce point.

CLEOPATRA est donc une approche qui fonctionne et qui aide les adultes à « augmenter » leur niveau de connaissances en sécurité et en vie privée dans un contexte non-académique.

TABLEAU 15 RÉSULTATS MESURÉS À L'ÉVALUATION

Prénom	Génération	Résultats AVANT la formation					Plan de formation	Résultats APRÈS la formation					Améliorations + : réussi * : gain suppl.				
	Modules	1	2	3	4	5		1	2	3	4	5					
	Notes de passage	*6*	*6*	*8*	*5*	*6*		*6*	*6*	*8*	*5*	*6*					
Valérie	Millénial	4	8	8	10	6	1 et 5 (optionnel)	9	8	10	10	8	+				+
Catherine	Millénial	4	6	5	7,5	5	1, 3 et 5	10	8	10	5	7	+	*		+	+
Sofie	Millénial	5	7	8	5	7	1 et 4 (optionnel)	8	6	8	7,5	8	+			*	*
William	Millénial	5	4	10	5	7	1 et 2	9	8	10	7,5	9	+	+		*	*
Evemarie	Millénial	8	8	8	7,5	8	1 à 5 au choix	10	8	8	7,5	8	+				
Caroline	Millénial	4	7	10	7,5	9	1	10	6	10	10	8	+			*	
Julien	Gén. X	5	7	8	10	6	1 et 5	9	8	8	5	7	+	*			+
Karine	Gén. X	8	8	5	7,5	8	3	8	8	8	7,5	9			+		*
Suzanne	Boomer	6	8	10	7,5	7	1 (optionnel)	10	8	10	10	9	+			*	*
Annick	Boomer	9	8	10	10	8	1 à 5 au choix	10	8	10	10	9	*				*

- *Module 1 : Connaissance de la règlementation*
- *Module 2 : Connaissance générale en sécurité informatique*
- *Module 3 : Connaissance générale en vie privée*
- *Module 4 : Informations personnelles*
- *Module 5 : Connaissances générale de la technologie Connaissance*

Chapitre 6. Conclusion

Bien que cette recherche porte sur les dispositifs portables intelligent, il faut comprendre que ce n'est qu'une seule des nombreuses technologies qui nous amènent à élaborer sur les risques inhérents à la vie privée de ces objets connectés et par conséquent nous incitent à trouver une façon intéressante d'en sensibiliser les utilisateurs à l'aide d'un moyen convivial et accessible.

La formation est un sujet qui peut être approché de multiples façons. En particulier, le design d'un système d'e-Learning bâti à partir d'un système de tutorat intelligent, qu'on combine à un curriculum adapté de formation en sécurité et en vie privée, nous fournit une fondation solide pour y arriver. Les méthodes modernes en éducation telles que le *microlearning* et l'approche andragogique (et heutagogique) tenant compte des styles d'apprentissage générationnels se sont avérées originales mais très pertinentes si on en croit les résultats de notre évaluation. Parce qu'il n'en existait pas réellement, nous avons opté pour utiliser une adaptation du curriculum axé sur la sécurité et vie privée de notre équipe de recherche du laboratoire Héron. Ce curriculum contient les domaines de connaissances à approfondir afin de mitiger les risques tels que nous les avons présentés dans l'introduction de cette recherche.

Notre approche s'est avérée fructueuse parce que nous avons obtenu des résultats positifs souvent meilleurs que ceux espérés. Nous avons constaté que l'approche générationnelle nous permet de rejoindre une majorité d'individus d'un groupe d'âge donné, à qui nous pouvons proposer une solution naturellement adaptée. Il aurait été intéressant de pouvoir valider le fonctionnement sur une plus grande population de nos trois générations mais force est de croire que nous aurions obtenu des résultats similaires sinon identiques.

La présente recherche a donc permis de jeter les bases de cette approche mais il reste beaucoup de travail en vue de l'améliorer, surtout par rapport à sa mise en place et ses tâches administratives. Une **première amélioration** à apporter s'appliquerait au niveau de la *détermination automatisée du genre des pages web*. Ceci nous permettrait de bâtir et maintenir plus efficacement notre base de connaissances en fonction de l'évolution du contenu disponible sur l'internet. Une **seconde amélioration** pourrait être celle *d'automatiser le processus d'amélioration continue* tel que nous le décrivons à la section 4.6 .A date, ce sont les deux tâches qui requièrent une intervention humaine

importante et qui feraient de CLEOPATRA un système plus alléchant à implanter quel que soit le sujet à approfondir par différentes classes d'individus.

Nous avons donc démontré la pertinence et l'utilité de CLEOPATRA au niveau de la sensibilisation aux impacts à la vie privée des dispositifs portables intelligents. Dans un avenir rapproché où les objets connectés prendront de plus en plus de place et amasseront des quantités encode plus importantes de données dans le *cloud*, il sera raisonnable de croire que CLEOPATRA aura permis de poser les premiers jalons d'une sensibilisation adéquate des utilisateurs de ces technologies.

Chapitre 7. Annexe

7.1 Test d'Évaluation des Connaissances

Ce test permet une évaluation initiale des connaissances du participant vet une évaluation de l'efficacité de l'apprentissage du système CLEOPATRA lorsque ce test est repassé suite au e-Learning avec CLEOPATRA.

Questions d'évaluation sur la sécurité informatique
Vous recevez un email du Bureau de soutien informatique: "À partir de la semaine prochaine, nous supprimerons tous les comptes de messagerie inactifs afin de créer de l'espace pour davantage d'utilisateurs. Vous devez envoyer les informations suivantes pour continuer à utiliser votre compte de messagerie. Si nous ne recevons pas ces informations d'ici la fin de la semaine, votre compte de messagerie sera fermé: Nom (prénom et nom), Identifiant de connexion, Mot de passe, Date de naissance, E-mail secondaire. Veuillez contacter l'équipe Webmail pour toute question. Merci pour votre attention immédiate". Que faire? (2 pts) A) Cela semble légitime. Je fournis toutes les informations requises B) Cela semble légitime, mais je veux faire attention. Je fournis une partie (mais pas la totalité) des informations requises C) Supprimer le message: un service d'assistance légitime ne demanderait jamais de telles informations confidentielles et sensibles par courrier électronique. ✓ D) Douteux. Je ne peux pas authentifier l'expéditeur. Je réponds et demande une confirmation. E) Douteux. Certaines des informations requises sont personnelles et sensibles, mais le fait qu'elles proviennent du centre d'assistance me rassure. Je réponds avec les informations requises
Bien que les appareils connectés à l'Internet des Objets (montres intelligentes, frigidaires intelligents, thermostats intelligents, etc) soient des produits innovants, ils ne sont pas conçus dans un souci de sécurité et de confidentialité. Laquelle de ces affirmations N'EST PAS VRAIE? (2 pts) A) Ils ont une procédure d'identification faible. B) L'application de correctifs de sécurité et de mises à jour est un processus fastidieux. C) Il faut des années pour développer un appareil de sa conception à sa commercialisation ✓ D) Les vulnérabilités apparaissent souvent dans les applications Web et mobiles des appareils.
Les nouvelles montres intelligentes sont fascinantes! Elles sont autonomes et certaines n'ont même pas besoin d'être jumelées à un smartphone. Elles utilisent la connectivité cellulaire 4G LTE, vous permettant de rester "en ligne" en tout temps. (2 pts) A) Les grandes marques (Apple, Garmin, Huawei, Fitbit, etc.) jouissent d'une excellente réputation et ne commercialiseraient pas un produit dangereux. Ce sont des personnes sérieuses et vous avez la certitude que vos informations personnelles sont protégées. B) Ces grandes marques (Apple, Garmin, Huawei, Fitbit, etc.) ont certainement respecté les normes de sécurité du secteur en ce qui concerne les appareils connectés. C) Il n'y a toujours pas de normes de sécurité dans le monde des appareils connectés sur Internet, car les entreprises doivent répondre à une demande rapide et croissante. ✓ D) Seulement les deux premières réponses sont vraies

Vous souhaitez installer sur votre smartphone une autre application que celle fournie par le manufacturier de votre smartwatch. Cependant, elles sont nombreuses dans l'AppStore. Elles ont toutes de bonnes critiques. Quels sont les bons critères sur lesquels vous pouvez compter? (2 pts)

A) Examinez attentivement la section d'informations supplémentaires: vous devez être en mesure d'authentifier facilement l'entreprise qui a développé l'application.
B) Une application sécurisée devrait limiter ses exigences d'accès aux données au minimum requis pour son bon fonctionnement et cette liste devrait être facilement disponible.
C) Il devrait y avoir un lien vers la politique de confidentialité de l'entreprise
D) Il devrait y avoir une adresse email pour l'information et le support
E) Toutes ces réponses sont bonnes ✓

Le jumelage entre une smartwatch (ou un bracelet intelligent) et un smartphone s'effectue généralement à l'aide de la technologie Bluetooth. Cette procédure est totalement sécurisée et la fuite de données privées est techniquement impossible. (1 pt)

A) Vrai
B) Faux ✓

Vous et votre conjoint possédez une montre intelligente. Vous aimez ce nouveau gadget techno mais vous préférez l'utiliser sans vous soucier de la configuration. A ce sujet, vous communiquez votre mot de passe à votre épouse et vous lui en déléguez le soutien. Quelle leçon devriez-vous apprendre de cela? (1 pt)

A) Votre mot de passe ne devrait jamais être partagé ✓
B) Vous n'avez rien à cacher
C) Votre épouse enregistre votre mot de passe sur sa smartwatch afin de ne pas l'oublier.
D) Votre épouse et vous décidez d'utiliser le même mot de passe.
E) Les deux smartwatches n'ont pas de mot de passe. En cas d'incident, peu importe, votre conjoint reconstruira la configuration à partir de zéro.

Questions d'évaluation sur la vie privée

Bibitte, une entreprise de bracelets intelligents bien connue, a une politique de confidentialité qui stipule que seules les données relatives à la santé, à l'âge et à la date de naissance sont conservées à des fins d'enseignement et de recherche. Votre nom ne sera jamais divulgué. Que pensez-vous de ce processus d'anonymisation des données? (3 pts)

A) L'anonymisation des données (telles que l'effacement, l'utilisation d'un pseudonyme, l'ajout de bruit) est une procédure sûre et irréversible.
B) Il est possible de croiser des données anonymisées avec des données obtenues d'autres sources (par exemple, des réseaux sociaux) pour avoir une possibilité de ré-identification. ✓
C) L'anonymisation n'est pas complètement sûre, mais il n'y a pas vraiment de risque que quelqu'un fouille une base de données aussi énorme

Vous êtes invités à visiter un célèbre cabinet d'avocats. Dans la grande salle de travail, des dizaines de professionnels travaillent sur des documents juridiques. Vous souhaitez prendre une photo de ces personnes au travail avec l'appareil photo intégré de votre nouvelle montre intelligente et la partager sur votre réseau social préféré. (3 pts)

A) Vous prenez discrètement la photo et ensuite la partagez.
B) Vous prenez la photo discrètement mais avant de la partager, vous la visualisez et confirmez qu'il n'y a pas de contenu sensible.

C) Vous demandez la permission avant de prendre la photo, vous vous assurez qu'il n'y a pas de contenu sensible et vous le cachez si nécessaire. Il serait souhaitable, en plus de valider la photo et d'obtenir une autorisation appropriée avant de la publier. ✓

Votre vie en tant que couple moderne est très chargée: travail, réunions, voyages d'affaires, restaurants, séances de gymnastique, etc. Ce sera bientôt votre anniversaire de mariage et vous envisagez de vous offrir une montre intelligente. Ce sera non seulement attrayant, mais pratique, car cela vous aidera à mieux communiquer les uns avec les autres. En effet, ces montres disposent d'un système de positionnement intégré (GPS) permettant de localiser et de suivre vos déplacements. Que pensez-vous de cette idée? (2 pts)

A) Nous devrions tous en avoir un. Pourquoi avons-nous attendu si longtemps?
B) Nos amis en ont déjà un et leurs commentaires sont positifs. C'est assez pour vous convaincre d'acheter.
C) Vous et votre conjoint pourrez connaître la position de chacun à tout moment. Ces données seront également archivées sur le site du fabricant, qui vous renseignera également sur vos déplacements quotidiens. ✓
D) Ne paniquez pas: Il s'agit de données de positionnement simples. Pas grave!
E) Le premier, second et quatrième choix sont de bons choix

Dernièrement, vous avez remarqué que certaines des données relatives à la santé rapportées par votre bracelet intelligent Bibitte sont très différentes de ce qu'elles étaient. Votre état de santé a peut-être changé, mais vos données peuvent également avoir été falsifiées. Quoi que ce soit: (2 pts)

A) Vous pensez que les choses finiront par se placer. En attendant, vous êtes le seul à être conscient de cette situation.
B) Il est possible que les données envoyées par votre application soient analysées et que vous receviez une publicité ciblée sur certains aspects de votre santé. Ces publications peuvent être pertinentes ou non, selon le motif du changement de données. ✓
C) Les données de votre traqueur peuvent être partagées ou revendues. Dans ce cas, votre compagnie d'assurance-vie pourrait en être informée et ajuster le montant de vos primes, éventuellement à votre désavantage.
D) Vos amis peuvent prendre conscience de cette situation sans que vous ayez à leur dire, car vous partagez déjà certaines données.
E) Le second, troisième et quatrième choix représentent la bonne réponse.

Questions d'évaluation sur les informations personnelles

Les activités de recherche en ligne, telles que les transactions électroniques, sont des points de données qui peuvent aider à former une identité numérique (2,5 pts)

A) Vrai ✓
B) Faux

Qu'est-ce qui ne représente PAS une donnée personnelle? (2,5 pts)

A) Adresse de votre résidence
B) Votre position géographique
C) Le numéro d'enregistrement d'une entreprise ✓
D) Votre nom et prénom
E) Le numéro d'une carte d'identité

Identifiez ce qui fait partie d'un dossier pédagogique (2,5 pts)

A) Résultat scolaire (note) / bulletin de notes
B) horaire d'un étudiant
C) examen, thèse, mémoire
D) adresse courriel d'un étudiant
E) Tous ces choix peuvent faire partie du dossier ✓

Les données financières peuvent rapidement devenir inutilisables après un vol, car les personnes peuvent rapidement changer le numéro de leur carte de crédit. Mais les données médicales ne sont pas périssables, ce qui les rend particulièrement utiles. (2,5 pts)

A) Vrai ✓
B) Faux

Questions d'évaluation sur la Technologie

Un pare-feu (firewall) n'est PAS conçu pour empêcher tout accès non autorisé vers ou depuis un réseau privé (1 pt)

A) Vrai
B) Faux ✓

Lequel des choix suivants est nocif pour un ordinateur? (1 pt)

A) Antivirus
B) Virus ✓
C) Gratuiciel (Freeware)
D) Partagiciel (Shareware)

Quel énoncé représente le mieux un VPN? (1 pt)

A) Un VPN est un réseau virtuel privé (Virtual Private Network)
B) Un VPN chiffre et masque votre adresse IP
C) Un VPN dissimule votre identité
D) Les 3 premières réponses sont bonnes ✓
E) Aucune de ces réponses

Les systèmes biométriques enregistrent des informations personnelles sur des individus identifiables. (1 pt)

A) Vrai ✓
B) Faux

Le cloud computing consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet (1 pt)

A) Vrai ✓
B) Faux

Identifiez un risque sur les réseaux sociaux? (1 pt)

A) Cybercriminalité
B) Cyberharcèlement
C) Agression sexuelle
D) Contacts indésirables
E) Données ineffaçables
F) Le premier, second, quatrième et cinquième choix
G) Toutes ces réponses ✓

Les applications de géolocalisation exécutées sur des appareils mobiles ne fournissent pas une expérience plus riche que celles exécutées sur des ordinateurs de bureau. (1 pt)

A) Vrai
B) Faux ✓

Comment la vie privée et la protection des données sont-elles liées? (1 pt)

A) La protection des données est un sous-ensemble de la vie privée
B) La vie privée est un sous-ensemble de la protection des données
C) C'est la même chose
D) Vous ne pouvez pas avoir de vie privée sans la protection des données ✓

Les courtiers en données sont des entreprises qui collectent des informations personnelles sur les consommateurs strictement auprès de sources publiques et les revendent à d'autres entreprises (1 pt)

A) Vrai
B) Faux ✓

_____ habilite l'IdO (Internet des Objets) en reliant entre eux des objets de la vie quotidienne. (1 pt)

A) L'Intelligence
B) La Connectivité ✓
C) La Nature Dynamique
D) La Grandeur d'Échelle

Questions d'évaluation sur la règlementation

Le Commissaire à la protection de la vie privée du Canada est un agent du Parlement canadien dont la mission est de protéger et de promouvoir le droit à la vie privée. (1 pt)

A) Vrai ✓
C) Faux

La Federal Trade Commission (FTC) des États-Unis recueille les plaintes relatives à des problèmes allant de la sécurité des données et de la publicité trompeuse au vol d'identité. La FTC collabore avec des organismes d'application de la loi étrangers dans le cadre d'enquêtes et d'affaires impliquant des consommateurs américains. (1 pt)

A) Vrai ✓
B) Faux

En application depuis le 25 mai 2018, le règlement général sur la protection des données (RGPD ou en anglais GDPR) est un règlement de l'Union européenne qui constitue le texte de référence pour la protection des données à caractère personnel. (1 pt)

A) Vrai ✓
C) Faux

La loi canadienne relative à la confidentialité des données est beaucoup plus complète que celle de l'Union européenne (RGPD) (1 pt)

A) Vrai ✓
C) Faux

ISO / IEC 27001 spécifie un système de management dont les objectifs se limitent à suggérer des exigences spécifiques en matière de sécurité de l'information. (1 pt)

A) Vrai
C) Faux ✓

Laquelle des affirmations ci-dessous est la moins probable à être présente dans une politique de confidentialité? (3 pts)

A) Les détails sur la conservation des informations (confidentielles ou non)
B) Une liste des informations spécifiques collectées
C) Avec quels partenaires seront partagées vos informations
D) La façon de présenter une demande concernant la législation en vigueur ✓

Qui suis-je? Une organisation composée de 36 pays membres, créée en 1961 et offrant une plate-forme pour comparer les expériences politiques, rechercher des réponses aux problèmes communs, identifier les bonnes pratiques et coordonner les politiques nationales et internationales de ses membres. (2 pts)

A) CNIL (Commission Nationale de l'Informatique et des Libertés)
B) COE (Council of Europe)
C) FTC (Federal Trade Commission)
D) OCDE (Organisation pour la Coopération et le Développement Économique) ✓

7.2 Curriculum de Formation en Vie Privée (Version complète)

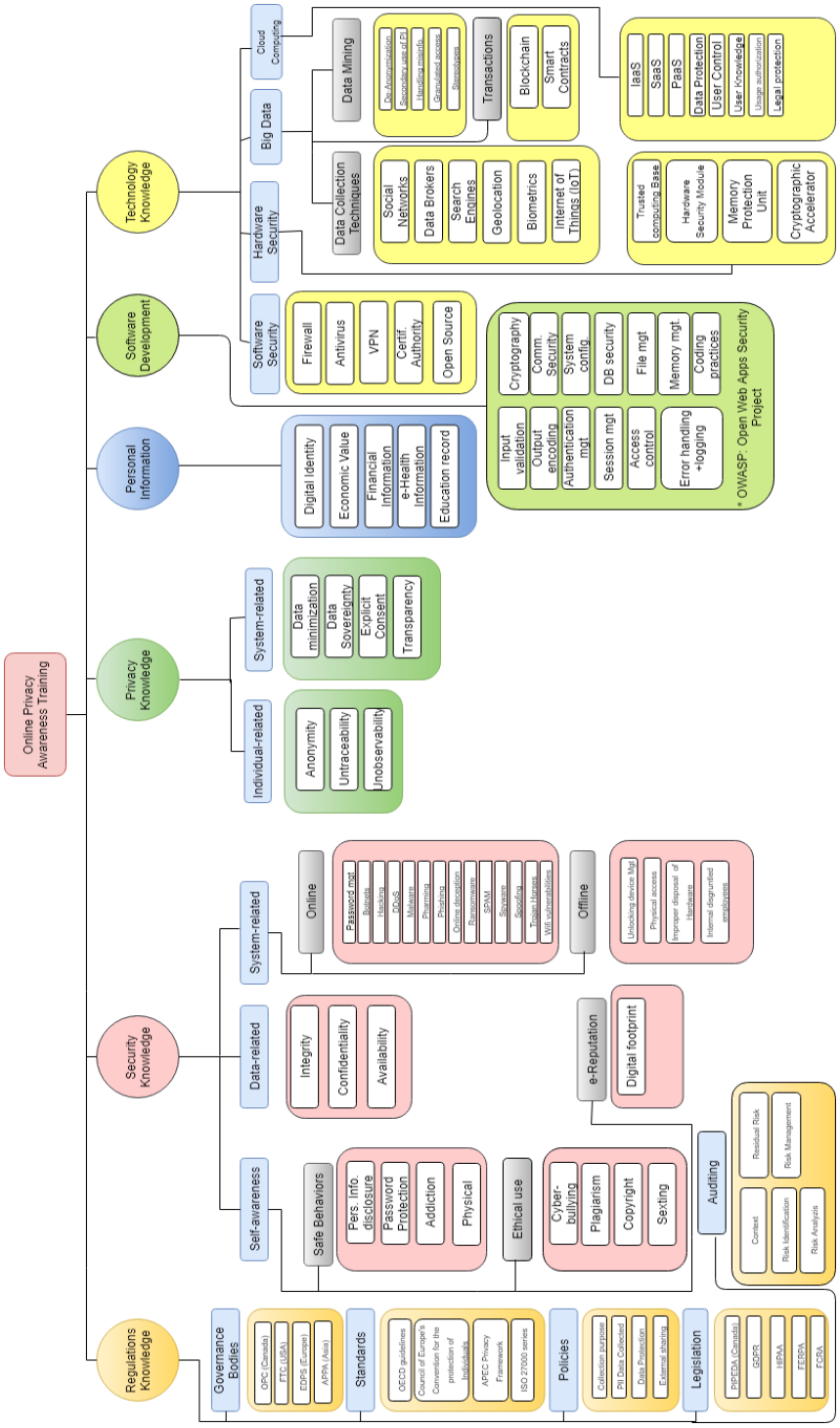


FIGURE 20 CURRICULUM COMPLET DE SENSIBILISATION À LA VIE PRIVÉE

7.3 Modèle de Base de Données de CLEOPATRA

Le système CLEOPATRA gravite autour d'une base de données relationnelles normalisée dont les tables sont représentées à la Figure 21. La présente section du document vous aidera à mieux comprendre sa structure, fournir des détails sur son contenu et visualiser les relations entre les différentes tables.

Comme nous l'avons expliqué à la section 4.2, cette structure est issue d'un concept existant et a été adaptée pour les besoins du présent projet de recherche. Ce faisant, il y a plusieurs champs des tables qui ne sont tout simplement pas utilisés et qui peuvent servir dans une version future.

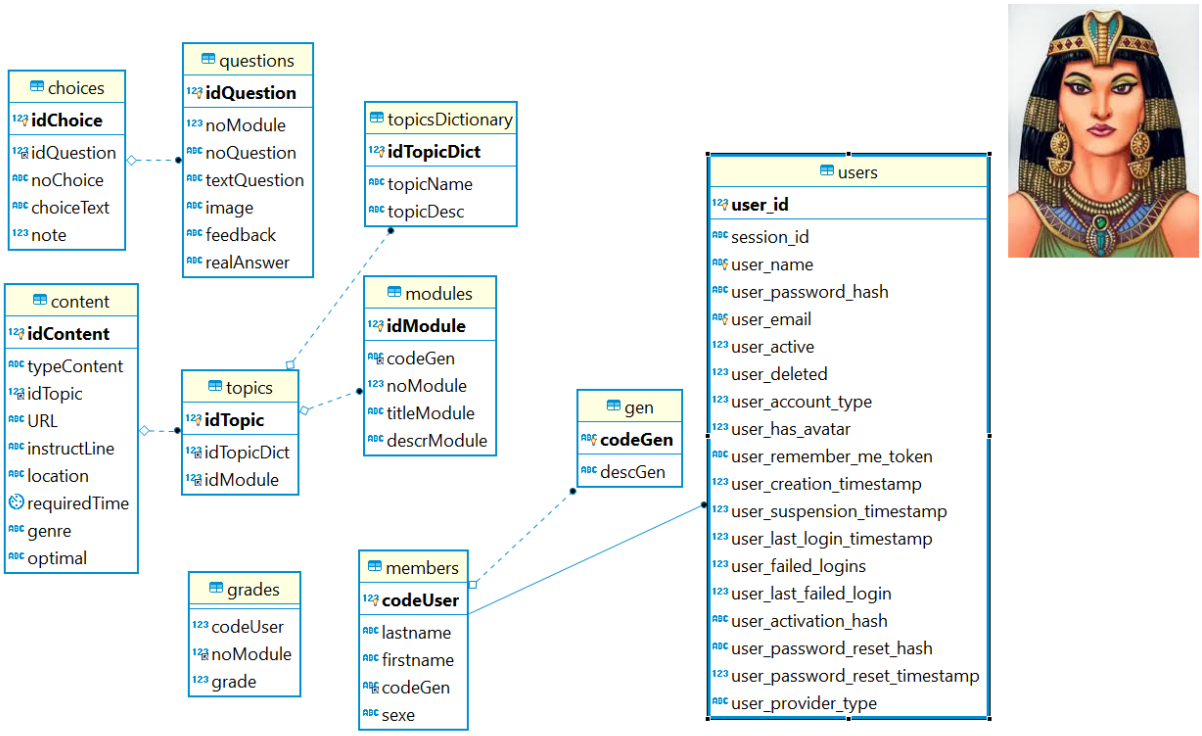
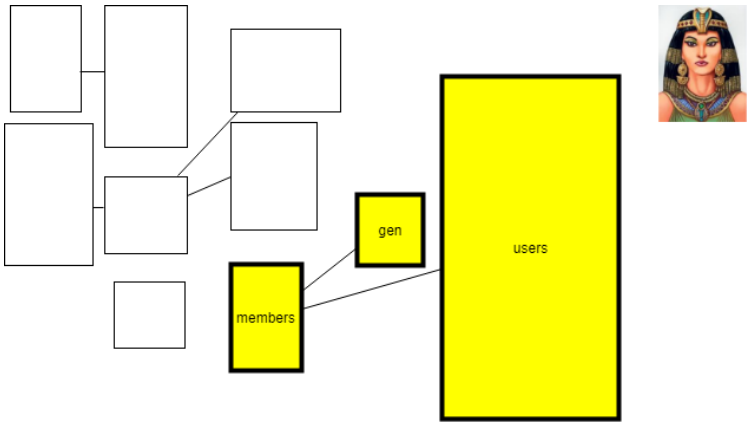


FIGURE 21 MODÈLE DE LA BD RELATIONNELLE DE CLEOPATRA

7.3.1 Tables *users – members - gen* :



La table *users* :

- Cette table détient les informations de *login* des utilisateurs du système CLEOPATRA
- On y retrouve le nom de l'utilisateur (*user_name*) et son mot de passe chiffré (*user_password_hash*).
- Le champ *user_id* est un code d'utilisateur unique qui est aussi utilisé comme clé primaire.
- Grâce au champ *user_active*, il est possible d'activer/désactiver un utilisateur.
- Lorsqu'activé, le champ *user_account_type* de cette table permet de passer en mode « administrateur » permettant d'afficher des rapports.

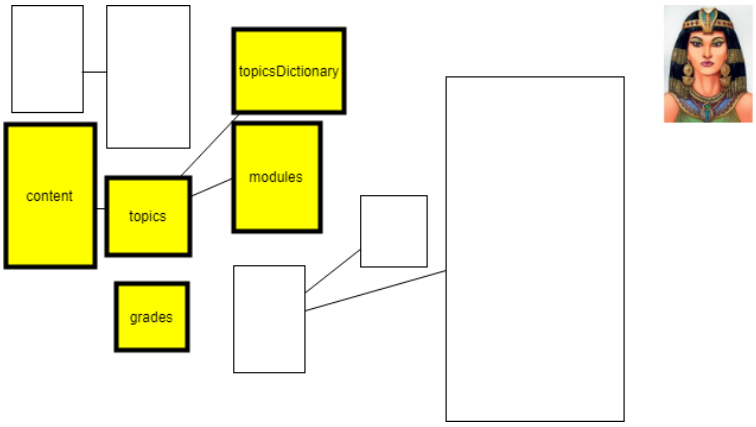
La table *members* :

- Cette table nous permet de sauvegarder le nom et prénom de l'apprenant, la génération et s'il s'agit d'un homme ou d'une femme.
- Le champ *user_id (*de la table *users*) est en relation un à un avec le champ *codeUser* de la table *members*

La table *gen* :

- Cette table désigne les générations qui sont connues de CLEOPATRA. Pour le moment nous utilisons trois générations d'adultes (baby-boomers, génération X et milléniaux)
- Chaque apprenant de la table *members* se voit assigner une génération (*codeGen*) qui lui permettra d'accéder éventuellement à un contenu de formation qui lui est adapté.

7.3.2 Tables *content – topics – topicsDictionary – modules - grades* :



La table *modules* :

- Elle contient l'information sur les différents modules de formation (domaines de connaissances), en fonction des générations
- La clé primaire est attribuée au champ *idModule* unique pour une génération et pour un numéro de module donné.

La table *grades* :

- C'est le bulletin scolaire de l'étudiant : Elle contient la note attribuée pour un module donné.
- La clé primaire est composée du code de l'utilisateur (*codeUser*). Il y a donc une note pour chaque élément de la clé primaire.

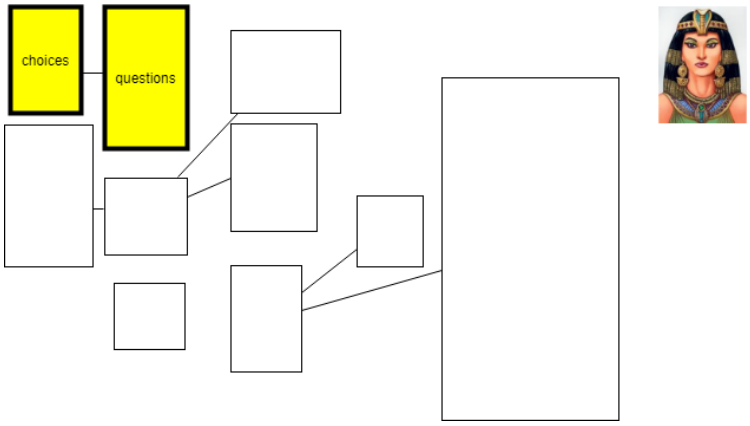
Les tables *topics* et *topicsDictionary* :

- La table topics contient les codes différents sujets contenus dans chacun des domaines de connaissances (*modules*) afin de pouvoir les rattacher à un code de ce domaine.
- La table topics se réfère à la table topicsDictionary qui lui fournit le nom et la description de chacun des sujets.

La table *content* :

- La table *content* est le cœur de cette base de données et contient les URL de chacun des sujets/module/génération.

7.3.3 Les tables *questions – choices*



- Ces deux tables sont utilisées pour la portion des quizzes, intégrés à CLEOPATRA.
- Elles sont interreliées mais fonctionnent de façon indépendante des autres tables.
- La table *question* contient le numéro et texte de la question, son image et le feedback qu'on veut donner à l'utilisateur par la suite.
- La table *choices* indique le choix de réponse fourni par l'utilisateur à la question

7.4 Courriels envoyés par CLEOPATRA

Voici les gabarits des messages envoyés à l'apprenant après qu'il ait complété le test d'évaluation. Il y a un premier message pour l'évaluation initiale à la Figure 22 (avant de suivre la formation) et un second après avoir suivi la formation et repassé le test à nouveau à la Figure 23.

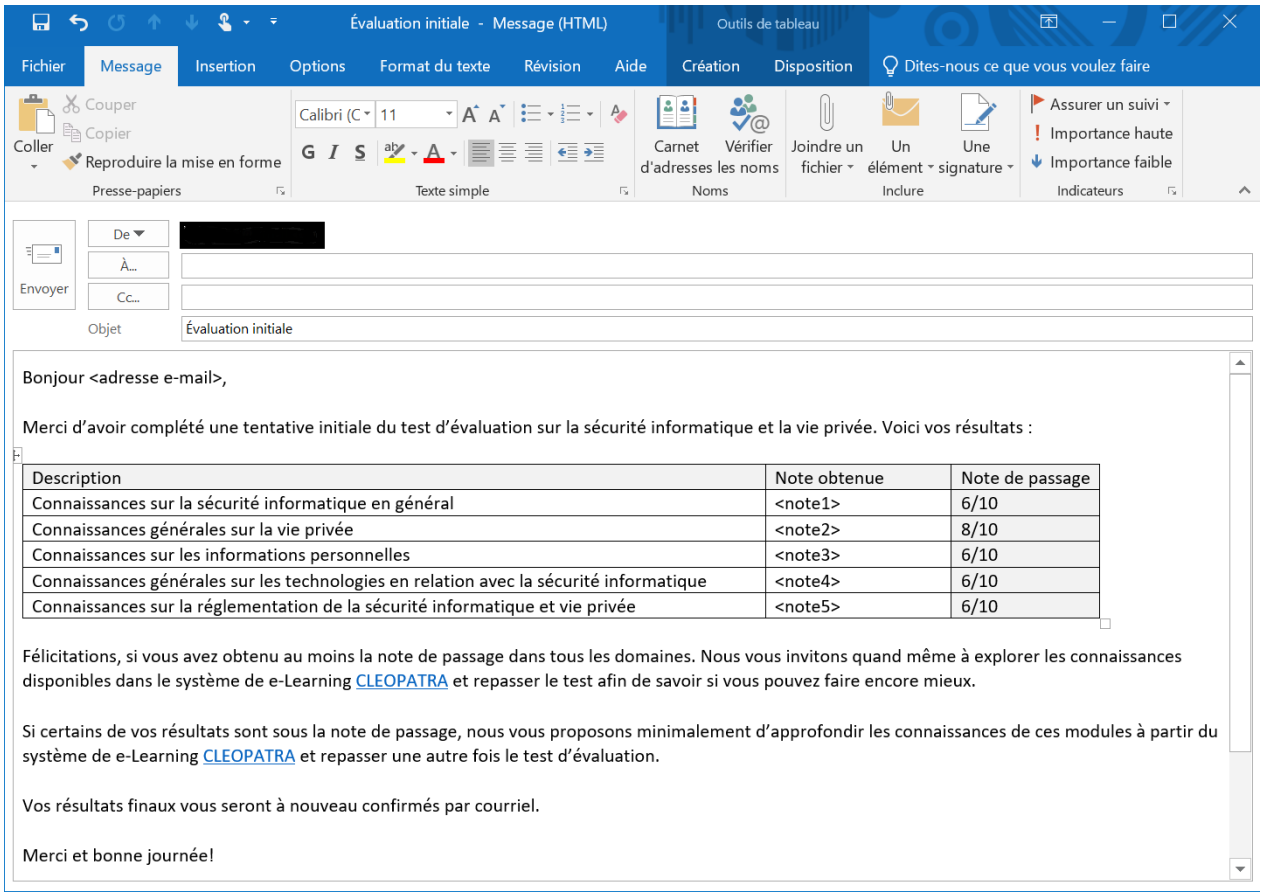


FIGURE 22 MESSAGE ENVOYÉ RÉSULTANT DU TEST D'ÉVALUATION

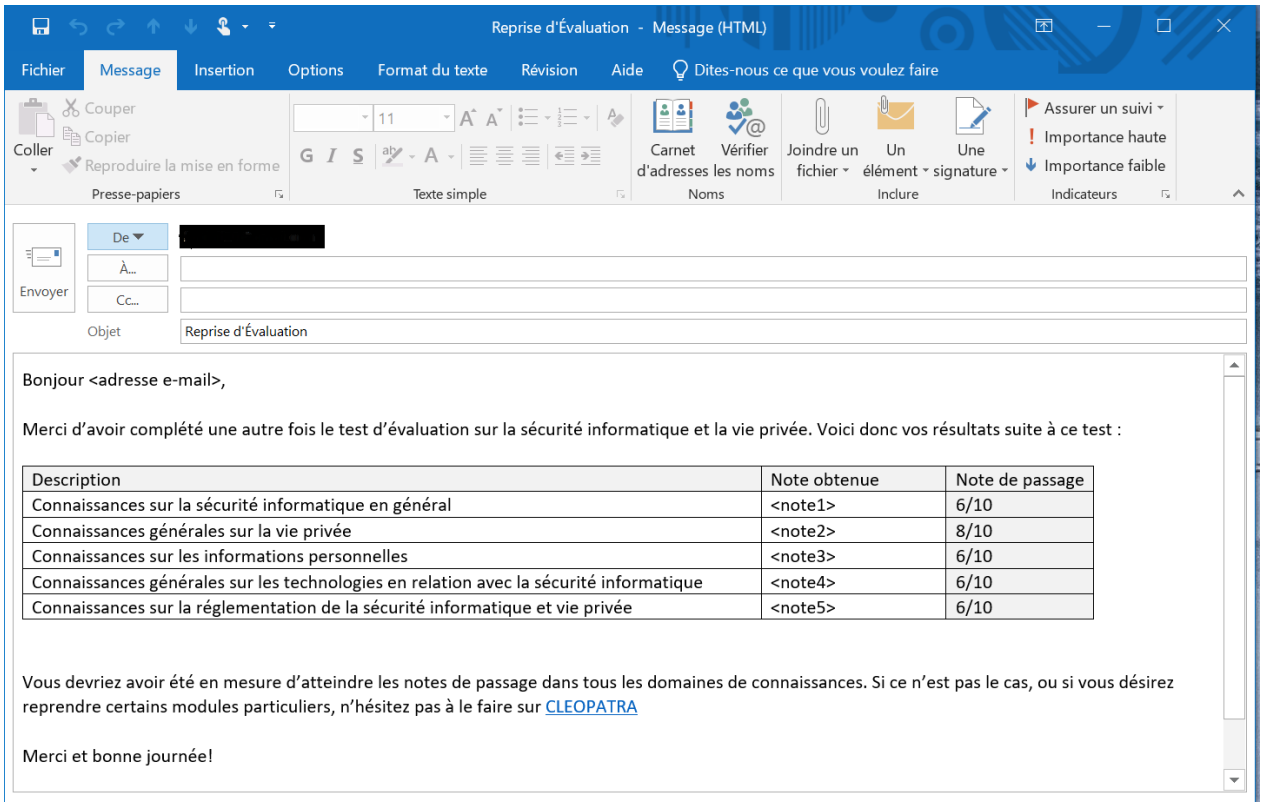


FIGURE 23 MESSAGE SUIVANT LA REPRISE DU TEST D'ÉVALUATION

7.5 Ressources sur les événements marquants les générations

TABLEAU 16 RESSOURCES[152] SUR LES ÉVÉNEMENTS MARQUANTS DU TABLEAU 6

Événement	Référence informative
1954 – Début des auditions de l'affaire McCarthy	http://ici.radio-canada.ca/emissions/aujourd_hui_1_histoire/2015-2016/chronique.asp?idChronique=396688
1962 – La crise des missiles cubains.	https://www.thecanadianencyclopedia.ca/fr/article/crise-des-missiles-cubains
1963 – L'assassinat du président John Kennedy.	http://perspective.usherbrooke.ca/bilan/servlet/BMEve?codeEve=232
1964 - L'Acte des Droits Civils de 1964 est accepté.	http://www.axl.cefan.ulaval.ca/amnord/USA-Civil_Rights_Act-1964.htm

[152] Tous les liens du Tableau 16 étaient fonctionnels au 2019-01-24

Événement	Référence informative
1965 – Les États-Unis envoient des troupes au Vietnam.	https://www.kartable.fr/ressources/histoire/etude-de-cas/la-guerre-du-vietnam-1965-1975/5900
1968 - Martin Luther King est assassiné.	https://www.la-croix.com/Debats/Ce-jour-la/4-avril-1968-lassassinat-Martin-Luther-King-Memphis-2018-04-04-1200928935
1968 - Robert Kennedy est assassiné.	http://www.lefigaro.fr/histoire/archives/2018/06/04/26010-20180604ARTFIG00269-5-juin-1968-robert-kennedy-est-assassine.php
1970 – Fusillade à l'Université Kent State.	http://internationalnews.over-blog.com/article-anniversaire-du-massacre-d-etudiants-par-la-police-de-nixon-sur-le-campus-de-kent-state-ohio-shooti-123808242.html
1970 – La crise d'Octobre 1970 (Canada): kidnappings politiques, Ottawa suspend les droits civils.	https://ici.radio-canada.ca/nouvelle/490462/octobre-1970-loi
1972 – Le scandale du Watergate	http://www.lefigaro.fr/international/2014/08/11/01003-20140811ARTFIG00244-il-y-a-40-ans-la-demission-fracassante-de-nixon-balaye-par-le-watergate.php
1972 - Le Terrorisme aux jeux olympiques de Munich.	http://www.lefigaro.fr/histoire/archives/2017/09/04/26010-20170904ARTFIG00226-il-y-a-45-ans-la-sanglante-prise-d-otages-au-jo-de-munich.php
1978 – Le suicide collectif de Jonestown	http://perspective.usherbrooke.ca/bilan/servlet/BMEve?codeEve=749
1979 - Effondrement de la centrale de Three Mile Island	https://sites.ina.fr/inalab-2018/focus/chapitre/4
1979 - La crise des otages iraniens	https://www.lesclesdumoyenorient.com/Crise-des-otages-americains-en.html
1980 – Le referendum du Québec sur la "souveraineté-Association" est perdu 60% contre, 40% pour.	https://www.thecanadianencyclopedia.ca/fr/article/referendum-du-quebec-1980
1982 – Le rapatriement de la Constitution Canadienne, accompagné de la Charte des Droits et Libertés.	https://www.thecanadianencyclopedia.ca/fr/article/canadianisation-de-la-constitution
1986 - Explosion de la navette spatiale Challenger.	http://www.lefigaro.fr/histoire/archives/2016/01/27/26010-20160127ARTFIG00357-la-

Événement	Référence informative
	navette-challenger-se-desintegre-devant-des-millions-de-telespectateurs-en-1986.php
1988 - Bombardement du vol de Lockerbie	http://www.crashdehabsheim.net/autre%20crash%20lockerbie.htm
1987 – La chute de la bourse	https://www.lapresse.ca/affaires/marches/201710/19/01-5140526-krach-boursier-doctobre-1987-le-jour-le-plus-long-en-bourse.php
1992 – L'Accord de Charlottetown (Canada) est rejeté par voie de referendum national.	https://www.thecanadianencyclopedia.ca/fr/article/accord-de-charlottetown
1995 - Le bombardement d'Oklahoma City	https://ici.radio-canada.ca/nouvelle/457256/rdi-15-oklahoma-city
1995 - Le referendum du Québec sur la souveraineté est perdu de justesse	http://plus.lapresse.ca/screens/124b8c23-a050-47b3-82ec-0b71a0090c24__7C___0.html

Bibliographie

[Al-Nakhal et Abu Naser, 2017] - Mohammed A. Al-Nakhal & Samy S. Abu Naser, (2017). **Adaptive Intelligent Tutoring System for learning Computer Theory.** *EUROPEAN ACADEMIC RESEARCH* 4 (10) pp 8770-8782

[Arias *et al*., 2015] O. Arias, J. Wurm, K. Hoang and Y. Jin, "**Privacy and Security in Internet of Things and Wearable Devices,**" in *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99-109, 1 April-June 2015. doi: 10.1109/TMSCS.2015.2498605

[Atwell, 2007] – Graham Atwell G. (2007), **"Personal Learning Environments - the future of eLearning ?",** *ELearning Papers*, *2*(January), 1–8. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.3011&rep=rep1&type=pdf consulté le 2018-10-30

[Barnes, 2003] - SHARON JAY BUTLER BARNES. (2003). **An examination of multi-generational work values of selected Texas A&M University employees.** Unpublished doctoral dissertation, Texas A&M University, College Station. https://search.proquest.com/docview/305269046?pq-origsite=primo consulté le 2018-10-30

[Brüseke, 2016] - Liana Brüseke, **"The influence of privacy perceptions on online shopping behavior – a comparison between millennials and baby boomers",** 7 th IBA Bachelor Thesis Conference, July 1st, 2016, Enschede, The Netherlands. https://essay.utwente.nl/70179/1/Brueseke_BA_BMS.pdf

[Blaschke, 2012] – Lisa Marie Blaschke, **"Heutagogy and Lifelong Learning: A Review of Heutagogical Practice and Self-Determined Learning",** Oldenburg University and University of Maryland University College (UMUC), http://www.irrodl.org/index.php/irrodl/article/view/1076/2087 (accédé le 2019-01-26)

[Caviglione et Coccoli, 2011] - L. Caviglione and M. Coccoli. (2011) **"Privacy problems with web 2.0. Computer Fraud & Security"**, 2011(10):16 – 19, 2011.

[Cavoukian et Dixon, 2013] - Ann Cavoukian, Mark Dixon, " **Privacy and Security by Design: An Enterprise Architecture Approach**", Information and Privacy Commissioner Ontario, Canada, Septembre 2013, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf (accédé le 2019-01-13)

[Cellary, 2013] - Wojciech Cellary, **"Smart Governance for Smart Industries"** ICEGOV '13 Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance, pages 91-93, 2013, doi: 10.1145/2591888.2591903

[Ching et Singh, 2016] - Ke Wan Ching and Manmeet Mahinderjit Singh, **"WEARABLE TECHNOLOGY DEVICES SECURITY AND PRIVACY VULNERABILITY ANALYSIS"**, International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.3, May 2016, pp. 19-30, 2016.

[Coffield *et al.*, 2004] - Frank Coffield, David Moseley, Elaine Hall, & Kathryn Ecclestone (2004). **Learning styles and pedagogy in post-16 learning: A systematic and critical review.** Learning and Skills Research Centre. Retrieved from http://www.leerbeleving.nl/wp-content/uploads/2011/09/learning-styles.pdf

[Coughlin, 2011] - Joseph F. Coughlin, **Baby Boomers & Technology: Possibilities, Privacy & Promise** https://bigthink.com/disruptive-demographics/baby-boomers-technology-possibilities-privacy-promise consulté le 2018-10-30

[Deshmukh et Devadkar, 2015] - Rashmi V. Deshmukha, Kailas K. Devadkar, **"Understanding DDoS Attack & Its Effect In Cloud Environment"**, Procedia Computer Science 49 (2015), doi: 10.1016/j.procs.2015.04.245 pp. 202 – 210

[Dimock, 2018] - Michael Dimock, (2018), **"Defining generations: Where Millennials end and post-Millennials begin",** Pew Research Center, Mars 2018 http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/ accédé le 2018-10-01

[Emerson et Berge, 2018] - Lynn C. Emerson, Zane L. Berge (2018). **Microlearning: Knowledge management applications and competency-based training in the workplace.** *Knowledge Management & E-Learning, 10*(2), 125–132.

[Eyerman et Turner, 1998] - Ron Eyerman & Bryan S. Turner (1998). **Outline of a theory of generations.** European Journal of Social Theory, 1, 91-106.

[Felton et Dooley, 2009] - Summer R. Felton, Larry M. Dooley (2009), **Training the different generations: the differences in training and development strategies among generations,** UFHRD https://www.ufhrd.co.uk/wordpress/wp-content/uploads/2009/07/5-21-refereed-paper.pdf (consulté le 2018-08-08)

[Giusto *et al.*, 2010] - D. Giusto, A. Iera, G. Morabito, L. Atzori(Eds.), **The Internet of Things**, Springer(2010) ISBN: 978-1-4419-1673-0

[Guay et Gaudreau, 2018] – Jean-Herman Guay, Serge Gaudreau (2018), « Bilan du Siècle : Site encyclopédique sur l'histoire du Québec depuis 1900 », http://bilan.usherbrooke.ca/bilan/ (accédé le 2019-01-17

[Hase et Kenyon, 2001] - Stewart Hase and Chris Kenyon (2001), **"From Andragogy to Heutagogy",** Southern Cross University, Original URL: http://pandora.nla.gov.au/nph-wb/20010220130000/http://ultibase.rmit.edu.au/Articles/dec00/hase2.htm , consulté le 2018-09-20

[Hassan *et al.*, 2017] - Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, Mohammed Atiquzzaman, **"Security threats in Bluetooth technology",** ScienceDirect computers & security 74 (2017) pp. 308–322 https://doi.org/10.1016/j.cose.2017.03.008

[Herder, 2016] - Herder, Eelco (2016), **« User modeling and Personalization"**, L3S Research Center, Leibniz University of Hanover. https://www.eelcoherder.com/images/teaching/usermodeling/03_user_modeling_techniques.pdf, consulté le 2018-09-27

[Hilts *et al.*, 2016] - Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, **"Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security".** Open Effect Report (2016). Available at: https://openeffect.ca/reports/Every_Step_You_Fake.pdf accédé le 2018-05-22

[Horrow et Sardana, 2012] - S. Horrow and A. Sardana (2012). **"Identity management framework for cloud based internet of things".** In Proceedings of the First International Conference on Security of Internet of Things, SecurIT '12, pages 200–203, New York, NY, USA, 2012. ACM.

[Hur et Im, 2013] - Mann Hyung Hur and Yeonwook Im, **"The Influence of E-Learning on Individual and Collective Empowerment in the Public Sector: An Empirical Study of Korean Government Employees"**, The International Review of Research in Open and Distributed Learning (2013), http://www.irrodl.org/index.php/irrodl/article/view/1498/2628 accédé le 2018-11-08

[Jebari, 2016] - Chaker Jebari (2016), **"A Segment-based Weighting Technique for URL-based Genre Classification of Web Pages",** Polibits, 01/31/2016, Vol.53, pp.43-48, doi: http://dx.doi.org/10.17562/PB-53-4

[Jiang *et al.*, 2015] H. Jiang, X. Chen, S. Zhang, X. Zhang, W. Kong and T. Zhang, "**Software for Wearable Devices: Challenges and Opportunities,**" *2015 IEEE 39th Annual Computer Software and Applications Conference*, Taichung, 2015, pp. 592-597. doi: 10.1109/COMPSAC.2015.269
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7273430&isnumber=7273299

[Jindal, 2018] – Aparna Jindal (2018), **"Ranking Criteria Classification for E-Learning Website Selection and Evaluation"**, BMIET Journal of Science, Technology and Management Vol. 2, Issue 1, June 2018, pp 20-26

[Kalbach, 2007] - Kalbach James (2007) **"Designing Web Navigation",** O'Reilly media, ISBN: 9780596528102, https://www.oreilly.com/library/view/designing-web-navigation/9780596528102/ch04s02.html**,** accédé le 2018-09-24

[Kamišalić *et al*, 2018] - Kamišalić, Aida; Fister, Iztok; Turkanović, Muhamed; Karakatič, Sašo. 2018. "Sensors and Functionalities of Non-Invasive Wrist-Wearable Devices: A Review." *Sensors* 18, no. 6: 1714.

[Karakaya *et al.*, 2016] - Murat Karakaya, Atila Bostan, Erhan Gökçay, **"How Secure is Your Smart Watch?",** INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE*,Vol. 5, No. 4,* pp 90-95, 2016. http://www.ijiss.org/ijiss/index.php/ijiss/article/view/222
[Kearsley, 2010] - Kearsley, G. (2010). Andragogy (M.Knowles). **The theory Into practice database.** https://elearningindustry.com/the-adult-learning-theory-andragogy-of-malcolm-knowles consulté le 2018-09-25

[Keefe, 1979] - Keefe, JamesW. (1979) **"Learning style: An overview."** NASSP's *Student learning styles: Diagnosing and proscribing programs* (pp. 1-17). Reston, VA. National Association of Secondary School Principles.

[Kennedy et Hunt, 2008] - Todd Kennedy, Ray Hunt, **"A Review of WPAN Security: Attacks and Prevention"**, Proceeding Mobility '08 Proceedings of the International Conference on Mobile Technology, Applications and Systems Article no. 56, 2008.

[Knight, 2016] - Knight Michaelle H. (2016) **"Generational Learning Style Preferences Based on Computer-Based Healthcare Training"**, *Brandman University*, Irvine California.

[Kokolakis, 2017] - Spyros Kokolakis, **Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon**, Computers & Security, Volume 64, 2017, Pages 122-134, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2015.07.002

[Kompara et Hölbl, 2017] - Marko Kompara, Marko Hölbl, "**Survey on security in intra-body area network communication",** Ad Hoc Networks 70 (2018) pp 23–43, https://www.sciencedirect.com/science/article/pii/S1570870517302068 accédé le 2019-01-15

[Kriegel, 2013] - Jessica Kriegel (2013), "**Differences in Learning Preferences by Generational Cohort: Implications for Instructional Design in Corporate Web-based Learning"**, Drexel University

[Lee *et al.*, 2017] - Youngjoo Lee, WonSeok Yang, Taekyoung Kwon **"POSTER: Watch out your smart watch when paired"**, Proceedings of the ACM Conference on Computer and Communications Security, 30 October 2017, pp.2527-2529, 2017.

[Lee *et al.*, 2018] - Youngjoo Lee, WonSeok Yang, Taekyoung Kwon **"Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things"**, IEEE Access Vol. 6, Juin 2018, pp.48994, 49006.

[Lee et Kim, 2010] - G. M. Lee and J. yun Kim. (2010) **"The internet of things - a problem statement. In Information and Communication"**, Technology Convergence (ICTC), 2010 International Conference on, pages 517–518, Nov 2010

[Liu et Sun, 2016] - Jiajia Liu, Wen Sun, **"Smart attacks against intelligent wearables in people-centric Internet-of-Things"**, IEEE Communications Magazine December 2016 pp. 44-49, 2016

[Longenecker, 2012] - Beth A. Longenecker (2012), **Teaching Across Generations: Understanding and Motivating Different Generations,** Baker College Effective Teaching and Learning Department, http://www.aacom.org/docs/default-source/2016-Annual-Conference/teaching_across_generations.pdf?sfvrsn=2 (consulté le 2018-08-08)

[Lubarsky, 2017] – Boris Lubarsky, **"RE-IDENTIFICATION OF "ANONYMIZED DATA"** " **,** 1 GEO. L. TECH. REV. 202 (2017), https://perma.cc/86RR-JUFT accédé le 2018-05-22

[Madakam *et al.*, 2015] - Somayya Madakam, R. Ramaswamy, Siddharth Tripathi (2015) **Internet of Things (IoT): A Literature Review Journal of Computer and Communications**, 2015, 3, 164-173 Published Online May 2015 in SciRes. http://www.scirp.org/journal/jcc http://dx.doi.org/10.4236/jcc.2015.35021

[Mishra, 2015] - **Mishra Sanjay M., "Wearable Android™: Android Wear & Google Fit App Development"**, Wiley, ISBN 978-1-119-05110-7, 2015

[Montgomery *et al.*, 2016] - Montgomery Kathryn C., Chester Jeff, Kopp Katharina, **"Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection**", Center for Digital Democracy, School of Communication, American University, Washington DC, 2016

[Muttik, 2016] - Igor Muttik (2016) "**Crowd-sourced analysis of end user license agreements"**, United States Patent Application Pub. No.: US 2016/0284.035 A1, Sep. 29, 2016 https://patents.google.com/patent/US20160284035A1/en (accédé le 2019-01-13)

[Nkambou *et al.*, 2010] - Roger Nkambou, Jacqueline Bourdeau, Riichiro Mizoguchi (2010), **« Advances in Intelligent Tutoring Systems »**, Springer, https://link.springer.com/content/pdf/10.1007%2F978-3-642-14363-2.pdf consulté le 2018-09-27

[O'Neill, 2010] - Dr. Michael O'Neill, **Generational Preferences: A Glimpse into the Future Office,** disponible à: https://www2.usgs.gov/humancapital/ecd/mentoringreadinglist/WP_GenerationalDifferences.pdf consulté le 2018-10-30

[Oussous *et al.*, 2018] - Ahmed Oussous, Fatima-Zahra Benjelloun, Ayoub Ait Lahcen, Samir Belfkih, **Big Data technologies: A survey**, Journal of King Saud University - Computer and Information Sciences, Volume 30, Issue 4, 2018, Pages 431-448, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2017.06.001.

[Pappas, 2013] - Pappas, Christopher (Mai 2013), **"The Adult Learning Theory - Andragogy - of Malcolm Knowles**", disponible ici: https://elearningindustry.com/the-adult-learning-theory-andragogy-of-malcolm-knowles, consulté le 2018-09-20

[Perez et Zeadally, 2018] - A. J. Perez and S. Zeadally, **"Privacy Issues and Solutions for Consumer Wearables,"** in *IT Professional*, vol. 20, no. 4, pp. 46-56, Jul./Aug. 2018. doi: 10.1109/MITP.2017.265105905

[Phobun et Vicheanpanya, 2010] - Phobun Pipatsarun, Vicheanpanya Jiracha (2010), **Adaptive intelligent tutoring systems for e-learning systems**, Procedia Social and Behavioral Sciences 2 pp 4064–4069 (2010)

[Pilcher, 1994] - Pilcher, Jane (September 1994). **"Mannheim's Sociology of Generations: An undervalued legacy"** (PDF). *British Journal of Sociology*. 45 (3): 481–495. doi:10.2307/591659. JSTOR 591659.

[Pritsos et Stamatatos, 2013] Dimitrios A. Pritsos and Efstathios Stamatatos University of the Aegean **Open-Set Classification for Automated Genre Identification**, ECIR 2013, LNCS 7814, pp. 207–217. Springer-Verlag Berlin Heidelberg 2013

[Qiu *et al.*, 2017] - Qiu Hao, Wang Xianping, Xie Fei, **"A Survey on Smart Wearables in the Application of Fitness", IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing,** 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 303-307, 2017. Doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.64

[Reeves, 2007] - Reeves, Thomas C., (2007) « **Do generational difference matter in instructional design?"**, Department of Educational Psychology and Instructional Technology, University of Georgia

[Rustad, 2001] - M. L. Rustad. (2001) **"Private enforcement of cybercrime on the electronic frontier",** Southern California Interdisciplinary Law Journal [Vol. 11:63]

[Sá *et al.*, 2015] - Lucas Camelo Sá, Amy Greene, James Loving, Ulziibayar Otgonbaatar, **"The internet of insecure things",** MIT 6.857 Final Paper, 2015. https://courses.csail.mit.edu/6.857/2015/files/camelosa-greene-loving-otgonbaatar.pdf accédé le 2018-05-26

[Sartor, 2006] - Sartor G. (2006) **Privacy, Reputation, and Trust: Some Implications for Data Protection**. In: Stølen K., Winsborough W.H., Martinelli F., Massacci F. (eds) Trust Management. iTrust 2006. Lecture Notes in Computer Science, vol 3986. Springer, Berlin, Heidelberg DOI **:** https://doi.org/10.1007/11755593_2

[Shepherd, 2017] - Jennifer Shepherd (2017), **A CAUSAL-COMPARATIVE STUDY OF GENERATIONAL DIFFERENCES IN LEARNING STYLE PREFERENCES AMONG ADULT LEARNERS IN THE UNITED STATES**, LaFetra College of Education, Organizational Leadership Department

[Schewe et Noble, 2000] - Charles D. Schewe et Stephanie M. Noble (2000). **Market segmentation by cohorts: the value and validity of cohorts in American and abroad.** Journal of Marketing Management, 16, 129- 142.

[Shrestha et Saxena, 2017] - PRAKASH SHRESTHA and NITESH SAXENA**, "An Offensive and Defensive Exposition of Wearable Computing",** *ACM Comput. Surv.* 50, 6, Article 92 (November 2017), 39 pages. https://doi.org/10.1145/3133837

[Stewart and Felicetti, 1992] - Stewart, Karen L.; Felicetti, Linda A. (1992). **Learning styles of marketing majors**. *Educational Research Quarterly,* 15(2), 15-23.

[Strauss et Howe, 1991] - William Strauss et Neil Howe (1991). **Generations: the history of America's future,** 1584- 2069. New York: William Morrow & Co.

[Strauss et Howe, 1997] - William Strauss et Neil Howe (1997). **The fourth turning.** New York, Broadway Books.

[Talebi *et al*, 2016] - Nasim Talebi, Cory Hallam, Gianluca Zanella**. "The New Wave of Privacy Concern in the Wearable Devices Era",** Proceedings of PICMET'16: Technology Management for Social Innovation, pp. 3208-3214, 2016.

[Tanner1, Mai 2018] - Robert Tanner, **15 Influential Events that Shaped Generation Y**, 12 mai 2018, https://managementisajourney.com/15-influential-events-that-shaped-generation-y-infographic/ consulté le 2018-10-30

[Tanner2, Mai 2018] - Robert Tanner, **15 Influential Events that Shaped Baby Boomers** https://managementisajourney.com/fascinating-numbers-15-influential-events-that-shaped-baby-boomers/

[Tanner, Juillet 2018] - Robert Tanner, **15 Influential Events that Shaped Generation X** https://managementisajourney.com/fascinating-numbers-15-influential-events-that-shaped-generation-x/

[Tripathy and Anuradha, 2017] – Tripathy BK and Anuradha J. **"Internet of Things (IoT): Technologies, Applications, Challenges and Solutions",** CRC Press Taylor & Francis Group, 2017.

[Twenge et Campbell, 2008] - Twenge, Jean M., & Campbell, Stacy M. (2008). **Generational differences in psychological traits and their impact on the workplace**. *Journal of Managerial Psychology, 23*, 862-877. doi:10.1108/02683940810904367

[Vasundhara, 2017] – Dr. S. Vasundhara (2017), "**Elliptic curve Cryptography and Diffie-Hellman Key exchange**", IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 13, Issue 1 Ver. I (Jan. - Feb. 2017), PP 56-61, DOI: 10.9790/5728-1301015661, http://www.iosrjournals.org/iosr-jm/papers/Vol13-issue1/Version-1/K1301015661.pdf accédé le 2018-12-19

[Vidalis et Angelopoulou, 2014] - Stilianos Vidalis et Olga Angelopoulou (2014). **"Assessing Identity Theft in the Internet of Things"**. IT Convergence Practice (INPRA). Volume 2, Number 1. p 15-21.

[Vidulin *et al.*, 2007] - Vedrana Vidulin, Mitja Lustrek, Matjaz Gams. **"Training a Genre Classifier for Automatic Classification of Web Pages",** Journal of Computing and Information Technology - CIT 15, 2007, 4, pp 305–311 doi:10.2498/cit.1001137

[Vijayaraghavan et Agarwal, 2018] - V. Vijayaraghavan, Rishav Agarwal ,**"Connected Environments for the Internet of Things",** Springer International Publishing, , Chap 2 Security and Privacy Across Connected Environments pp 19-39, 2018 https://doi.org/10.1007/978-3-319-70102-8_2

[Willingham *et al.*, 2015] - Daniel T. Willingham, Elizabeth M. Hughes, and David G. Dobolyi **"The Scientific Status of Learning Styles Theories »** Society for the Teaching of Psychology Teaching of Psychology 2015, Vol. 42(3) 266-271 (2015) doi: 10.1177/0098628315589505

[Yeoh, 2017] - Peter Yeoh **"The Fourth Industrial Revolution : Technological Impact and Privacy and Data Security Issues"**, 38 Business Law Review, Issue 1, pages 9-13, 2017

[Yu-li et Yuntsai, 2018] - Yu-li Liu, Yuntsai Jessica Chou, **Big data, the Internet of things, and the interconnected society,** Telecommunications Policy, Volume 42, Issue 4, 2018, Pages 277-281, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2018.03.014.

[Zafari *et al.*, 2016] - Faheem Zafari, Ioannis Papapanagiotou, Konstantinos Christidis, **"Microlocation for Internet-of-Things-Equipped Smart Buildings",** IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 1, pp. 96-112, FEBRUARY 2016.

[Zemke *et al.*, 2000] - Ron Zemke, Claire Raines, Bob Filipczak (2000). **« Generations at work: Managing the clash of veterans, boomers, Xers, and nexters in your workplace".** Washington, DC: American Management Association, 2000

[Ziegeldorf *et al.*, 2015] - Jan Henrik Ziegeldorf1, Oscar Garcia Morchon, and Klaus Wehrle, **"Privacy in the Internet of Things: Threats and Challenges",** https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf (accédé le 2018-05-18), 2015.

Overview of Learning styles, learning-styles.com (2018), https://www.learning-styles-online.com/overview/ consulté le 2018-09-25

Understanding your learning style, Wilfrid Laurier University, Study Skills & Supplemental Instruction Centre (2008), disponible ici: https://web.wlu.ca/learning_resources/pdfs/Learning_Styles.pdf, consulté le 2018-09-25

Pontydysgu, http://www.pontydysgu.org/pontydysgu-and-people/graham-attwell, **consulté le 2018-09-30**

Adult Learning Theory (Andragogy), **"An overview of the Adult Learning Theory and definition of Andragogy",** Northern Arizona University, disponible ici: https://sites.google.com/a/nau.edu/educationallearningtheories/adult-learning-theory-andragogy-by-barbara-miroballi, consulté le 2018-09-20