

Louvain School of Management

L'éducation à la citoyenneté numérique comme solution pour conscientiser les utilisateurs européens à la protection de leurs données personnelles

Auteure : Jacques Justine
Promoteur : Paque Bernard
Année académique 2021-2022
Mémoire en vue d'obtenir le titre de
Master [120] en sciences de gestion, à finalité spécialisée

Je tiens tout d'abord à remercier mon promoteur, Bernard Paque, pour son expertise, ses conseils et sa disponibilité tout au long de la rédaction de ce mémoire.

Je souhaite également remercier Madame Virginie Tyou, Monsieur Thomas Jadin et les élèves de secondaire pour m'avoir accordé de leur temps afin de répondre à mes interviews, ainsi que les personnes ayant accepté de répondre à mes questionnaires.

Enfin, je souhaite remercier ma famille et mes amis pour la relecture, leur soutien et leurs encouragements durant toutes mes années d'études et particulièrement tout au long de ce projet.

TABLE DES MATIÈRES

GLOSSAIRE	1
INTRODUCTION	3
PARTIE 1 : REVUE SCIENTIFIQUE.....	6
PARTIE 1 A : Compréhension des mécanismes et des dangers liés à la collecte des données personnelles.....	6
Chapitre 1 : Définitions.....	6
2.1. Données personnelles	6
2.2. Données sensibles	6
Chapitre 2 : les mécanismes de collecte, de stockage et de traitement de données	7
2.1. Qui détient quel type de donnée ? Les différents types de marchés	7
2.1.1. <i>Marché primaire</i>	7
2.1.2. <i>Marché secondaire</i>	8
2.1.3. <i>Marché tertiaire</i>	9
2.1.4. <i>Conclusion</i>	9
2.2. Les différents types de base de données	10
2.2.1. <i>Base de données relationnelle</i>	10
2.2.2. <i>Base de données orientée graphe</i>	10
Chapitre 3 : L'influence et les dangers des réseaux sociaux et des grandes plateformes	12
3.1. Les réseaux sociaux et la vie privée	12
3.1.1. <i>Définitions</i>	12
3.1.2. <i>Chiffres clés</i>	12
3.1.3. <i>Les réseaux sociaux et les données personnelles</i>	13
3.1.4. <i>Piratage et cybercriminalité</i>	13
3.2. Les grandes plateformes.....	15
3.2.1. <i>Caractéristiques</i>	15
3.2.2. <i>Avantages</i>	15
3.2.3. <i>Inconvénients liés à la vie privée</i>	16
PARTIE 1b : Conscientisation des utilisateurs de la collecte et du traitement de leurs données personnelles.....	19
Chapitre 1 : Perception des internautes quant à l'utilisation de leurs données personnelles	19
1.1. Inquiétude des utilisateurs.....	19
1.1.1. <i>Facteurs individuels</i>	20
1.1.2. <i>Facteurs externes</i>	21
Chapitre 2 : L'éducation à la citoyenneté numérique comme solution.....	21
2.1. Introduction	21
2.2. Education en milieu familial	23
2.3. Education en milieu scolaire	24
2.4. Actions et stratégies mises en place	25
2.4.1. <i>Better internet for kids</i>	25
2.4.2. <i>Conseil européen</i>	26
2.4.3. <i>Belgique : Autorité de protection des données</i>	27
2.4.4. <i>France : Commission Nationale de l'Informatique et des Libertés</i>	27
Conclusion de la revue scientifique.....	28
Hypothèses à tester	28
PARTIE 2 : ETUDES QUALITATIVES	29
Chapitre 1 : Méthodologie	29
1.1. Choix des personnes interviewées	29
1.2. Méthodologie et recherche.....	30
1.3. Analyse des données	31

1.4. Limites de la méthodologie	31
Chapitre 2 : Analyse des résultats.....	32
2.1. Hypothèse 1a	32
2.2. Hypothèse 1b	34
2.3. Hypothèse 2a	36
2.4. Hypothèse 2b	38
PARTIE 3 : ETUDES QUANTITATIVES.....	40
Chapitre 1 : Méthodologie	40
1.1. Conception des questionnaires.....	40
1.2. Choix des échantillons	41
1.3. Pré-tests	41
1.4. Matrices Hypothèses/ questions.....	42
1.5. Distribution des questionnaires	43
Chapitre 2 : Analyse des résultats.....	44
2.1. Préparation des données	44
2.2. Description des échantillons.....	44
2.2.1. Echantillon enseignants	44
2.2.2. Echantillon parents	46
2.3. Résultats	49
2.3.1. Hypothèse 1a.....	49
2.3.2. Hypothèse 1b.....	50
2.3.3. Hypothèse 2a.....	51
2.3.4. Hypothèse 2b.....	53
PARTIE 4 : DISCUSSION	55
4.1. Interprétation des résultats.....	55
4.2. Recommandations.....	60
CONCLUSION.....	62
BIBLIOGRAPHIE.....	64
A. Articles Scientifiques	64
B. Ouvrages de référence	70
C. Sites internet	70
D. Autres	75
ANNEXES	76

GLOSSAIRE

Agrégateur : Site Web ou logiciel qui, automatiquement et régulièrement, détecte et rassemble les mises à jour de sites prédéterminés par un internaute, et les lui adresse.

Camgirl : Femme exposant son corps sur internet de manière sexuellement explicite par le biais d'une webcam, souvent pour gagner de l'argent.

CNIL : Commission Nationale de l'Informatique et des Libertés

Cookies : Petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web)

Courtier de données : Prestataire marketing spécialisé dans l'achat et la revente de données utilisées à des fins marketing

Cyberculture : Culture liée à l'informatique et à internet

Cybercriminalité : Ensemble des infractions pénales qui sont commises dans le cyberspace

Cyberharcèlement : Acte agressif, intentionnel perpétré par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée à l'encontre d'une victime qui ne peut facilement se défendre seule

Cyber-obscénité : Désigne tout ce qui est à caractère obscène dans le cyberspace (paroles, images,...)

Cyberspace : Désigne le monde virtuel, dans lequel on se plonge lorsqu'on touche à un réseau informatique et surtout, Internet, le réseau des réseaux

Donnée agrégée : Données constituées à partir d'un fichier de microdonnées et qui sont le résultat d'une combinaison de différentes mesures

INSEE : Institut National de la Statistique et des Etudes Economiques

Hacking : Consiste en l'accès non autorisé à un système informatique. Cette pratique désigne le fait de s'introduire dans le système informatique de quelqu'un à son insu.

Langage de requête structurée (SQL) : « Structured Query Language », est un langage de « programmation » standardisé qui est utilisé pour gérer des bases de données relationnelles et effectuer diverses opérations sur les données qu'elles contiennent

NoSQL : « Not Only SQL », est une approche de la conception de bases de données qui peut s'adapter à une grande variété de modèles de données, y compris les formats avec des clés, des documents, des colonnes et des graphiques

Phreaking : Action de pirater les réseaux téléphoniques

RGPD : Règlement Général de la Protection des Données

Utilisateur : Personne qui utilise les grandes plateformes, les sites internet ou encore les objets connectés

INTRODUCTION

A l'ère du numérique, l'utilisation d'internet et des technologies ne cesse de croître. En 2021, selon le Digital Report de We Are Social, 4,66 milliards de personnes utilisent internet et 4,2 milliards sont sur les médias sociaux. Depuis 2020, l'augmentation des utilisateurs des médias sociaux a augmenté de 13%. En moyenne, 1,3 millions d'utilisateurs ont rejoint les médias sociaux en 2020 soit 15,5 nouveaux utilisateurs par seconde au cours de cette année-là. Le nombre d'objets connectés, c'est-à-dire des appareils physiques connectés à internet et capables de communiquer entre eux (Balagué 2021) a également explosé ces dernières années. L'entreprise américaine de conseil Gartner a prédit qu'il existerait, à la fin de l'année 2021, 25 milliards d'objets connectés.

Ces objets connectés, les plateformes ou encore les sites internet facilitent nos vies mais, en les employant, les utilisateurs dévoilent de plus en plus leur vie privée et leurs données personnelles.

Les données des utilisateurs étant de plus en plus nombreuses et facilement accessibles, les grandes plateformes telles que Facebook, Amazon ou encore Google les ont collectées, traitées et utilisées. Suite à ces collectes de millions de données, obtenues sans le consentement des utilisateurs, de nombreux scandales, liés à ces géants du net, ont éclaté au grand jour. Ces scandales ont fait les gros titres des médias, ce qui a alerté beaucoup d'utilisateurs (Maurel 2019). Cependant, bien que ceux-ci se soient montrés plus inquiets pour leur vie privée, la Commission Nationale de l'Informatique et des Libertés (CNIL) ayant enregistré un total de 13 585 plaintes en 2020, ils continuent à utiliser ces plateformes et ces objets connectés qui leur apportent de nombreux avantages et facilitent leur quotidien (Maurel 2019).

Suite à ces nombreux scandales ayant mis en péril les données de milliers d'utilisateurs, l'Union Européenne a mis en vigueur, le 25 mai 2018, le Règlement Général de la Protection des Données personnelles (RGPD). Ce nouveau cadre européen définit six grands principes pour assurer la protection des données des utilisateurs. Les entreprises doivent dorénavant répondre à des normes de conformité en ce qui concerne d'une part, leurs méthodes de collecte et de traitement de données personnelles et d'autre part, les conditions d'utilisation de leurs services (Hassani 2019).

Cependant, malgré la mise en place de ce règlement et les amendes salées que reçoivent les entreprises qui ne le respectent pas, les données des utilisateurs ne sont toujours pas suffisamment protégées car les géants du Net parviennent à contourner les lois ou payent les amendes pour obtenir toujours un maximum de données. Cette affirmation est confirmée par La Quadrature du Net. Une autre solution serait de conscientiser les utilisateurs et les éduquer à protéger leur données personnelles et à porter davantage d'attention à leur vie privée lorsqu'ils utilisent les technologies et les plateformes. En effet, pour le moment, les utilisateurs n'ont pas les clés pour se protéger correctement.

La littérature en matière d'éducation au numérique étant très pauvre, réaliser un travail de recherche sur cette thématique s'avère intéressant.

Dès lors, la problématique de ce mémoire recherche s'intitule « **L'éducation à la citoyenneté numérique comme solution pour conscientiser les utilisateurs européens à la protection de leurs données personnelles** ».

L'objectif de ce mémoire est ainsi de déterminer si l'éducation à la citoyenneté numérique peut aider les utilisateurs à prendre conscience de la nécessité de protéger leurs données personnelles et leur vie privée. Ce problème concernant la protection de la vie privée et des données personnelles est très actuel et touche des milliers de personnes. Pourtant, aucune réelle solution n'a jusqu'à présent été mise en œuvre pour conscientiser les gens à protéger leurs données ou pour leur expliquer la façon de les gérer.

Diverses raisons m'ont poussée à réaliser mon mémoire sur ce sujet. Tout d'abord, la problématique des données personnelles est une problématique actuelle, qui touche des millions de personnes et qui n'a pas encore de réelle solution. J'utilise quotidiennement les grandes plateformes et j'ai remarqué de nombreuses fois que mes données étaient utilisées. Malgré cela, je continue d'«accepter les cookies» et de «donner mon consentement» pour que mes données soient utilisées car je ne connais pas beaucoup d'autres alternatives où les services proposés sont meilleurs et toujours gratuits. Je ne sais pas non plus comment me protéger de cela. J'ai souhaité ainsi en apprendre davantage sur le sujet pour y trouver une solution. De plus, beaucoup de membres de ma famille travaillent dans l'enseignement et ce secteur m'a toujours plu. En discutant avec certains d'entre eux, j'ai me suis rendue compte à quel point l'école était un élément clé dans l'éducation citoyenne et l'apprentissage.

Ce mémoire se divise en plusieurs parties. La première partie comprend la recherche empirique, réalisée en utilisant la méthode de l'entonnoir. Elle comporte une section décrivant les aspects plus techniques du sujet et une section ciblant les utilisateurs (perceptions, éducation, ...). Sur base de cette théorie, quatre hypothèses ont été posées. La deuxième partie est consacrée aux enquêtes qualitatives et comprend la méthodologie pour réaliser celles-ci et l'analyse des résultats. La méthodologie et l'analyse des résultats des deux enquêtes quantitatives sont détaillées dans la troisième partie. La dernière partie comprend une discussion découlant des résultats des enquêtes qualitatives et quantitatives et de l'étude empirique réalisée plus tôt. Enfin, ce mémoire se termine par les conclusions de cette recherche ainsi que par des recommandations sur le sujet.

PARTIE 1 : REVUE SCIENTIFIQUE

PARTIE 1 A : Compréhension des mécanismes et des dangers liés à la collecte des données personnelles

Chapitre 1 : Définitions

2.1. Données personnelles

Surnommées l'or noir de l'économie numérique (Grumbach & Frénot 2013), les données personnelles sont un sujet qui a pris de l'ampleur ces dernières années, entre autres suite à l'apparition de certains scandales dans les médias.

Lorsqu'on parle de données personnelles, il est important de pouvoir différencier les différents types de données. Une donnée personnelle est « *toute information se rapportant à une personne physique identifiée ou identifiable* » (RGPD 2018). Il en existe deux sous-catégories : les données personnelles directes et indirectes. Le premier type permet d'identifier directement un individu, comme son nom ou son prénom. Les données personnelles indirectes, quant à elles, sont par exemple le numéro de téléphone, le numéro de sécurité sociale, l'adresse postale ou encore la plaque d'immatriculation. Il est important de noter que ce type de données personnelles (directes et indirectes) peut être collecté et traité tant que le procédé respecte les lois et la protection des données (CNIL).

Les données personnelles directes et indirectes peuvent également se croiser et former, à plusieurs, une énième donnée personnelle permettant d'identifier plus précisément une personne. Par exemple, une femme, née à telle date, habitant dans telle ville et roulant avec telle voiture. Lorsque ces données sont assemblées, elles créent alors un faisceau de données qui prend de plus en plus de valeur car il permet l'identification plus rapide et plus précise d'un individu (Deltorn 2017).

2.2. Données sensibles

Il existe également une catégorie spéciale dans les données personnelles, nommée « données sensibles ». Les données sensibles fournissent des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale. Ces données sensibles comprennent également les données génétiques ou biométriques, les données concernant la santé ou les données concernant

la vie sexuelle ou l'orientation sexuelle d'une personne physique (RGPD 2018). La CNIL approuve également cette définition. Les données sensibles sont des informations plus privées et pouvant avoir des effets discriminants, elles doivent donc être traitées avec plus de sécurité. Le RGPD interdit d'ailleurs le stockage et le traitement de celles-ci, sauf sous certaines conditions devant être acceptées par la CNIL. Les conditions sont, par exemple, *«le consentement explicite de la personne, la protection de la vie humaine, le traitement justifié par un intérêt public (traitement statistique réalisé par l'INSEE, défense ou exercice d'un droit en justice) »*.

Chapitre 2 : les mécanismes de collecte, de stockage et de traitement de données

2.1. Qui détient quel type de donnée ? Les différents types de marchés

Les données personnelles sont utilisées, stockées, traitées, échangées et font très souvent l'objet d'une exploitation marchande. Les internautes, qui sont à la source des données, peuvent constater les effets de cette marchandisation mais n'en comprennent pas les mécanismes. Sans cette compréhension, il leur est impossible d'intervenir activement pour stopper cet échange marchand sur lequel ils n'ont ainsi aucun pouvoir (Rallet 2008).

La marchandisation des données est un mécanisme assez complexe. Les données personnelles parcourent trois marchés distincts, détaillés ci-dessous. La nature et la valeur de celles-ci changent au cours de leur cheminement (Acquisti 2016).

Avant d'analyser les trois marchés de données, il est important de redéfinir la notion de marché en économie. Selon les économistes, le marché est *“un lieu de rencontre des vendeurs et des acheteurs de biens et de services où, de la confrontation entre l'offre et la demande, va naître le prix d'échange”*.

2.1.1. Marché primaire

Le premier marché, à la base de la pyramide, est appelé le marché primaire. Il est caractérisé par un échange de données entre des individus et des collecteurs de données. Dans une grande majorité des cas, qui concerne les internautes classiques, les individus sont les personnes qui vont échanger leurs données contre un service, généralement gratuit. Les collecteurs de données, eux, sont généralement des entreprises commerciales, des plateformes ou encore des administrations (Acquisti, 2016). Cependant, sur base de la définition ci-dessus, ce marché ne

peut pas vraiment être appelé “marché” car il n’y a ni vendeur ni acheteur, ni même de prix fixé. En effet, les individus qui utilisent ces services ne vendent pas leurs données mais donnent normalement leur consentement pour que leurs données soient utilisées. Dans la plupart des cas, les utilisateurs n’ont pas l’occasion de donner explicitement leur consentement (Rallet 2008).

L’échange cité ci-dessus est donc un échange implicite car il n’y a pas de volonté initiale de l’acheteur de payer pour cela. Cet échange “donnée contre service” apparaît très inégal si l’on compare les gains des individus et ceux des collecteurs. Ces collecteurs de données, à savoir principalement les plateformes et applications mobiles, ont entrepris ce procédé à défaut de pouvoir gagner directement de l’argent en échange du service qu’ils proposent (Rallet 2008). Cependant, les utilisateurs sont de plus en plus informés au sujet de la collecte de leurs données personnelles et les entreprises risquent de compromettre la confiance des utilisateurs en utilisant celles-ci sans leur consentement. La confiance des clients envers une entreprise étant essentielle pour la viabilité de celle-ci, les entreprises doivent se montrer prudentes quant à la collecte des données de leurs clients afin de ne pas perdre gros tant au niveau de leur image qu’au niveau économique (BCG & DLA Piper 2014).

2.1.2. Marché secondaire

Le deuxième marché, imbriqué dans le marché primaire, est nommé marché secondaire. Une fois que les collecteurs de données ont collecté les données personnelles des utilisateurs des services, ils vont les vendre à des agrégateurs, aussi appelés courtiers de données ou « data brokers ». Dans ce cas-ci, on peut réellement parler de marché car il y a un échange entre des vendeurs (les collecteurs) et des acheteurs (les agrégateurs) avec en contrepartie de l’argent. On parle ici d’économie du numérique, où les collecteurs, à défaut de pouvoir tirer un revenu direct du service offert aux utilisateurs, obtiennent un revenu indirect des agrégateurs. Le prix des données varie en fonction du type de donnée. Une adresse électronique a, par exemple, moins de valeur qu’un historique de crédit (Rallet 2008).

Les vendeurs ont des droits exclusifs sur les données qu’ils ont collectées mais peuvent les transmettre à d’autres grâce à une licence. Celle-ci comprend les droits d’accès et d’utilisation des données. Il est important de noter également que dans ce marché secondaire, il y a énormément d’échanges entre courtiers. Ceux-ci échangent bien entendu avec les collecteurs sur le marché primaire mais la grande majorité des échanges se fait entre agrégateurs du marché secondaire (Rallet 2008).

Enfin, la plupart des collecteurs de données, des applications mobiles ou des plateformes par exemple, cèdent leurs données pour engendrer des revenus mais s'en servent aussi dans le but d'améliorer l'efficacité de leur service.

2.1.3. Marché tertiaire

Le dernier marché, le marché tertiaire, est caractérisé par un échange entre les agrégateurs et les entreprises. En effet, les agrégateurs ont, sur le second marché, acheté les données aux collecteurs. Les données recueillies sont des données brutes qui n'ont pas vraiment d'importance si elles sont utilisées seules. Cependant, l'insertion d'une donnée brute dans un ensemble de données apporte quelque chose de très intéressant (Lambrecht et Tucker, 2017). Les agrégateurs, lorsqu'ils achètent les données aux collecteurs, agrègent les données pour construire ensuite des profils-types d'utilisateurs en fonction des données collectées (Akçura et Srinivasan, 2005). Ils les vendent ensuite à des entreprises ou des annonceurs publicitaires qui les utilisent principalement à des fins marketing. Les entreprises se servent de ces profils pour innover leurs services, personnaliser leur offre ou encore réaliser des campagnes de publicité ciblées et très spécifiques (Rallet 2008).

Il existe des cas exceptionnels où les données ne circulent pas entre les trois marchés: les grandes plateformes. En effet, pour celles-ci, les marchés secondaire et tertiaire sont regroupés en un seul marché. Facebook ou Google, par exemple, collectent les données de leurs utilisateurs et créent directement des profils de ceux-ci dont ils se servent à des fins commerciales ou qu'ils revendent à d'autres entreprises pour engendrer un revenu supplémentaire (Rallet 2008).

2.1.4. Conclusion

Il est important de retenir de ce processus de marchandisation des données que celles-ci se transforment en passant d'un marché à l'autre. De données brutes individuelles à profil d'utilisateur, en passant par la forme de données agrégées, elles prennent de la valeur en se propageant d'un marché à l'autre. Les individus ne sont pas conscients de cette valorisation de leurs données personnelles et sont encore moins conscients des revenus que peuvent en tirer les collecteurs et les agrégateurs. L'échange "données contre service" n'est pas équitable, particulièrement sur le marché primaire. Les données individuelles brutes n'ont pas beaucoup de valeur mais lorsque les data brokers les acquièrent, leur valeur marchande explose.

2.2. Les différents types de base de données

Comme constaté ci-dessus, les données sont collectées, exploitées, revendues sur différents marchés. Tout cela est possible grâce à des mécanismes spécifiques : les bases de données. Une base de données est « *un ensemble d'informations qui est organisé de manière à être facilement accessible, géré et mis à jour. Elle est utilisée par les organisations comme méthode de stockage, de gestion et de récupération de l'information* » (Oracle).

2.2.1. Base de données relationnelle

Le modèle de base de données relationnelle est utilisé, depuis les années 70, pour collecter, stocker et manipuler des données. Les données collectées sont stockées sous forme de tables, chaque table contenant des lignes et des colonnes. Les lignes représentent les produits et les colonnes représentent les attributs. Ce système est appelé le langage de requête structuré (SQL) (Medhi & Baruah 2017). C'est le modèle de base de données le plus traditionnel, il était auparavant le plus utilisé. Il a longtemps dominé l'industrie d'internet car c'est un modèle performant, fiable et mature qui met en avant de manière très intuitive la relation entre les données. Il possède également d'autres avantages, comme l'indépendance des données ou le fait qu'aucun attribut ne soit répété (Oracle). Cependant, il est moins utilisé depuis quelques années suite à l'explosion des données et l'utilisation massive de celles-ci. Ce modèle n'est en effet pas conçu pour traiter un trop grand nombre de données. Le modèle de base de données relationnelle possède un schéma trop rigide ne permettant pas l'ajout de beaucoup de nouvelles relations entre les points (Medhi & Baruah 2017).

2.2.2. Base de données orientée graphe

Il existe à l'heure actuelle une solution intéressante, le modèle de base de données orientée graphe. Il permet de stocker, manipuler et collecter un plus grand nombre de données de manière beaucoup plus performante. Les bases de données orientées graphes sont des bases de données de type «NoSQL», «Not Only SQL» qui désignent des systèmes de données non-relationnelles (Medhi & Baruah 2017). Pour stocker des données et représenter les relations entre celles-ci, ces modèles utilisent une structure en graphe avec des nœuds de données, des arêtes et des propriétés. Les nœuds représentent des entités comme des personnes ou des entreprises. Les arêtes représentent les relations entre les nœuds, ce sont les lignes qui les relient entre eux. Les propriétés sont des informations qui sont associées aux nœuds. Par exemple, si «ordinateur» est un nœud, il peut être lié à des propriétés comme «technologie» ou «internet» (Batra & Tyagi 2012).

Ces bases de données orientées graphes permettent d'analyser et de comprendre des informations et présentent de nombreux avantages. Tout d'abord, les graphes permettent de comprendre les relations de manière claire et simple. La vitesse de la requête est rapide car elle dépend du nombre de relations et non de la quantité de données. Ainsi, même si les données sont très nombreuses et les relations entre celles-ci très complexes, cela n'affectera pas négativement le processus de requête des données. Cependant, ces modèles présentent quand même quelques aspects négatifs. En effet, il n'y a pas de langage de requête standard et les processus sont élaborés pour une architecture à serveur unique (Ionos 2020).

Les bases de données orientées graphes sont très utiles pour analyser les réseaux sociaux et le comportement d'achat des clients. En effet, puisque ce modèle met très facilement en évidence les relations, les entreprises qui les utilisent peuvent faire de nombreuses recommandations (Batra & Tyagi 2012). Par exemple, avec Facebook, il est très facile d'établir des relations entre les utilisateurs et de faire des recommandations d'amis ou de pages à un utilisateur en fonction des autres amis ou pages qu'il aime (en fonction des autres relations). Concernant le comportement d'achat des clients, les entreprises peuvent recommander certains produits à certains clients en analysant les produits qu'ils achètent, l'historique des clics, ... Les bases de données sont aussi très utiles pour détecter les cas de fraude ou dans la chaîne logistique.

Pour bien comprendre la différence entre ces deux bases de données, voici un exemple. Pour ajouter ou modifier une relation, il est beaucoup plus simple d'en créer une supplémentaire sur le graphe de gauche, qui représente une base de données orientée graphe. En effet, à droite, l'ajout est plus compliqué car il faut rajouter plusieurs tables pour créer cette relation. Cela coûte donc plus d'argent et prend plus de temps (Medhi & Baruah 2017).

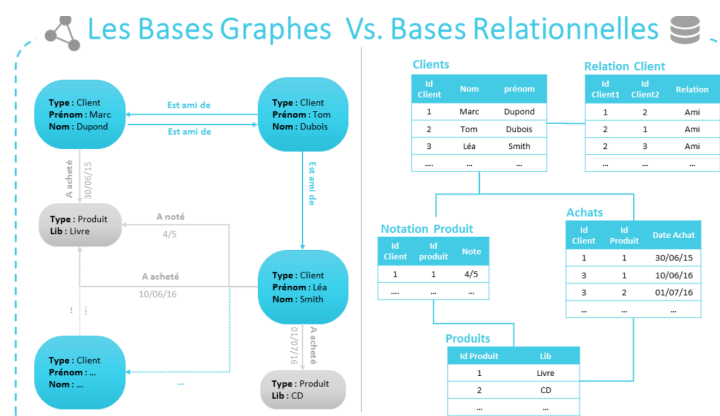


Figure 1 : Les bases Graphes VS. Bases Relationnelles

Source : IllustraData.com

Chapitre 3 : L'influence et les dangers des réseaux sociaux et des grandes plateformes

3.1. Les réseaux sociaux et la vie privée

Les réseaux sociaux sont très utilisés, et ce, par des internautes de plus en plus jeunes selon une étude réalisée par Themis en 2021. Les utilisateurs y exposent des milliers de données rendues publiques sans se rendre réellement compte des risques. Leur vie privée est compromise.

3.1.1. Définitions

Selon Michel Forcé (2008), un réseau social « *est un ensemble de relations entre un ensemble d'acteurs* ». Cet ensemble peut être organisé (une entreprise, par exemple) ou non (comme un réseau d'amis) et ces relations peuvent être de nature fort diverse (pouvoir, échanges de cadeaux, conseils, etc.), spécialisées ou non, symétriques ou non (Lemieux, 1999).

Mercklé (2016) détaille davantage sa définition en affirmant que les réseaux sociaux « *ont pour caractéristiques communes d'offrir à leurs utilisateurs : la possibilité de créer un espace personnel de présentation de soi, où ils peuvent mettre à disposition de tous les informations et les images qu'ils souhaitent, leur permettant de dire ce qu'ils sont et ce qu'ils font, ce qui définit leur 'profil' ; la possibilité d'accéder, selon des modalités et à des degrés variés, aux 'profils' mis en ligne selon le même principe par les autres membres du réseau ; la possibilité de nouer des relations avec des membres du réseau, relations qui font ensuite partie de leurs 'profils' respectifs, et contribuent donc ainsi à les définir, puisque la liste des 'amis' peut être affichée dans le profil au même titre que les goûts musicaux ou littéraires* ».

3.1.2. Chiffres clés

Depuis plusieurs décennies, l'utilisation d'internet et des réseaux sociaux ne cesse de croître. En juillet 2021, selon le "Digital 2021 July Global Statshot Report", il y avait 4,80 milliards d'internautes, soit 61% de la population mondiale. En ce qui concerne l'utilisation des réseaux sociaux, les chiffres sont encore une fois en hausse, avec 4,48 milliards d'utilisateurs soit 57% de la population mondiale. Plus précisément encore, selon les nouvelles données de GWI, 95% des utilisateurs d'internet âgés entre 16 et 64 ans surfent sur les réseaux sociaux chaque mois. Les réseaux sociaux sont ainsi l'activité en ligne la plus utilisée au monde.

En ce qui concerne les différents réseaux sociaux, Facebook est la plateforme qui rassemble le plus d'utilisateurs à savoir 2, 853 milliards. YouTube arrive en seconde position avec 2, 291 milliards d'utilisateurs et WhatsApp en troisième position avec 2 milliards d'utilisateurs.

3.1.3. Les réseaux sociaux et les données personnelles

Comme le prouvent les chiffres ci-dessus, les réseaux sociaux ont du succès. Cependant, ceux-ci présentent tout de même certains aspects négatifs. La plupart des utilisateurs n'emploient pas ces plateformes correctement car ils gèrent mal les fonctionnalités de celles-ci et la confidentialité de leurs données. Les utilisateurs ne sont pas toujours conscients qu'ils ne sont pas propriétaires de leurs publications et que celles-ci ne sont pas privées. Ils ne cessent de publier du contenu sur leurs activités personnelles, leurs données personnelles (téléphone, ...), leurs vacances et tout ce qui concerne leur vie privée. Ces milliers d'informations étant publiques, il y a beaucoup de risques de cybercriminalité comme les piratages de comptes, les vols de données personnelles, l'utilisation de celles-ci à des fins commerciales (Fire et al., 2014). Malheureusement, les utilisateurs manquent de connaissances et de cyberculture (Zeebaree et al. 2020). Ils pensent qu'en possédant des antivirus et en mettant à jour leurs logiciels régulièrement, ils seront protégés de tous les risques comme les vols de données ou le piratage. Cependant, cela ne suffit pas car les techniques de piratage et de vol évoluent très vite et les outils que les utilisateurs emploient pour se protéger ne sont pas toujours réactifs à ces nouvelles techniques (Sylvestre 2017).

3.1.4. Piratage et cybercriminalité

La définition de piratage informatique ou « hacking » a évolué depuis quelques décennies. Selon Sterling (1992), hacker signifiait « *l'exploration intellectuelle en roue libre du potentiel le plus élevé et le plus profond des systèmes informatiques. Le piratage peut décrire la détermination à rendre l'accès aux ordinateurs et à l'information aussi libre et ouvert que possible* ». Plus tard, Brenner (2001) définit le piratage informatique comme « *le geste d'accéder à un système informatique sans autorisation* ».

Le nombre de piratages et de cybercriminalité ne cesse d'augmenter depuis des années. Selon une étude réalisée à l'université de Maryland, il y a une attaque de hacking toutes les 39 secondes aux États-Unis (Cukier 2007). Cela s'explique surtout par l'augmentation du nombre de personnes qui possèdent des smartphones et donc du nombre de personnes qui utilisent

internet et les réseaux sociaux, regorgeant de données pour les hackers (Chan & Virkki, 2014). Une deuxième raison est la cyberculture très pauvre qu'ont les internautes, ils ne sont donc pas conscients de tous les risques auxquels ils sont exposés lorsqu'ils utilisent les plateformes et les réseaux sociaux (Chan & Virkki, 2014). Enfin, la dernière raison est l'apparition continue de nouvelles technologies et de nouveaux outils toujours plus performants qui permettent de hacker les utilisateurs ou pire encore, les systèmes de protection comme les antivirus (Nixon 2021).

Wall (2007) distingue 3 types de cybercriminalité. La première, « crime against machine » menace l'intégrité des ordinateurs. Elle comprend la cyber-intrusion ou les piratages téléphoniques (phreaking). Les utilisateurs vont ainsi recevoir des spams ou des parasites informatiques. Le deuxième type, « crime using machine » correspond aux délits assistés par les ordinateurs. Ce sont principalement des « cyber-vols », c'est-à-dire des dommages acquisitifs ayant lieu dans le cyberspace. Ce deuxième type comprend les vols de secrets commerciaux, les vols d'identités, les vols de données personnelles ou encore les utilisations frauduleuses des cartes de crédits. Enfin, le dernier type de cybercriminalité, « crime in the machine » est basé sur les infractions liées au contenu. Wall distingue ici deux sous-catégories. La première concerne la cyber-obscénité, c'est-à-dire le commerce de matériel sexuellement expressif dans le cyberspace. Cette catégorie correspond au cyber-sex et comprend par exemple le commerce sexuel en ligne, les sites de Camgirls et tout ce qui est lié à la pornographie. La deuxième sous-catégorie est liée à la cyber-violence, c'est-à-dire à l'impact violent des cyber-activités d'autrui sur un individu ou un groupe social ou politique. Les activités visées ici peuvent inclure le cyber-harcèlement ou les discours de haine.

Le nombre de vols de données et de hacking ne cesse d'augmenter et les grandes entreprises doivent mettre en place des systèmes de protection afin d'assurer la sécurité des données de leurs utilisateurs. En 2019, 4,1 milliards de données ont été volées durant le premier semestre (Forbes). Le vol le plus connu est celui de l'affaire Cambridge Analytica. Cette entreprise britannique a analysé les données de 87 millions d'utilisateurs Facebook. Elle a offert ses services à Donald Trump lors de la campagne présidentielle américaine en 2016 (Le Monde). D'autres scandales ont régulièrement lieu. Par exemple, les données de 139 millions d'utilisateurs de Canva, un site internet australien connu pour la réalisation de design et graphiques en ligne, ont également été volées par un hacker connu sous le nom de

« GnosticPlayers ». Depuis février 2021, il a piraté 939 millions de données de 44 entreprises dans le monde (ZDNet 2019).

3.2. Les grandes plateformes

3.2.1. Caractéristiques

Depuis plus d'une décennie, les grandes plateformes, dont les GAFAM, c'est-à-dire Google, Apple, Facebook, Amazon et Microsoft, sont devenues des incontournables d'internet. Ces géants du net constituent aujourd'hui l'oligopole d'internet (Smyrnaio 2016). A cela sont venues récemment s'ajouter les NATU, Netflix, Airbnb, Tesla et Uber, qui détiennent un nombre de parts de marché sans précédent. Utilisées par des milliards d'utilisateurs pour communiquer, se déplacer, se loger, regarder des films ou encore faire des achats, ces plateformes ne cessent d'accroître leur notoriété (Bourreau & Perrot 2020).

Les plateformes sont un marché multi-face (Tyrol 2006). Qualifiées d'intermédiaires, elles mettent en relation deux groupes d'utilisateurs. Par exemple, des personnes qui cherchent à se déplacer avec des personnes qui conduisent des voitures (Uber), ou bien des personnes cherchant à se loger avec des personnes possédant une maison ou une chambre libre (Airbnb) (Viossat 2018).

Ces plateformes sont des marchés de réputation (Viossat 2018). Elles sont caractérisées par des effets réseaux positifs, c'est-à-dire que plus les gens parlent de celles-ci, plus elles vont paraître attractives et vont donc attirer les utilisateurs des deux groupes (Belleflamme 2017). Par exemple, Uber attire de nombreux utilisateurs. Plus il y aura d'utilisateurs d'un groupe, ceux qui souhaitent se déplacer, plus cela va attirer les utilisateurs de l'autre groupe, ceux qui conduisent les voitures. Plus il y aura d'offres, donc de voitures disponibles partout, plus les utilisateurs demandeurs vont souhaiter utiliser ce service. Les interactions entre les deux groupes d'utilisateurs apportent donc de la valeur à la plateforme (Belleflamme 2017).

3.2.2. Avantages

Si ces grandes plateformes sont autant utilisées, c'est parce qu'elles présentent de nombreux avantages à la société. Premièrement, elles offrent des services avantageux et innovants pour les citoyens. Grâce à celles-ci, ils peuvent facilement communiquer, regarder des films, se déplacer, se loger ou encore faire des achats. Les opportunités économiques offertes par ces

plateformes à leurs utilisateurs sont également estimables (Bourreau & Perrot 2020). Ces nouveaux modèles de services sont généralement moins chers que les services traditionnels, comme c'est le cas d'Uber, qui est économiquement plus intéressant qu'un taxi traditionnel (Le Parisien 2015). De plus, ces plateformes, qui au départ, étaient principalement utilisées pour du commerce et de la vente, se sont, petit à petit, tournées vers des services et une économie collaborative (Ert et al. 2016). L'économie collaborative, ou « sharing economy » désigne « *un ensemble de modèles organisationnels et commerciaux fondés sur des approches de "partage", de "collaboration", de "gig" ou d'"accès" à l'utilisation des ressources.* » (Schlagwein et al. 2019). Les utilisateurs soutiennent cette économie avantageuse tant sur les plans économiques et écologiques que sociétaux (Botsman and Rogers, 2011).

3.2.3. Inconvénients liés à la vie privée

Malheureusement, les services qu'offrent les grandes plateformes à leurs utilisateurs ne sont pas vraiment gratuits. Les internautes vont en réalité échanger leurs données contre ces services « gratuits ». Comme expliqué précédemment avec les marchés primaire, secondaire et tertiaire, les grandes plateformes (entre autres) collectent, traitent et vendent les données personnelles des utilisateurs sans réel consentement de leur part (Rallet 2008).

La plupart des utilisateurs commencent maintenant à comprendre que leurs données sont utilisées. En 2015, selon une étude réalisée par Symantec, 59% des européens étaient inquiets à propos de leurs données personnelles. Pourtant, il est ressorti de l'enquête que seule une personne sur quatre lisait les conditions d'utilisation avant de procéder à un achat ou de s'inscrire sur un site pour obtenir un service. Ce comportement paradoxal est appelé « Privacy Paradoxe » (Barnes 2006). Les utilisateurs sont prêts à échanger leurs données contre des avantages, ici des services, mais se plaignent que leurs données soient utilisées et sont inquiets. Ils sont ainsi partagés entre ne pas divulguer leurs données et compromettre leur vie privée et bénéficier de services avantageux (Norberg et al. 2007).

Un autre problème qui expliquerait que les utilisateurs peuvent difficilement se passer des grandes plateformes, telles que Facebook, est lié à leur place dominante sur le marché. Comme expliqué ci-dessus, les effets réseaux en sont la cause principale. En effet, un utilisateur qui souhaiterait se retirer de ce réseau social, suite, par exemple, à un scandale comme Cambridge Analytica, se verrait alors coupé de toutes les relations sociales qu'il possède sur la plateforme car Facebook a une position dominante et met en relation des milliers de personnes. Aucun

utilisateur ne souhaite faire le premier pas, de peur de se retrouver seul. Quitter ces grandes plateformes est une solution idéale à titre individuel mais pas d'un point de vue collectif (Maurel 2019).

Un des problèmes majeurs de ces plateformes, et même de la plupart des sites internet, est le design de ceux-ci (Chatellier et al. 2019). En effet, ils sont créés de façon à ce que les utilisateurs donnent leur consentement en ce qui concerne la protection de leurs données personnelles. Le RGPD, dans son article 25, soulève la question du « privacy by design », c'est-à-dire les différentes techniques utilisées par les plateformes, principalement au niveau du design, pour protéger, ou non, les données des utilisateurs (RGPD 2018). Le design des interfaces influence la façon dont les utilisateurs se comportent à l'égard de ces plateformes et, la plupart du temps, ne respecte pas le RGPD surtout en termes de transparence et de consentement. Celles-ci développent des interfaces trompeuses en se jouant de l'attention des utilisateurs et les influencent donc à partager leurs données personnelles sans réel consentement (Chatellier et al. 2019).

Il existe de nombreux biais cognitifs sur lesquels jouent les plateformes et les sites internet pour tromper leurs utilisateurs et ainsi collecter des données personnelles de manière relativement simple.

Tout d'abord, la surcharge informationnelle qui signifie que lorsqu'un individu a une trop grande quantité d'informations à lire, il les ignore. Bien souvent, les utilisateurs doivent lire de longues pages de conditions d'utilisations, écrites en tout petits caractères, ils ne prennent donc pas le temps de les lire. Le vocabulaire utilisé est généralement très spécifique et donc peu compréhensible pour les internautes (Chatellier et al. 2019).

Un deuxième biais cognitif est l'effet d'ancrage, où les utilisateurs ont pris l'habitude de cliquer sur « accepter » sans se poser trop de questions. Les bannières de « cookies » en sont un exemple pur (Chatellier et al. 2019).

L'aversion à la perte est également un biais cognitif auquel les utilisateurs doivent faire face régulièrement. Par exemple, lorsqu'un utilisateur lit un article sur un site internet, il lui arrive très souvent de devoir payer ou se connecter pour lire la suite de celui-ci. L'utilisateur, ayant déjà commencé celui-ci, a tendance à encoder ses données pour terminer sa lecture alors que si

on lui avait demandé ses données avant le début de la lecture, il ne l'aurait sans doute pas accepté (Chatellier et al. 2019).

Un dernier biais cognitif est l'effet de cadrage, c'est-à-dire la façon dont les éléments sont présentés aux utilisateurs des sites internet. Par exemple, lorsqu'ils doivent accepter les cookies, le mot « accepter » sera généralement en couleur alors que le mot « refuser » ne ressortira pas (Chatellier et al. 2019).

PARTIE 1b : Conscientisation des utilisateurs de la collecte et du traitement de leurs données personnelles

Chapitre 1 : Perception des internautes quant à l'utilisation de leurs données personnelles

1.1. Inquiétude des utilisateurs

La prise de conscience de la nécessité de protéger ses données personnelles croît chez les internautes depuis près de 10 ans et encore plus depuis 2018 et l'apparition du RGPD. Bien qu'ils ne comprennent pas vraiment les processus de la collecte et du traitement de leurs données personnelles, comme déjà mentionné précédemment, de nombreuses études prouvent que les utilisateurs s'inquiètent de plus en plus de la collecte de leurs données personnelles lorsqu'ils naviguent sur des sites internet ou des applications.

Selon une enquête réalisée par Forgerock en Allemagne, en France, aux États-Unis et au Royaume-Uni, plus de la moitié des utilisateurs s'inquiètent pour leurs données personnelles. Il en est ressorti que la moitié des personnes interrogées ne savent pas à quel point leur identité digitale (et donc leurs informations personnelles) est partagée. Pour 76% d'entre elles, il y a une différence entre ce qu'elles pensent avoir partagé et ce qu'elles partagent réellement. Les résultats de l'enquête montrent également que les utilisateurs ne sont pas assez informés dans ce domaine. 31% des répondants savent qui serait responsable en cas de vol de données, 57% ne savent presque rien ou rien à propos de leurs droits sur leurs données personnelles et 35% seulement savent comment supprimer leurs données d'un site.

Selon une autre enquête réalisée par la CNIL, 66% des français sont devenus plus sensibles à la protection de leurs données personnelles. 46% des répondants ont constaté des abus dans l'utilisation de leurs données personnelles dont 30% n'ont rien fait contre cela. Concernant ce qui les a rendus plus sensibles à la question de la protection des données personnelles, voici les trois raisons les plus importantes : 22% ont répondu avoir peur du vol de données ou du piratage, 11% des sollicitations commerciales et 10% des scandales et de ce qu'ils entendent dans les médias.

Comme le prouvent les chiffres ci-dessus, l'inquiétude autour des données personnelles est bien présente. De nombreux facteurs peuvent influencer l'attitude des utilisateurs à l'égard de la collecte de leurs données personnelles. Beaucoup d'internautes prennent peur face à ce traitement des données et cette crainte ne cesse de s'accroître ces dernières années. Les facteurs justificatifs peuvent être classés en deux catégories (Miltgen 2010).

1.1.1. Facteurs individuels

Cette catégorie peut être divisée en sous-catégories. Tout d'abord, les traits de personnalité des utilisateurs. En effet, le caractère de l'utilisateur peut influencer son comportement, certains sont plus méfiants, d'autres plus curieux. L'importance de l'image fait également partie de cette catégorie car, si les utilisateurs font très attention à leur image, ils auront tendance à moins se dévoiler et à craindre davantage l'exposition de leurs données (Miltgen 2010).

La deuxième sous-catégorie comprend l'expérience (Miltgen 2010). Un premier exemple pour justifier ce facteur est la collecte de données par mail. Un utilisateur qui encode une adresse mail et qui reçoit par la suite plein de publicités dans sa boîte mail va, par expérience, ne plus encoder son adresse sur n'importe quel autre site pour ne pas être envahi de publicités. Un deuxième exemple concerne les bannières de publicités ciblées. Plus ils utilisent Facebook, plus les internautes vont se rendre compte que les bannières affichées sont en lien avec leurs récentes recherches sur internet. Selon une enquête réalisée par la CNIL, les spams et autres sollicitations commerciales sont le deuxième facteur accentuant le plus la peur chez les internautes.

Enfin, les facteurs sociodémographiques comme l'âge ou l'éducation sont également des facteurs individuels qui influencent l'inquiétude des utilisateurs quant au traitement de leurs données. Selon Miltgen et Peyrat-Guillard (2014), les jeunes, même s'ils prétendent accorder de l'importance à la sécurité de leurs données, éprouvent moins d'inquiétude que les personnes plus âgées. Quant à l'éducation, Zhang, Chen et Lee (2013) prouvent que celle-ci est positivement corrélée à la peur du vol des données personnelles. Cela signifie que les personnes bénéficiant d'un niveau d'éducation élevé ont plus de connaissances à ce sujet et peuvent ainsi plus facilement percevoir les risques et diminuer alors leurs craintes.

1.1.2. Facteurs externes

Les facteurs environnementaux influencent l'attitude et donc la peur des individus.

Le premier facteur est l'exposition médiatique. En effet, de nombreux scandales liés au vol des données personnelles impactant des milliers d'utilisateurs ont vu le jour ces dernières années (Miltgen 2010). Le plus connu est celui de Cambridge Analytica et Facebook, comme expliqué précédemment. Tous ces scandales ont fait la une des journaux et ont donc alerté beaucoup d'utilisateurs à propos du traitement de leurs données personnelles. Selon Benamati, Ozdemir et Smith (2017), l'exposition aux médias forme le niveau de connaissances des utilisateurs quant au respect de leur vie privée et du vol de leurs données.

Ensuite, le bouche-à-oreille est également un facteur important. Bien qu'on en parle certainement plus dans les médias, l'avis des personnes de l'entourage d'un utilisateur a généralement un impact très fort sur sa façon de se comporter et peut donc accentuer sa peur face à cette récolte de données.

La culture peut influencer les utilisateurs quant à leur attitude face à la collecte de leurs données (Miltgen 2010). En Europe, par exemple, les internautes sont beaucoup plus inquiets quant à la préservation de leurs données personnelles que les utilisateurs américains. Aux États-Unis, les internautes acceptent plus facilement d'être « le produit » et de bénéficier des services « gratuits » en échange de leurs données personnelles (Darnault 2021).

L'apparition du RGPD est également un facteur lié à la peur des internautes. En effet, ce règlement a été très médiatisé et a été un sujet de discussion dans beaucoup d'entreprises également (Mercier 2019).

Chapitre 2 : L'éducation à la citoyenneté numérique comme solution

2.1. Introduction

Le numérique a révolutionné nos habitudes et notre quotidien, nous offrant de nouvelles opportunités mais nous mettant aussi face à certains dangers. Dans cette ère numérique, suite à l'apparition continue de nouvelles technologies, telles que les objets connectés, la géolocalisation ou l'intelligence artificielle, les données personnelles sont de plus en plus nombreuses. Elles constituent une mine d'or pour les entreprises mais les utilisateurs doivent

se méfier et les protéger. Outre l'apparition de nouvelles technologies et donc de nouvelles données personnelles à pouvoir collecter, de nouvelles techniques pour collecter et traiter les données personnelles se sont développées (CNIL).

L'inquiétude des consommateurs quant à la protection de leurs données ne cesse de croître depuis l'apparition de ces technologies. Bien que de plus en plus de lois et règlements semblent se mettre en place pour protéger les citoyens, tel que le RGPD en Europe en 2018, cela ne suffit pas à rassurer ceux-ci, ni à empêcher la collecte des données par la plupart des entreprises, selon une enquête réalisée par la CNIL.

Une solution à la conscientisation et la protection des données personnelles serait l'éducation au numérique (Conseil Européen 2016). En effet, les citoyens ne connaissent que très peu de leurs droits concernant leur vie privée, la protection de leurs données, leurs obligations et les risques auxquels ils sont exposés. Il faut donc les éveiller par rapport à cela.

La citoyenneté numérique est « *le maniement efficace et positif des technologies numériques (créer, travailler, partager, établir des relations sociales, rechercher, jouer, communiquer et apprendre), la participation active et responsable (valeurs, aptitudes, attitudes, connaissances) aux communautés (locales, nationales, mondiales) à tous les niveaux (politique, économique, social, culturel et interculturel), l'engagement dans un double processus d'apprentissage tout au long de la vie (dans des structures formelles, informelles et non formelles) et la défense continue de la dignité humaine.* » (Conseil Européen 2016).

L'éducation à la citoyenneté numérique désigne « *l'autonomisation des enfants par le biais de l'éducation ou l'acquisition de compétences pour apprendre et participer activement à la société numérique. Il s'agit des connaissances, des aptitudes et de la compréhension nécessaires aux utilisateurs pour exercer et défendre leurs droits et responsabilités démocratiques en ligne et promouvoir et protéger les droits de l'homme, la démocratie et l'État de droit dans le cyberspace.* » (Conseil Européen 2016).

Puisqu'il existe de plus en plus de technologies qui accaparent nos données, les jeunes sont exposés de plus en plus tôt aux risques concernant leurs données personnelles et leur vie privée. L'éducation au numérique doit donc se faire assez tôt dans la vie des jeunes, tant dans l'environnement familial que dans les écoles. La famille et l'école sont deux éléments clés dans

le processus d'éducation d'un enfant et pour que celui-ci soit une réussite, il faut que les deux les éléments travaillent ensemble (Henderson et Berla 1994).

2.2. Education en milieu familial

Les parents sont assez inquiets quant aux dangers auxquels sont exposés leurs enfants en utilisant internet (Livingstone 2002). Les parents sont surtout concernés par les risques qui peuvent mettre en danger la vie privée de leurs enfants (Ou et al. 2011). Ceux-ci s'inquiètent par rapport à la protection des données personnelles de leurs enfants. Ils savent que les jeunes ne font pas attention aux politiques de confidentialité et qu'ils ne comprennent pas les mécanismes de collecte de données (Ou et al. 2011).

La famille est un lieu sacré d'apprentissage pour les enfants qui répètent généralement les pratiques de leurs parents. Ceux-ci ont une influence considérable sur la façon dont leurs enfants se comportent (Combs-Ronto et al. 2009 ; Reitz et al. 2006 ; Miller-Lewis 2006). Il est de leur devoir de leur expliquer le fonctionnement d'internet, les risques et les dangers auxquels ils peuvent être exposés. Il a été prouvé que les parents ayant de bonnes connaissances à ce sujet et prenant le temps de superviser leur enfant avaient un effet positif sur la façon dont le jeune utilisait internet. Celui-ci sera davantage conscient des dangers et ne divulguera pas, ou moins, ses données et ses informations personnelles sur internet (Feng & Xie, 2014). Au contraire, il a également été prouvé qu'un jeune n'ayant reçu aucune supervision et aucune règle utilise internet sans se soucier de la protection de sa vie privée et de ses données personnelles (Feng & Xie, 2014).

Comme le suggérait le Conseil Européen, l'éducation serait ainsi une bonne solution pour conscientiser les citoyens, et surtout les jeunes, à la protection de leurs données personnelles et de leur vie privée. Cependant, cette solution comporte deux problèmes.

Le premier est que les parents, qui sont sans doute la première génération de parents à devoir faire face à une aussi grande évolution des technologies, n'ont pas toujours les connaissances requises pour pouvoir par la suite les transmettre à leurs enfants (Fluckiger 2010). Que cela soit lié aux nouvelles technologies de l'information et de la communication, aux nouvelles plateformes ou simplement à l'usage du numérique au niveau scolaire, la plupart des parents ne sont pas conscients des risques et des dangers auxquels ils sont confrontés ni des risques auxquels leurs enfants le sont (Rohmer 2021).

Le deuxième problème concerne la fracture du numérique (Rizza 2006). L'Organisation de Coopération et de Développement Economique (OCDE) définit, en 2001, la « fracture numérique » comme « *l'écart entre les individus, les foyers, les entreprises, les espaces géographiques et les différences socio-économiques, concernant leurs opportunités d'accès aux technologies de l'information et de la communication et de l'usage d'internet pour l'ensemble de leurs activités. La fracture numérique reflète ainsi les profondes divergences entre et à l'intérieur des pays* ». Ainsi, de nombreuses familles issues, entre autres, de milieux sociaux précaires n'ont pas les moyens d'avoir accès à ces technologies et n'ont pas les compétences requises pour les utiliser.

2.3. Education en milieu scolaire

Ces dernières années ont été marquées par une augmentation de l'utilisation et de l'accès au numérique dans les familles, tant pour les enfants que pour les parents (Rideout 2015). De plus, beaucoup d'écoles ont décidé d'intégrer progressivement la technologie et le numérique au sein de leur établissement. Ces deux raisons ont poussé les écoles à mettre en place un plan pour inclure l'éducation à la citoyenneté numérique dans leur projet. L'éducation au numérique aborde les sujets tels que le cyberharcèlement, les discours de haine ou encore la protection des données personnelles et de la vie privée (Lauricella et al. 2010).

L'augmentation de l'utilisation de ces technologies chez les enfants (Milenkova et al., 2018) a également changé la mentalité des enseignants. Ceux-ci reconnaissent l'influence de ces technologies sur les enfants et assument leur rôle à jouer dans l'apprentissage de l'utilisation appropriée de ces nouvelles technologies. Ils tentent de les guider positivement à adopter un comportement éthique et sans danger (Lauricella et al. 2010). Cependant, les enseignants n'ont pas toutes les compétences requises pour enseigner le numérique (Dioni 2008). Selon Bruillard et Baron (2006), l'enseignement du numérique repose sur trois compétences : la technique, la didactique et la pédagogie. Les enseignants doivent accompagner les élèves dans le changement, compétence à laquelle ils ne sont pas formés à la base. Les élèves sont pour le moment ainsi très autodidactes. Pour pouvoir enseigner le numérique correctement, les profs souhaitent se former, mais pas uniquement sur les aspects techniques (Dioni 2008). Malheureusement, les moyens alloués aux formations des enseignants en ce qui concerne l'apprentissage de la citoyenneté numérique sont actuellement limités (Livingstone et al., 2011).

2.4. Actions et stratégies mises en place

Différents projets ont déjà été mis en place par des associations ou administrations dans le but de sensibiliser les parents et de former les enseignants à la protection de leur vie privée et de leurs données personnelles ainsi que celles des enfants.

2.4.1. Better internet for kids

La Commission Européenne a lancé une nouvelle stratégie visant à améliorer l'utilisation d'internet chez les enfants et à les éveiller aux risques et aux dangers auxquels ils sont confrontés. Cette stratégie, nommée Better Internet for Kids (BIK), a pour but d'offrir aux enfants des compétences afin qu'ils puissent utiliser les outils informatiques en toute sécurité et qu'ils puissent pleinement développer leur créativité en exploitant tout le potentiel du marché. La stratégie européenne, qui vise également les parents et les enseignants, a influencé les politiques nationales dans la plupart des pays de l'UE. Chaque année, diverses actions et campagnes menées dans le cadre de la stratégie touchent des milliers d'écoles et de jeunes, de parents et d'enseignants. Selon les estimations, 61 millions de personnes ont été touchées par les différentes campagnes et activités mises en place en 2019 et 2020. Une des activités les plus connues est le Safer Internet Day, journée mondiale qui promeut un usage d'internet plus responsable auprès des jeunes, des parents et des enseignants. En 2021, 200 pays ont célébré cette journée.

La Commission européenne, en lien avec sa stratégie, cofinance, dans les États membres et dans certains autres pays européens, des « National Safer Internet Centers », c'est-à-dire des centres destinés à aider les jeunes, les parents et les enseignants à utiliser internet de manière plus sûre et à les sensibiliser en leur proposant des contenus et des services.

En Belgique, le centre s'appelle Child Focus et dispose d'un portail de prévention où toutes sortes d'articles et de vidéos sont disponibles. L'association a maintenant mis en place la « Child Focus Academy » qui conçoit des programmes de formations sur des sujets liés à la sécurité et l'utilisation d'internet. Les parents peuvent, par exemple, assister à des séances d'informations « Webetic » pour apprendre à mieux gérer internet au sein de leur famille en encadrant les enfants correctement et en les sensibilisant. Les enseignants peuvent suivre les formations « Clicksafe » où Child Focus présente les outils pédagogiques nécessaires pour apprendre aux élèves une utilisation responsable d'internet. Child Focus propose également dans les écoles des ateliers destinés aux enfants et aux adolescents.

2.4.2. Conseil européen

En 2016, le Comité Directeur pour les Politiques et Pratiques Educatives (CDPPE) du Conseil Européen a lancé une nouvelle action : « Éducation à la citoyenneté numérique ». Ce projet intergouvernemental a pour but de « redéfinir le rôle que joue l'éducation pour permettre à tous les enfants d'acquérir les compétences dont ils ont besoin en tant que citoyens numériques pour participer de manière active et responsable à la société démocratique, que ce soit hors ligne ou en ligne. »

Les experts du projet ECN ont identifié 10 domaines numériques regroupés en 3 catégories distinctes qui vont permettre de définir clairement les connaissances que les citoyens numériques devraient acquérir et développer.

La première catégorie, **Être en ligne**, comprend 3 domaines qui prônent un accès au web et à l'espace virtuel à n'importe quel citoyen. L'objectif est de veiller à ce que chaque citoyen soit intégré et sache utiliser le web en développant sa créativité grâce aux outils numériques et technologiques.

La deuxième catégorie, **Bien-être en ligne**, comprend des domaines relatifs au comportement et à l'attitude des citoyens en ligne, des interactions les uns avec les autres. Ils concernent également la prise de conscience des problèmes que peuvent rencontrer les citoyens dans l'ère du numérique et qui sont néfastes à leur bien-être ou à leur image.

La dernière catégorie, la plus intéressante, est la catégorie **Mes droits en ligne**. Elle comprend 4 domaines dont la « participation active », c'est-à-dire la manière dont les citoyens numériques interagissent dans l'environnement numérique. Le deuxième domaine « droit et responsabilité » consiste à conscientiser les utilisateurs à tous les nouveaux droits qu'ils détiennent dans l'environnement numérique tels que le droit du respect de la vie privée, le droit de liberté d'expression ou encore le droit d'accès. Le domaine suivant est celui de la « vie privée et sécurité » et est lié à la protection des données, la gestion de l'identité et de la sécurité en ligne. Enfin, dernier domaine concerne la « sensibilisation des consommateurs », c'est-à-dire comment sensibiliser, par exemple, les internautes aux nouveaux modèles qui prélèvent leurs données et qui les utilisent à des fins commerciales.

2.4.3. Belgique : Autorité de protection des données

En Belgique, l'Autorité de protection des données, qui était auparavant la Commission de vie privée, a pour mission de veiller à la protection des données des citoyens. Elle a mis en place, il y a quelques années, un site internet, "jedecide.be", afin de sensibiliser les jeunes, les parents et les enseignants. Il a été réadapté et est bien plus complet depuis l'apparition du RGPD. Sur ce site, on retrouve de nombreux conseils et de nombreuses vidéos pour éveiller les jeunes utilisateurs d'internet, mais aussi des recommandations pour les parents et les enseignants.

2.4.4. France : Commission Nationale de l'Informatique et des Libertés

En France, la CNIL va plus loin, elle a introduit un référentiel de formation à la protection des données personnelles à destination des enseignants dans un premier temps. En 2016, la conférence des autorités de protection des données a adopté ce référentiel, à l'international. Ce référentiel, initié par la CNIL, est donc adressé aux enseignants qui ne sont eux-mêmes pas toujours bien au courant des dangers de la collecte de données et des traitements qui en découlent. Il semblait donc important pour la Commission de commencer par former les enseignants qui à leur tour pourront former les élèves et les éveiller aux dangers qu'ils peuvent encourir à cause du partage des données. La CNIL souhaite que le référentiel soit utilisé dans le cadre du programme scolaire.

Selon la CNIL, l'objectif de ce référentiel est d'« *Acquérir une connaissance et une compréhension critiques des droits et responsabilités numériques, développer auprès des jeunes une démarche réflexive sur les usages qui sont faits des données personnelles, sensibiliser sur les risques et enseigner les pratiques permettant de se mouvoir dans l'environnement numérique avec confiance, lucidité et dans le respect des droits de chacun* ».

Les actions quant à l'éveil à la protection des données personnelles chez les jeunes, leurs parents et les enseignants se multiplient mais l'apparition d'un programme complet dans les écoles semblent encore loin.

Conclusion de la revue scientifique

De nombreuses recherches ont déjà été réalisées en ce qui concerne les mécanismes des données personnelles, la façon dont elles sont collectées par les grandes plateformes, ... De nombreuses études ont également démontré la place des réseaux sociaux et de ces plateformes dans la vie des utilisateurs et les conséquences que celles-ci peuvent avoir sur la vie privée des internautes. De plus en plus d'études sont réalisées pour analyser l'attitude des utilisateurs par rapport à cette collecte de données, leurs inquiétudes par exemple.

En revanche, en ce qui concerne l'éducation à la citoyenneté numérique, la littérature scientifique est encore très pauvre. Peu de recherches et d'études ont été réalisées à ce sujet. Il est difficile d'évaluer la capacité des parents et des enseignants à l'éducation numérique. Cependant, de nombreux sites internet, ne faisant pas partie de la littérature scientifique, ont déjà abordé le sujet. Les sites d'organisations telles que la Commission Européenne, la CNIL ou le Conseil Européen, ou bien les sites de certaines associations ont écrit des articles à ce sujet. La plupart de ces sites ont également mis en place des formations en ligne à disposition des parents, des enseignants et des enfants pour les éduquer au numérique. La mise en place de formations et le contenu de certains articles rédigés par les grandes organisations citées ci-dessus, permettent de déduire que les parents et les enseignants manquent de connaissances pour éduquer au numérique.

Hypothèses à tester

Hypothèse 1a : Les enseignants ont les connaissances et les compétences pour conscientiser les élèves à protéger leurs données personnelles.

Hypothèse 1b : L'école a un rôle à jouer dans l'éducation à la citoyenneté numérique des jeunes.

Hypothèse 2a : Les parents ont les connaissances et les compétences pour conscientiser leur enfant à la protection des données personnelles.

Hypothèse 2b : Les parents contrôlent l'utilisation du numérique par leurs enfants.

PARTIE 2 : ETUDES QUALITATIVES

Afin de répondre à la problématique et de tester les différentes hypothèses, plusieurs méthodes ont été utilisées pour collecter des données. Pour obtenir un maximum d'informations provenant de différentes parties prenantes, le choix s'est porté sur une méthode mixte, c'est-à-dire une combinaison de méthodes de collecte et d'analyse de données qualitatives et quantitatives (Pluyes 2012). L'utilisation de méthodes mixtes permet de combiner les forces des méthodes qualitatives et quantitatives (Pluyes 2012). De plus, utilisées conjointement, les limites de chacune des méthodes seraient compensées (Denzin, 2017). La méthode mixte permet également d'obtenir des données plus riches (Sechrest and Sidana, 1995).

Dans cette partie se trouvent la collecte de données et l'analyse qualitative de celles-ci. L'étude qualitative permet d'analyser la problématique de manière plus approfondie et plus détaillée (Vandercammen et Gauthy-Sinéchal, 2014). Elle permet d'obtenir plus d'informations sur les attitudes et les comportements des répondants et donc d'obtenir une richesse de résultats (Pleyers 2020).

Chapitre 1 : Méthodologie

1.1.Choix des personnes interviewées

Afin de tester les différentes hypothèses, une liste des parties potentiellement intéressantes a été dressée puis contactée. Trois d'entre elles ont répondu positivement.

La première personne interviewée est Monsieur Thomas Jadin, directeur d'une école secondaire, le Collège des Hayeffes, et également directeur de l'Association des Directeurs du Brabant-Wallon et Bruxelles. Le deuxième échantillon comprend des élèves, âgés entre 15 et 17 ans, provenant de différentes écoles du Brabant Wallon telles que le Collège des Hayeffes, le Collège du Christ-Roi ou encore le Lycée Martin V. Enfin, la dernière personne interrogée est Madame Virginie Tyou, une auteure, conférencière, formatrice et hypnothérapeute. Elle a notamment écrit des livres comme « Cliky », un roman passant par la fiction pour éduquer les jeunes au numérique. Elle organise des formations sur l'éducation au numérique dans les écoles, aussi bien pour les élèves que pour les enseignants. Elle s'est également lancée dans la formation adressée aux parents.

Trois interviews ont donc été menées auprès de ces parties prenantes afin de tester les différentes hypothèses. La réalisation de plusieurs types d'entretiens auprès de parties prenantes sur un sujet permet d'avoir des points de vues différents et permet également d'obtenir des informations plus complètes et plus variées (Peyers 2020).

1.2.Méthodologie et recherche

Premièrement, un focus group, appelé également groupe de discussion, a été réalisé auprès de six élèves provenant d'écoles secondaires différentes (voir annexe 1). Le focus group est une technique de recherche qui collecte des données à travers les interactions d'un groupe sur un sujet déterminé par le chercheur qui guide cet entretien (Morgan 1996). Cette méthode de collecte de données permet d'obtenir beaucoup d'informations grâce à la dynamique de groupe et aux interactions entre les participants (Peyers 2020).

L'approche utilisée pour réaliser ce focus group est celle de l'entonnoir. L'entretien a donc débuté par des questions globales sur le sujet pour évaluer les connaissances des intervenants, puis des thèmes plus spécifiques ont été abordés (Peyers 2020). Ce focus group a permis d'obtenir des informations supplémentaires provenant des élèves et donc d'adapter certaines questions du guide d'entretien adressé au directeur d'école.

Ensuite, un entretien semi-directif (voir annexe 1) a été conduit auprès d'un directeur d'école. L'entretien semi-directif consiste à poser une série de questions ouvertes prédéterminées mais l'interviewer peut ajouter d'autres questions émergeant de la conversation (Britten, 1995). Ces interviews semi-structurées permettent également aux répondants d'exprimer librement leurs idées dans leurs propres mots et à leur manière. Ces entretiens fournissent des informations fiables et qualitatives (Peyers 2020). Ils permettent d'obtenir des informations plus détaillées que celles obtenues avec d'autres méthodes de collecte de données, comme des enquêtes (Boyce & Neale, 2006).

Enfin, un dernier entretien semi-directif également (voir annexe 1), a été réalisé auprès de Madame Virginie Tyou afin d'obtenir des informations d'une troisième partie prenante, intervenante dans les écoles et apportant donc d'autres informations pertinentes d'un point de vue extérieur à l'école.

1.3. Analyse des données

Après avoir réalisé les différents entretiens, la phase suivante consistait à analyser toutes les données obtenues. Pour ce faire, une analyse qualitative de contenu a été privilégiée. Cette méthode consiste à résumer, classer et organiser les informations provenant des entretiens (Hsieh et Shannon, 2005). L'analyse de contenu ne se contente pas de classer uniquement des mots, mais analyse de manière approfondie le langage afin de pouvoir classer de grandes quantités de textes dans un nombre efficace de catégories (Weber, 1990).

Dans un premier temps, tous les entretiens ont été retranscrits. La phase de retranscription est essentielle pour faciliter la lecture et en avoir une trace fidèle (Auerbach, Silverstein, 2003). Après cela, l'analyse de contenu a pu débuter. Toutes les informations importantes de chaque entretien ont été relevées. Elles ont d'abord toutes été classées par interview. Ensuite, elles ont été attribuées à une ou plusieurs hypothèses. Certaines informations sont apparues dans plusieurs interviews différentes et ont donc pu être comparées.

1.4. Limites de la méthodologie

Premièrement, les entretiens individuels semi-directifs ne sont pas généralisables d'un point de vue statistique (Boyce & Neale, 2006). Ensuite, l'utilisation d'entretiens semi-directifs limite parfois les répondants à développer leurs idées sur un sujet et l'interviewer peut parfois passer à côté d'informations importantes (Britten, 1995). Concernant les focus groups, les réponses provenant des intervenants ne sont pas généralisables à toute une population (Pleyers 2020).

Enfin, pour compléter la partie qualitative de ce mémoire, il aurait fallu obtenir la réponse favorable à une interview de la part d'une grosse organisation telle que la Commission Européenne, la CNIL ou encore l'Autorité de la Protection des Données. Cela aurait permis d'obtenir des informations plus complètes et d'avoir un point de vue encore différent, plus éloigné de celui des écoles, cette fois.

Chapitre 2 : Analyse des résultats

2.1. Hypothèse 1a

Les enseignants ont les connaissances et les compétences pour conscientiser les élèves à protéger leurs données personnelles.

Selon le directeur du Collège des Hayeffes, Monsieur Thomas Jadin, les enseignants ont des connaissances sur les données personnelles et le Règlement Général de la Protection des Données personnelles. Tous les enseignants ont accès à des données confidentielles et sont donc tenus par un secret professionnel. Avec le développement de la plateforme numérique Smartschool, ils sont encore plus confrontés à cela. *« En début d'année, les enseignants signent une adhésion à certains articles du RGPD. Chaque membre du personnel est donc sensibilisé à la question. »* Selon lui, *« cela doit transparaitre à travers les cours, mais certains cours plus que d'autres »*. Toutes ces questions d'éthique et de vie personnelle sont bien entendu plus facilement abordables dans des cours comme français ou religion plutôt que dans des cours de mathématiques. Les élèves interrogés confirment également que les professeurs abordent les sujets qui touchent aux données personnelles et à la vie privée dans leurs cours. *« Les profs en parlent, ils y font pas mal allusion »*, dit une élève. Dans une autre école, *« les profs nous en ont déjà parlé, mais surtout quand on était en début de secondaire », « de temps en temps les profs ouvrent un site devant nous et ils voient une page avec des cookies, ils nous soulignent de faire gaffe à ça mais nous n'avons jamais eu d'activité là-dessus pendant le cours »* expliquent certains élèves. Enfin, un autre élève raconte *« lors de mon examen d'audition en néerlandais, c'était sur les dangers d'internet et sur nos données personnelles »*. Tous ces témoignages d'élèves confirment bien que les enseignants du secondaire parlent de ce sujet dans leurs cours de temps en temps, sans créer une réelle activité dessus. Ils tentent de conscientiser les élèves avec leurs connaissances de base mais n'ont aucune formation là-dedans. Selon ces élèves, pour pouvoir vraiment les conscientiser, il faudrait une autre alternative que juste en parler de temps en temps car *« cela n'a pas beaucoup d'impact de parler de cela 10 minutes pendant un cours »* et *« ils ne nous apprennent pas beaucoup plus que ce que l'on sait déjà pour le moment »*.

Madame Virginie Tyou, auteure de « Cliky » confirme cela. Pour elle, il est urgent de former les professeurs et c'est ce qu'elle tente de faire en réalisant des formations essentiellement adressées aux écoles primaires pour le moment car *« la notion de l'intimité se développe chez les enfants à partir de 8 ans »* et que les données personnelles et la vie privée relèvent de l'intimité. De plus, *« à l'adolescence, on n'a plus envie d'écouter les bons conseils des parents »*.

et des enseignants ». Selon l'auteure, il leur manque principalement deux choses : d'une part, une formation technologique et, d'autre part, une formation psychopédagogique. Pour le premier argument, elle cite : « *Ils ne sont pas des pros du net et c'est normal !* » En effet, la majorité des enseignants n'a pas baigné dans le numérique dès la naissance. Il y a un écart générationnel entre les enseignants et les élèves en ce qui concerne le numérique, tant au niveau de l'utilisation des technologies que des perceptions de celles-ci (Dioni 2008).

En ce qui concerne le psychopédagogique, Virginie Tyou souligne que la méthode d'apprentissage du numérique est différente des méthodes d'enseignement basiques. « *Apprendre le numérique avec des règles, cela ne marche pas, ça c'est l'enseignement d'avant, le numérique c'est quelque chose qui doit être beaucoup plus pratique. Dans l'enseignement d'avant, on apprenait aux enseignants à maîtriser parfaitement leur matière, à tout savoir sur un sujet. Le numérique évolue tout le temps et il faut donc se mettre régulièrement à jour. C'est une démarche action-recherche. Il faut se poser des questions et chercher les meilleures informations possible, tout le temps* ». Elle appuie son argument en expliquant également que les professeurs ont été formés à éduquer mais pas à faire du psychologique et de l'accompagnement. « *Avec le numérique, de nouvelles compétences doivent être mises en place* » souligne Virginie Tyou qui insiste sur l'importance de former les enseignants au numérique, mais pas uniquement sous l'aspect technologique.

Selon l'auteure, les professeurs n'ont donc pas les connaissances requises pour enseigner le numérique et ils ne sont surtout pas formés correctement à enseigner une telle matière, « *il est donc primordial de former les enseignants au numérique et encore plus sur la manière dont ils vont conscientiser et former à leur tour leurs élèves* ». Comme déjà mentionné ci-dessus, « *apprendre le numérique avec des règles, cela ne marche pas* ». Lors de ses formations adressées aux enseignants, Virginie Tyou travaille donc aussi sur le processus d'apprentissage. Les enseignants, pédagogues, ont les clés de l'apprentissage et connaissent les étapes de ce processus. Le premier stade est l'attention que l'on porte à une matière, le deuxième est l'implication, le troisième est le retour sur erreur et le quatrième est la consolidation. « *C'est sur base de ces trois premières étapes que l'on peut consolider en se disant « qu'est-ce que je vais retenir de tout cela, qu'est-ce qui est essentiel pour moi de savoir ? » C'est à ce moment-là qu'on peut en tirer des règles de vie et de comportement* » explique Virginie Tyou. « *Pour le moment, les enseignants, lorsqu'ils en parlent, sont dans la dernière phase, la phase de consolidation mais sans passer par les 3 premières étapes* ». Et, selon elle, enseigner le

numérique simplement avec des règles, sans pratique et sans passer par les trois premières étapes, cela ne peut pas fonctionner.

2.2. Hypothèse 1b

L'école a un rôle à jouer dans l'éducation à la citoyenneté numérique des jeunes

En récoltant les opinions des différentes parties prenantes, l'école semble avoir un réel rôle à jouer dans l'éducation au numérique. Thomas Jadin, directeur, l'affirme : « *La révolution numérique qu'on est en train de vivre mériterait que les écoles se dotent de cours et de contenus* ». Il ajoute qu'« *éduquer au numérique devrait être présent dans les grilles d'horaire de tous nos élèves ... il y a un déficit d'accompagnement où chacun se débrouille un peu avec les moyens qu'il a* ».

Virginie Tyou partage cet avis et va même plus loin : « *Il faut parler aux enfants du numérique avant qu'ils soient adolescents. Il faut les familiariser quand ils ont 8-9 ans à la protection de leur intimité ; qu'est-ce que l'intimité, qu'est-ce que ma vie privée ; qu'est-ce qui est secret et qu'est-ce qui ne l'est pas ,...* ». Selon elle, l'école joue un rôle important et il faut commencer à éduquer les jeunes vers 8 ans, soit à l'école primaire.

Virginie Tyou argumente également ce fait que l'école a un réel rôle à jouer dans l'éducation au numérique, en comparant deux méthodes de conscientisation. D'une part, les formations que les jeunes pourraient recevoir dans une école, données par des intervenants externes, ou encore mieux par des professeurs formés, et d'autre part, les campagnes de prévention réalisées par des organisations ou des associations telles que Child Focus. « *Ce sont des campagnes de prévention mais ce n'est pas de l'éducation au numérique. Des animations d'une heure, même dans les écoles, que voulez-vous que ça change ?* » argumente-t-elle. Elle raconte également une anecdote sur sa fille à propos de ces campagnes de prévention : « *Ma fille a eu un jour une cyber-animation à l'école dans le cadre d'une campagne et elle m'a dit « c'était tellement horrible ce qu'ils racontaient sur les réseaux, que des gens nous observaient etc. et en fait on s'est tous dit , on n'écoute rien du tout ». Cela durait 50 minutes, comment voulez-vous faire en 50 minutes ?* »

L'auteure relève quand même un point positif, celui de l'évolution des mentalités dans les écoles. A l'heure de cette révolution numérique, beaucoup d'écoles lui demandent de venir former les enseignants et les enfants, ce qui n'était pas le cas il y a quelques années. Elle raconte que même les professeurs de maternelle souhaitent maintenant suivre des formations. « *Quand*

j'ai commencé en 2015, certaines écoles n'étaient pas du tout pour et me disaient qu'il ne fallait surtout pas parler de ça aux élèves sinon on allait les inciter à aller dessus ». Maintenant, les écoles sont conscientes qu'elles ont un réel rôle à jouer, comme l'avait expliqué le directeur Thomas Jadin, et certaines mettent des choses en place, en contactant, par exemple, des intervenants professionnels comme Virginie Tyou. Dans certaines écoles, les élèves ont déjà l'occasion d'avoir de petites formations sur certains sujets liés au numérique, animés par des partenaires externes. Le directeur Thomas Jadin cite par exemple : « En première, la police fédérale est venue expliquer à nos élèves ce qu'était le droit à l'image, le droit à l'intimité, au respect de la vie privée, aux dangers et menaces des réseaux sociaux. Une ASBL qui s'appelle ACBJ est venue informer les élèves de cinquième à propos des droits d'auteur et de la problématique de plagiat. C'est une question nouvelle due au déploiement du numérique ces dernières années. »

Les élèves interrogés sont du même avis quant au rôle que l'école joue dans l'éducation au numérique, *« l'école serait la meilleure solution, c'est là que ça aurait le plus d'impact », « l'école c'est mieux car sur internet il y a beaucoup de fake news ».*

Ils vont même plus loin en proposant des solutions à mettre en place dans les écoles. *« Avoir des formations avec un professionnel qui fait des chouettes activités cela peut être chouette, beaucoup plus qu'un prof qui nous parle de cela 10 minutes pendant un cours, cela aura plus d'impact. » « Comme on a les formations du planning familial, il faudrait avoir des formations quelques fois par an sur le numérique. » « Je suis d'accord, une formation pour sensibiliser plutôt que d'avoir un cours là-dessus. »*

Virginie Tyou suggère également cela *« quand j'étais petite, on avait des cours d'hygiène corporelle, on nous apprenait à bien nous laver les mains, qu'il fallait prendre une douche tous les jours, ... je dis qu'aujourd'hui, il faudrait des cours de base du numérique, qui commencent par savoir comment cela fonctionne, pourquoi on doit se protéger, ... ».*

Une autre élève ajoute également *« dans mon école, une nouvelle option a ouvert, sur l'écologie et la transition, donc pourquoi pas ouvrir un cours lié à ça ».* L'ouverture d'un cours sur la transition, hors programme scolaire habituel, est positif car cela veut dire qu'il y a du changement dans les écoles, une évolution.

L'auteure explique également qu'avec Cliky, la mascotte de son livre qui représente une donnée personnelle, on peut faire des statistiques dans le cadre du cours de mathématiques, en calculant, par exemple le pourcentage des enfants qui ont un ordinateur chez eux, une tablette ou un smartphone. On peut aussi travailler les compétences émotionnelles, l'intimité, ...

Cependant, le directeur soulève un point important, les écoles manquent considérablement de moyens et, en Belgique, la Fédération Wallonie-Bruxelles n'en donne aucun pour encadrer ce déploiement numérique. *« Tout directeur doit s'adapter, par exemple trouver un prof d'informatique qui n'a pas un horaire complet et lui donner quelques heures non chargées de cours. (...) Quand à l'intégration dans les programmes de cours, la Fédération dit qu'ils ne vont pas faire cela maintenant, on va attendre l'arrivée du tronc commun (prévue pour 2026). Mais le changement c'est maintenant. Il y a un manque de réactivité par rapport à la réalité que vivent les écoles parce que le virage numérique on est en plein dedans. »* Thomas Jadin suggère *« la reconnaissance d'un référent numérique dans chaque école »*.

2.3. Hypothèse 2a

Les parents ont les connaissances et les compétences pour conscientiser leur enfant à la protection des données personnelles

Les différents élèves adolescents interrogés ont donné leur ressenti face aux connaissances de leurs parents quant aux dangers d'internet et plus particulièrement par rapport à la protection des données personnelles. Cette interview a permis de constater que les parents manquent cruellement de connaissances par rapport aux données personnelles. Selon les adolescents interrogés, les parents savent qu'il y a un danger par rapport aux données, ils comprennent que leurs données sont utilisées, mais ils ne connaissent rien en profondeur et ne peuvent donc pas instruire et conscientiser pleinement leurs enfants à faire attention. *« Mes parents me disent de faire attention à mes informations, mais ils ne savent pas où vont nos informations, ils ne connaissent pas les mécanismes qui se cachent derrière cela »,* témoigne une élève. *« Ils m'ont déjà parlé des dangers d'internet et un peu sur les données personnelles, mais sur ce qu'ils savent, donc pas grand-chose »,* raconte une autre élève. *« On sait tous qu'il y a quelque chose mais sans savoir réellement quoi. On ne fait rien pour protéger nos données car on ne sait pas comment faire, ni nous, ni nos parents »,* ajoute un autre répondant. Un dernier appuie les arguments précédents en donnant un exemple concret : *« On a un groupe WhatsApp familial et ma mère souhaite qu'on utilise Signal à la place maintenant. Elle dit que c'est mieux pour nos données car c'est plus sécurisé mais elle ne sait pas nous dire pourquoi. Elle pense que comme ça n'appartient pas à Facebook, il y a moins de dangers mais c'est tout. »*

Selon Virginie Tyou, les parents ont de très grosses lacunes en ce qui concerne les risques sur internet et surtout en ce qui concerne les notions de vie privée, d'intimité, de protection des données.

Les enfants et les adolescents étant nés « dans le bain » d'internet, ils ont beaucoup plus de connaissances que leurs parents. Elle explique que lors de certains ateliers organisés pour des parents, certains ne savaient même pas d'où venait le Wifi. *« S'ils ne savent déjà pas ça, comment peuvent-ils savoir et comprendre les risques des données personnelles et de la vie privée sur internet ? »* se demande-t-elle.

Certains élèves confirment ces propos : *« Ma maman apprend en même temps que nous les risques. »* ou *« J'ai l'impression que notre génération est plus instruite que la leur. Mes parents, c'est parfois moi qui dois leur dire de faire attention. »* Pour Virginie Tyou, puisque les parents ont moins de connaissances que les enfants, il est super important de former les élèves à ce sujet dans les écoles. Elle justifie que *« comme les parents ne sont au courant de rien par rapport à cela, ça serait bien qu'il y ait une transmission de l'enfant vers son parent et qu'il y ait un vrai dialogue entre le parent, l'enfant et l'enseignant »*. L'enfant apporterait donc des connaissances supplémentaires à sa famille et à ses parents, très pauvres à ce sujet.

La plupart des parents ont peu de connaissances et si, selon quelques élèves, certains adultes ont quand même quelques notions plus approfondies, c'est grâce à leur travail. *« Mon père travaille dans un poste haut placé à la police, il contrôle le trafic de certaines choses qui se font sur internet et donc il a pas mal de notions dans le domaine, par contre ma maman apprend en même temps que nous. »* explique une élève. *« Mon parrain travaille dans la sécurité et a donc plus de connaissances. Par exemple, il m'avait dit qu'il ne publiait jamais des photos de ses enfants car elles pouvaient être réutilisées sur des sites illégaux. »* explique une autre.

Ces propos peuvent rejoindre ceux du directeur, Monsieur Jadin, qui expliquait avoir des notions sur la problématique des données personnelles en tant que directeur et que *« les enseignants signent une adhésion à certains articles du RGPD. Chaque membre du personnel est donc sensibilisé à la question »*, pense-t-il.

Sans connaissances, les parents sont incapables de transmettre celles-ci à leurs enfants. Pour la plupart d'entre eux, ils ne connaissent pas grand-chose et surtout rien en profondeur. *« Les adolescents connaissent plus que leurs parents. En ce qui concerne les enfants, certains ont également plus de connaissances »*. Virginie Tyou explique également qu'il n'y a pas de dialogue avec les enfants à ce sujet. Elle a pu le constater depuis qu'elle a lancé son activité, il

y a 6 ans. *« Cela fait 6 ans que je fais des formations dans les écoles à l'aide du personnage Cliky et quand je demande aux enfants la simple question « qu'est-ce qu'une donnée personnelle », au départ personne ne sait répondre correctement. »* C'est une preuve que les parents ne conscientisent pas leurs enfants à cela, même malgré le peu de connaissances qu'ils ont.

2.4. Hypothèse 2b

Les parents contrôlent l'utilisation du numérique par leurs enfants

Le contrôle parental est essentiel pour protéger les jeunes des risques engendrés par internet. Les parents ne montrent pourtant pas un intérêt très important pour le contrôle parental. D'après les adolescents interrogés, leurs parents se montrent peu préoccupés par le fait de contrôler ce qu'ils font sur internet. La plupart témoignent qu'ils contrôlaient un peu au tout début de leur adolescence mais cela s'arrête à cela : *« Lorsque je me suis inscrite sur les réseaux sociaux, ils m'ont bien entendu averti des dangers surtout pour ce que je poste dessus. » « Au début, ils contrôlaient nos téléphones, mais maintenant plus. Il y a juste mon frère qui, quand il veut télécharger des applications, a un mot de passe à mettre qui vient de mes parents, pour les achats. » « Ils me suivent sur Instagram pour regarder ce que je publie mais c'est tout .»*

Certains parents, provenant surtout de l'école primaire *« ne contrôlent rien du tout »* témoigne Virginie Tyou. Pourtant, à cet âge-là, il est primordial, en tant que parent, de contrôler ce que fait son enfant. Les parents et les enfants sont trop connectés et, dans beaucoup de familles, il n'y a aucune limite, ou très peu. Elle souligne que *« le niveau de connexion dépend du niveau socio-culturel des parents, plus il est bas, plus les enfants sont connectés. On pourrait croire le contraire, que dans des milieux plus aisés on donne facilement une tablette à l'enfant mais non. Les parents éduqués connaissent mieux les risques et ont une réflexion par rapport aux écrans et à internet, des règles sont installées »*. Selon Virginie Tyou, le contrôle et les règles sont donc liés au niveau d'éducation. Elle a pu le constater à de nombreuses reprises en Belgique et en France.

Lors de ses formations, la formatrice a constaté l'absence de contrôle parental avec de nombreux faits marquants qui engendrent des conséquences sur les enfants : *« Il y a des familles où plus personne ne se parle car ils sont tout le temps tous sur les écrans, même en mangeant. Des petits bouts de deux ans ne parlent toujours pas car leurs parents ne leur parlent pas, ils sont trop occupés à leurs écrans »*. Elle insiste sur le fait *« qu'il faut que les parents changent*

leurs pratiques, pour eux et surtout pour leurs enfants ». Par changements de pratiques, elle entend contrôler le temps d'écran, et ce, pour les parents également, mais aussi ce que les enfants font sur internet etc.

PARTIE 3 : ETUDES QUANTITATIVES

Dans cette partie se trouvent les résultats des deux enquêtes quantitatives, adressées aux enseignants du primaire et du secondaire, ainsi qu'aux parents d'enfants âgés entre 8 et 18 ans. L'étude quantitative permet d'obtenir des résultats fiables, précis et généralisables à une population étudiée (Weinreich 1996). Elle permet de collecter des informations spécifiques telles que les attitudes, les motivations, les comportements ou les caractéristiques démographiques (Pleyers 2020).

Chapitre 1 : Méthodologie

1.1. Conception des questionnaires

Le questionnaire est l'un des éléments primordiaux de l'enquête puisqu'il constitue un outil d'enregistrement et de stockage des informations (Vandercammen & Gauthy-Sinéchal 2014). Il a été créé de manière à ce que les répondants n'abandonnent pas avant la fin. Pour cela, les mots utilisés doivent être simples et les questions ne doivent pas être complexes à comprendre, ni répétitives. Le style d'écriture choisi doit être le plus clair possible et les questions ne doivent pas influencer les internautes dans leur réponse (Pleyers 2020).

Les deux questionnaires (voir annexe 2) sont structurés de la même manière, avec la technique de l'entonnoir, qui consiste à poser des questions générales au début et à poser par la suite des questions plus spécifiques (Pleyers 2020). Le questionnaire débute par quelques phrases d'introduction pour présenter l'interviewer, pour motiver les répondants à répondre aux questions et pour présenter le thème de l'enquête et son utilité. Il est structuré en différentes sections afin d'aider les répondants à remplir celui-ci. La première section comporte une question filtre. Elle permet de s'assurer que les répondants correspondent bien aux critères de sélection de l'enquête (Pleyers 2020). La deuxième section comprend quelques questions pour évaluer les connaissances des internautes sur le sujet. La troisième section contient des questions plus spécifiques, relatives à la capacité des enseignants ou des parents à pouvoir transmettre des connaissances à leurs élèves ou à leurs enfants. La quatrième section s'intéresse au point de vue des enseignants quant au rôle joué par l'école dans l'éducation numérique. Pour les parents, la quatrième section s'intéresse aux contrôles mis en place pour leurs enfants par rapport au numérique. Enfin, la dernière section comprend les caractéristiques

sociodémographiques de l'échantillon. Ces questions, d'ordre plus personnel, sont posées à la fin pour éviter que certains répondants ne renoncent à y répondre. Toutes les questions posées sont des questions fermées.

1.2. Choix des échantillons

La technique d'échantillonnage utilisée est la même pour les deux enquêtes. La technique est celle de l'effet boule de neige, une méthode non-probabiliste. Cette technique de l'effet boule de neige consiste à identifier un petit groupe d'individus avec des caractéristiques spécifiques qui vont à leur tour inviter d'autres personnes ayant les mêmes caractéristiques (Pleyers 2020). Le choix de l'échantillon de la première enquête s'est porté sur les enseignants du primaire et du secondaire car les jeunes internautes qu'il faut éduquer à la protection de leurs données personnelles ont entre 8 et 18 ans et sont donc des élèves d'écoles primaires ou secondaires. Le choix du deuxième échantillon s'est porté sur les parents d'enfants âgés entre 8 et 18 ans.

En effet, une étude réalisée par Themis en 2021 a montré que 98% des 8 – 11 ans avaient accès à un écran chez eux. 50% d'entre eux possèdent leur propre téléphone dont 25% possèdent en plus une tablette ou un ordinateur. Quant à l'utilisation des réseaux sociaux, qui est légalement interdite avant 13 ans, 54% d'entre eux possèdent un compte TikTok. En ce qui concerne l'âge limite pris en compte, il est justifié par la fin de l'autorité parentale, lorsque l'enfant a 18 ans.

1.3. Pré-tests

Le pré-test est la dernière étape avant de pouvoir envoyer ou donner le questionnaire aux répondants. Il consiste à tester le questionnaire auprès de quelques personnes afin d'identifier les erreurs potentielles, de vérifier la compréhension des questions, la formulation des phrases ou encore la durée du questionnaire (Pleyers 2020).

Les pré-tests ont été réalisés auprès de 5 personnes et ont permis de détecter certaines erreurs. Pour commencer, un répondant a testé la question filtre en cochant la réponse non adéquate et le questionnaire n'a pas pris fin. De plus, certaines questions définies comme obligatoires ne devaient pas l'être. Ensuite, certaines questions ont été reformulées de manière à faciliter leur compréhension. Certains répondants ont également souligné qu'il était préférable de modifier une question ne présentant qu'un seul choix de réponse en y ajoutant la possibilité de cocher plusieurs réponses. Enfin, ce pré-test a permis de relever quelques fautes d'orthographe.

1.4. Matrices Hypothèses/ questions

Matrice enseignants :

	H1a	H1b	Analyse de l'échantillon
Q1	Question filtre		
Q2	X		
Q3	X		
Q4	X		
Q5	X		
Q6	X		
Q7			
Q8	X	X	
Q9	X	X	
Q10			
Q11			
Q12		X	
Q13			
Q14		X	
Q15			X
Q16			X
Q17			X
Q18			X

Matrice parents :

1.	H2a	H2b	Analyse de l'échantillon
Q1	Question filtre		
Q2	Question filtre		
Q3		X	
Q4	X		
Q5	X	X	
Q6	X	X	
Q7	X		
Q8	X		

Q9		X	
Q10	X		
Q11	X		
Q12	X		
Q13	X		
Q14	X		
Q15	X		
Q16	X		
Q17		X	
Q18		X	
Q19		X	
Q20			X
Q21			X
Q22			X
Q23			X

1.5. Distribution des questionnaires

Les questionnaires ont été conçus via un Google Form et ont été distribués via les réseaux sociaux ainsi que par mail durant 6 jours, au cours du mois de novembre 2021. Les questionnaires ont été diffusés à des internautes ayant des profils différents selon l'âge, le sexe, le niveau d'éducation ou encore la profession, de façon à ce que l'échantillon soit le plus représentatif possible.

Cette méthode de collecte de données, en ligne, a été privilégiée car l'enquête concerne des personnes qui utilisent internet. De plus, cette méthode présente de nombreux avantages. Premièrement, elle permet d'atteindre un grand nombre de personnes rapidement et à faible coût. Elle permet également de contrôler l'ordre des questions et d'enregistrer automatiquement les réponses. Le traitement automatique des réponses permet de constater directement les résultats et de réajuster éventuellement par la suite l'envoi du questionnaire à certaines personnes selon les critères sociodémographiques. Par exemple, si les trois quarts des répondants sont des hommes, le questionnaire peut être envoyé à des femmes pour avoir un échantillonnage complet (Pleyers 2020).

Cependant, cette méthode présente tout de même certaines limites. Premièrement, la représentativité de l'échantillon peut parfois être biaisée, surtout si l'interviewer diffuse son questionnaire auprès de ses connaissances (Pleyers 2020). Ensuite, comme il n'y a pas d'interviewer pour aider les répondants à la compréhension des questions, ceux-ci peuvent plus facilement abandonner l'enquête. De plus, sans interviewer, il n'y a pas de contrôle d'identité des répondants, ce qui est moins fiable (Pleyers 2020).

Chapitre 2 : Analyse des résultats

2.1. Préparation des données

Pour les deux questionnaires, les données ont été exportées du Google Form vers Microsoft Excel. Il est recommandé de transférer les données sur ce logiciel afin de pouvoir correctement préparer les données avant de les envoyer vers le logiciel SPSS (Weiss & Townsend, 2005). La base de données initiale comprenait 45 répondants mais, avec la question filtre, une personne ne correspondant pas à la cible n'a pas pu poursuivre la réponse au questionnaire. La ligne de ce répondant a été supprimée. La colonne « horodateur », provenant automatiquement de Google Form, a également été supprimée. L'étape suivante consistait à simplifier le nom des variables et à transformer les valeurs nominales en valeurs numériques afin de les exploiter plus facilement dans le logiciel SPSS (voir annexe 3). Finalement, toutes les données provenant d'Excel, ont été exportées vers le logiciel SPSS.

2.2. Description des échantillons

2.2.1. Echantillon enseignants

L'échantillon final est composé de 44 répondants dont 79,5% de femmes et 20,5% d'hommes. Quatre catégories d'âge ont été créées et chacune d'elle est représentée : les 20 – 30 ans, les 31 – 40 ans, les 41 – 50 ans et les 51 ans et +. La catégorie la plus importante est celle des 41- 50 ans (40,9%). En ce qui concerne le type d'enseignement, 62,8% des enseignants interrogés travaillent dans une école secondaire et 31,2% dans une école primaire. Seulement 6,8% des enseignants, primaire et secondaire confondus, sont des professeurs d'informatique. 100% des répondants savent ce qu'est une donnée personnelle et utilisent les grandes plateformes telles que Facebook, Amazon ou Google. 84,4% les utilisent au moins deux fois par jour.

Avant d'analyser les résultats, il est essentiel d'analyser la représentativité de l'échantillon afin de ne pas extrapoler ou inférer des résultats obtenus auprès d'un échantillon à la population totale. De plus, cette représentativité de l'échantillon va apporter un poids supplémentaire aux résultats obtenus (Jourdan 2008). La représentativité de l'échantillon a ici été évaluée par rapport à sa population cible, c'est-à-dire les enseignants belges du primaire et du secondaire.

Pour commencer, un test binomial a été réalisé afin de déterminer si la proportion d'observations (échantillon) en fonction du genre correspondait à la proportion donnée (de la population). L'hypothèse nulle signifie que les effectifs observés correspondent aux effectifs de la population, donnés par la Fédération Wallonie-Bruxelles.

Binomial Test						
		Category	N	Observed Prop.	Test Prop.	Exact Sig. (1-tailed)
Genre	Group 1	1	35	,80	,75	,309
	Group 2	2	9	,20		
	Total		44	1,00		

Figure 2 : Test binomial pour le genre

La p-valeur est supérieure à 0,05 (0,309) ce qui signifie que l'hypothèse H_0 n'est pas rejetée et que l'échantillon est représentatif de la population cible en ce qui concerne le genre. En effet, 75% des enseignants du primaire et du secondaire sont des femmes et l'échantillon est constitué de 79,1% de femmes enseignantes.

Un autre test binomial a été réalisé afin de déterminer si la proportion d'observations (l'échantillon) correspondait à la proportion donnée en ce qui concerne le type d'enseignant, c'est-à-dire du primaire ou du secondaire. L'hypothèse nulle signifie que les effectifs observés correspondent aux effectifs de la population, donnés par la Fédération Wallonie-Bruxelles.

NPar Tests						
[DataSet1]						
Binomial Test						
		Category	N	Observed Prop.	Test Prop.	Exact Sig. (1-tailed)
Type d'enseignement	Group 1	1	14	,32	,48	,022 ^a
	Group 2	2	30	,68		
	Total		44	1,00		

a. Alternative hypothesis states that the proportion of cases in the first group < ,48.

Figure 3 : Test binomial pour le type d'enseignant

La p-valeur est inférieure à 0,05 (0,022) ce qui signifie que l'hypothèse H_0 est rejetée et que l'échantillon n'est donc pas représentatif de la population cible en ce qui concerne le type d'enseignant. Dans ce cas-ci, la catégorie des enseignants du secondaire est plus représentée (68,2%) que celle des enseignants du primaire alors qu'en réalité, selon la Fédération Wallonie-Bruxelles, parmi les enseignants du primaire et du secondaire, 51,76% sont des enseignants du secondaire.

Enfin, un test d'ajustement Chi-carré a été réalisé afin de tester si la proportion d'observations (l'échantillon) en fonction des différentes catégories d'âge correspondait à la proportion donnée. L'hypothèse nulle signifie que les effectifs observés correspondent aux effectifs de la population donnés par la Fédération Wallonie-Bruxelles.

Âge					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	18,2	18,2	18,2
	2	10	22,7	22,7	40,9
	3	18	40,9	40,9	81,8
	4	8	18,2	18,2	100,0
Total		44	100,0	100,0	

Test Statistics	
Âge	
Chi-Square	4,651 ^a
df	3
Asymp. Sig.	,199
a. 0 cells (0,0%) have expected frequencies less than 5. The minimum expected cell frequency is 7,1.	

Figures 4 : Test d'ajustement Chi-carré pour les catégories d'âge

La p-valeur observée est supérieure à 0,05 (0,199) ce qui signifie que l'hypothèse H_0 n'est pas rejetée et que l'échantillon est représentatif de la population cible en ce qui concerne les catégories d'âge.

En conclusion, l'échantillon est assez représentatif. En ce qui concerne la différence entre les types d'enseignants du primaire et du secondaire, cela peut s'expliquer par le fait que l'échantillon soit non-probabiliste, d'effet « boule de neige » et que le questionnaire ait été envoyé à des proches, surtout enseignants du secondaire, qui ont à leur tour fait passer le questionnaire à leurs collègues, principalement du secondaire également.

2.2.2. Echantillon parents

L'échantillon final est composé de 68 personnes, dont 52,9% de femmes et 47,1% d'hommes. Quatre catégories d'âges ont été créées et chacune d'elle est représentée : les 25 – 35 ans, les 36 – 45 ans, les 46 – 55 ans et les + de 55 ans. Les deux catégories les plus importantes sont

celle des 36 - 45 ans (33,8%) et celle des 46 – 55 ans (39,7%). En ce qui concerne le niveau d'études des parents, la plupart d'entre eux ont réussi des études supérieures, dont 36,8% de type court et 39,7% de type long. Enfin, plus de la moitié des répondants sont des employés (52,9%), les indépendants (20,6%) et les dirigeants d'entreprise (17,6%) sont les deux catégories suivantes à être le plus représentées. Tous les répondants possèdent un smartphone ou ordinateur et pour 86,8% d'entre eux, leur enfant possède également un ordinateur ou un smartphone. Enfin, 100% des parents interrogés savent ce qu'est une donnée personnelle et utilisent les grandes plateformes telles que Facebook, Amazon ou Google. 76,47% les utilisent au moins deux fois par jour.

Pour commencer l'analyse de la représentativité de l'échantillon, un test binomial a été réalisé afin de savoir si la proportion d'observations en fonction du genre correspondait à la proportion donnée. L'hypothèse nulle signifie que les effectifs observés correspondent aux effectifs de la population, donnés par Statbel.

Binomial Test						
		Category	N	Observed Prop.	Test Prop.	Exact Sig. (1-tailed)
GENRE	Group 1	1	36	,53	,51	,422
	Group 2	0	32	,47		
	Total		68	1,00		

Figure 5 : test binomial pour le genre

La p-valeur est supérieure à 0,05 (0,422) ce qui signifie que l'hypothèse H_0 n'est pas rejetée et que l'échantillon est représentatif de la population cible en ce qui concerne le genre. En effet, la proportion de femmes dans la population belge est de 51% et elle est de 53% dans l'échantillon.

Ensuite, un test d'ajustement Chi-carré a été réalisé afin de tester si la proportion d'observations (l'échantillon) en fonction des différentes catégories d'âge correspondait à la proportion donnée.

Chi-Square Test			
Frequencies			
AGE			
	Observed N	Expected N	Residual
1	12	16,7	-4,7
2	27	16,8	10,2
3	23	17,3	5,7
4	6	17,3	-11,3
Total	68		

Test Statistics	
AGE	
Chi-Square	16,807 ^a
df	3
Asymp. Sig.	<,001

Figures 6 : Test d'ajustement Chi-carré pour les catégories d'âge

Puisque la p-valeur est bien inférieure à 0,05, l'hypothèse H_0 est rejetée et l'échantillon n'est donc pas significatif. Les données utilisées pour tester la représentativité de l'échantillon sont celles correspondant à toute la population belge par tranches d'âge et pas uniquement aux parents d'enfants âgés entre 8 et 18 ans. Vu le manque de données correspondant aux critères de sélection de l'échantillon, il n'était pas possible d'évaluer cela correctement.

Catégorie d'âge	Échantillon	Population belge
25 – 35 ans	17,7%	24,54%
36 – 45 ans	39,79%	24,66%
46 – 55 ans	33,8%	25,40%
+ de 55 ans (56 – 65 ans)	8,8%	25,39%

Cependant, il est important de relever que peu de parents ont encore un enfant après 45 ans, il apparaît donc normal que la dernière tranche d'âge soit beaucoup moins représentée dans l'échantillon. En ce qui concerne la première catégorie, c'est-à-dire les 25 – 35 ans, la proportion de l'échantillon est moins élevée que celle de la population, la moyenne d'âge d'une mère donnant naissance à son premier enfant étant de 29 ans en Belgique. Il y a donc moins de jeunes parents ayant déjà un enfant de 8 ans dans cette catégorie. En tenant compte de ces arguments, l'échantillon pourrait être considéré comme représentatif de sa population.

2.3. Résultats

Avant de commencer l'analyse des résultats, il est essentiel de souligner que certains tests se sont montrés non-significatifs, probablement en raison de la petite taille de l'échantillon (44 répondants) et de sa distribution, le questionnaire ayant été distribué principalement à des personnes proches et à leur entourage. Cet échantillon ne peut donc pas être considéré comme un échantillon aléatoire. Cependant, certains tests se sont quand même révélés significatifs et certaines questions ont apporté des réponses très claires ne nécessitant pas une analyse dans SPSS. L'analyse des résultats s'est donc montrée relativement complète, malgré le manque de significativité de certains tests.

2.3.1. Hypothèse 1a

Les enseignants ont les connaissances et les compétences pour conscientiser les élèves à protéger leurs données personnelles.

Premièrement, l'étude réalisée auprès des enseignants a permis de constater que 100% des répondants savent ce qu'est une donnée personnelle. 95,3% d'entre eux savent également que les plateformes collectent leurs données sans leur réel consentement et que celles-ci les revendent à des entreprises qui les utilisent principalement à des fins publicitaires.

Il est important de relever que 86% des répondants utilisent ces grandes plateformes au moins 2, 3 voire 4 fois par jour (voir annexe 4).

Bien que la majorité des enseignants ait répondu savoir que leurs données étaient collectées, seulement 25,6% de l'échantillon pensent avoir les connaissances nécessaires pour sensibiliser les élèves à ce sujet et à la protection de leurs données personnelles. Quant à la capacité de pouvoir eux-mêmes expliquer aux élèves comment faire pour protéger leurs données, ils ne sont que 20% à se sentir capables de le faire (voir annexe 5).

Certains professeurs interrogés ont déjà suivi des formations à ce sujet. Afin de vérifier si les formations aidaient à avoir plus de connaissances par rapport à cela, un test d'indépendance Chi-carré a été réalisé et celui-ci s'est montré significatif. La p-valeur étant inférieure à 0,05, l'hypothèse H_0 a été rejetée, ce qui a permis d'affirmer qu'il y a bien un lien significatif entre le fait de suivre des formations sur les données personnelles et d'avoir des connaissances à ce sujet. Un autre test a été effectué pour voir si le fait d'avoir suivi des formations avait un lien significatif avec le fait de se sentir capable de pouvoir expliquer et montrer aux élèves comment protéger leurs données personnelles. Malheureusement la p-valeur étant supérieure à 0,05,

l'hypothèse H_0 n'a pas pu être rejetée et il n'y a donc pas de lien entre ces deux variables (voir annexe 6).

Une autre information pertinente à relever est celle qui concerne les professeurs d'informatique. Bien qu'il n'y ait que 3 professeurs d'informatique représentés dans l'échantillon, ce qui n'est donc pas très représentatif, les résultats peuvent tout de même être interprétés pour appuyer l'hypothèse. Deux tests Chi-carré ont été réalisés, d'une part, pour déterminer s'il y avait un lien entre le fait d'être professeur d'informatique et d'avoir les connaissances pour conscientiser les élèves et, d'autre part, pour vérifier si le fait d'être professeur d'informatique avait un lien avec la capacité à expliquer et à montrer aux élèves comment protéger leurs données personnelles. Les deux tests se sont révélés significatifs. Dans les deux cas, la p-valeur était inférieure à 0,05 et les hypothèses H_0 ont donc été rejetées (voir annexe 7).

55,9% des répondants disent avoir déjà discuté du sujet des données personnelles lors de leur cours. Un test a donc été réalisé pour déterminer s'il y avait un lien entre le fait d'avoir des connaissances à ce sujet et le fait d'en avoir parlé durant un cours. Le test s'est révélé significatif. La p-valeur étant inférieure à 0,05, l'hypothèse H_0 a été rejetée (voir annexe 8).

Enfin, concernant le type d'enseignement, à savoir primaire ou secondaire, aucun test ne s'est révélé significatif pour cette hypothèse. Il n'y a donc aucun lien significatif entre le fait d'être enseignant en primaire ou en secondaire et le fait d'avoir suivi des formations, d'avoir des connaissances à ce sujet pour conscientiser les élèves ou encore le fait de se sentir capable d'expliquer aux élèves comment protéger leurs données personnelles.

2.3.2. Hypothèse 1b

L'école a un rôle à jouer dans l'éducation à la citoyenneté numérique des jeunes

Premièrement, 97,7% des répondants pensent que l'école a un rôle à jouer dans l'éducation au numérique. De plus, 97,7% d'entre eux pensent que les parents n'éveillent pas assez les enfants et les adolescents à cela, ce qui renforce l'avis que l'école a un rôle-clé dans l'éducation au numérique. La réponse à ces deux questions est déjà très significative. Quelle que soit la catégorie d'âge, le genre ou encore le type d'enseignant (primaire ou secondaire), l'école a un rôle à jouer selon eux (voir annexe 9).

Puisque cette hypothèse est vraie, il est également important de comprendre comment l'école peut jouer ce rôle. Les professeurs ont ainsi dû recommander les moyens qui devraient être mis

en place afin d'éduquer les élèves au numérique de la meilleure des façons. Le meilleur moyen, selon 86% des répondants, est de le faire sous forme d'une activité ludique à l'école. Un test Chi-carré a été réalisé pour voir s'il y avait un lien significatif entre le type d'enseignant et le fait de mettre en place des activités ludiques. Il s'est révélé significatif. En effet, les professeurs de primaire, à l'unanimité, souhaitent mettre en place une activité ludique afin de conscientiser leurs élèves à protéger leurs données personnelles et de les éveiller sur les risques liés à cette problématique (voir annexe 10).

Les enseignants interrogés, étant pour la quasi-totalité persuadés que l'école a un rôle à jouer dans l'éducation au numérique, sont 55,9% à avoir déjà discuté de la protection des données personnelles et des risques avec leurs élèves. Parmi eux, 62,5% ont répondu l'avoir fait « par hasard », au détour d'une conversation, tandis que les 37,5% autres ont organisé une activité à ce propos (voir annexe 11).

2.3.3. Hypothèse 2a

Les parents ont les connaissances et les compétences pour conscientiser leur enfant à la protection des données personnelles

Premièrement, il est important de souligner que 100% des répondants savent ce qu'est une donnée personnelle et utilisent les grandes plateformes telles que Facebook, Amazon, Google. 98,9% d'entre eux les utilisent quotidiennement dont 76,74% plusieurs fois par jour. Une autre donnée importante à relever est que 88,2% savent que leurs données sont collectées et revendues à des entreprises qui les utilisent principalement à des fins commerciales (voir annexe 12).

En ce qui concerne la façon dont ils ont appris ces mécanismes de collecte de données, 26,5% des répondants s'en rendent compte en apercevant sans cesse des pubs bannières sur des sujets qui les intéressent. 20,6% l'ont appris par le bouche-à-oreille et 19,1% par les médias suite à l'explosion de scandales (voir annexe 13).

Un constat à propos des connaissances des parents est assez interpellant. 63,2% d'entre eux disent ne pas avoir les connaissances nécessaires pour éveiller leurs enfants à la protection de leurs données personnelles. Pourtant, comme cité ci-dessus, 88% savent que leurs données sont collectées pour être revendues à des fins publicitaires (voir annexe 14).

Pour comprendre qui, dans l'échantillon de parents, a les connaissances nécessaires pour éveiller les enfants aux risques et à la protection des données personnelles, un premier test Chi-carré a été réalisé. Celui-ci avait pour but de déterminer s'il existait un lien entre le fait d'avoir des connaissances à ce sujet et le niveau d'études des répondants. Ce test s'est avéré significatif. La p-valeur étant inférieure à 0,05, l'hypothèse H_0 a pu être rejetée. Un autre test a été réalisé pour vérifier si le niveau d'études avait aussi un lien avec la capacité des parents à expliquer et montrer à leurs enfants comment se protéger face aux risques de cette problématique. Ce deuxième test s'est révélé significatif. Dans les deux cas, c'est-à-dire tant pour les connaissances que pour la capacité à expliquer, le niveau d'études a un lien significatif avec ces deux variables (voir annexe 15).

Pour aller plus loin, deux autres tests ont été réalisés en liant à nouveau, d'une part les connaissances et d'autre part, la capacité à pouvoir expliquer, avec le statut des répondants, à savoir leur métier. Dans les deux cas, les tests ont été significatifs. La p-valeur étant inférieure à 0,05, les hypothèses H_0 ont pu être rejetées. Le métier a donc un lien avec ces deux variables (voir annexe 16).

Enfin, 69,1% des parents disent avoir déjà sensibilisé leur enfant à cette problématique (voir annexe 17). Les tests liés à cette variable réalisés pour prouver l'hypothèse ne se sont pas montrés significatifs. Cependant, sur le tableau ci-dessous, il ressort que, parmi tous les répondants ayant des connaissances sur le sujet, un seul n'en a pas déjà parlé à son enfant.

CONN * SENS Crosstabulation

Count

		SENS		
		0	1	Total
CONN	0	20	23	43
	1	1	24	25
Total		21	47	68

Figure 7 : Test Chi-carré sur les connaissances et la sensibilisation

2.3.4. Hypothèse 2b

Les parents contrôlent l'utilisation du numérique par leurs enfants

Premièrement, 27,9% ont mis en place un logiciel de contrôle parental chez leurs enfants.

Un premier test, test t pour échantillons indépendants, a été réalisé afin de vérifier si le contrôle parental et l'âge des parents avaient un lien et ce test s'est avéré significatif (voir annexe 18). Sur le graphe ci-dessous, il en ressort même que les jeunes parents ont plus tendance à mettre en place un contrôle parental que les parents plus âgés.

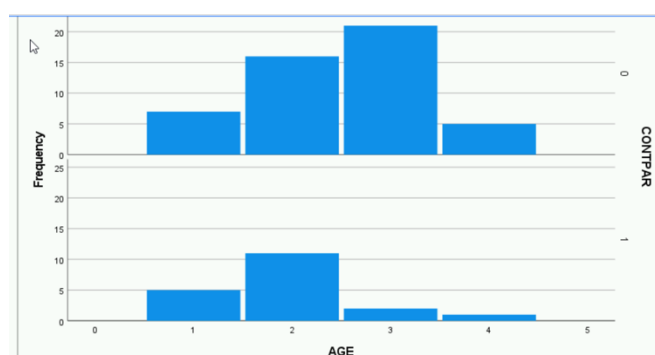


Figure 8 : Histogramme sur le contrôle parental et les catégories d'âge

Ensuite, un autre test Chi-carré d'indépendance a été réalisé pour déterminer s'il y avait un lien entre la peur et le mise en place du contrôle parental. Celui-ci s'est avéré significatif. La p-valeur étant inférieure à 0,05, l'hypothèse H_0 a pu être rejetée. Cependant, 33 répondants qui se disent inquiets n'ont pas mis en place de contrôle parental (voir annexe 19).

Afin de constater l'importance de certains contrôles qui devaient être mis en place par les parents ou qui le sont vraiment, ceux-ci ont dû évaluer l'importance qu'ils accordaient à certains contrôles et puis cocher ceux qu'ils contrôlaient vraiment. Des tests Chi-carré d'indépendance ont été réalisés afin de déterminer s'il y avait un lien entre l'importance qu'accordaient les parents à un type de contrôle et le fait de mettre en place un vrai contrôle. La quasi-totalité des tests s'est révélée significative. Le plus intéressant ici est d'analyser les tableaux où sont croisées les données. En ce qui concerne le temps d'écran, les résultats paraissent très logiques car les parents qui accordent le moins d'importance à cela ne contrôlent pas et ceux qui y accordent beaucoup d'importance ont mis en place un contrôle. A propos des sites fréquentés, sur les 66 répondants trouvant ce facteur important et très important, la moitié d'entre eux seulement contrôle les sites fréquentés par leurs enfants. Du point de vue des réseaux sociaux, 17 parents contrôlent cette variable sur les 48 répondants qui y accordent de l'importance ou

beaucoup d'importance. Enfin, concernant les achats en ligne, la proportion est moindre, un tiers des répondants disant y accorder de l'importance ne met pas en place de contrôle (voir annexe 20).

Enfin, d'autres tests ont été réalisés afin de déterminer s'il existait un lien entre le niveau d'études des parents et la mise en place d'un contrôle parental général ou la mise en place de contrôles ciblés (sites fréquentés, le temps d'écran, ...). Ces tests se sont tous montrés non-significatifs. Ces mêmes variables ont été reprises pour voir s'il existait éventuellement un lien avec le métier des répondants mais ils se sont également avérés non-significatifs.

PARTIE 4 : DISCUSSION

4.1. Interprétation des résultats

Grâce aux enquêtes qualitatives et quantitatives, de nombreuses données ont été collectées et analysées. Premièrement, tant chez les parents que chez les enseignants, ils sont plus de 88% à savoir que leurs données sont collectées par de grandes plateformes et revendues à des entreprises. Pourtant, la grande majorité de ceux-ci (au moins 76%) utilise ces plateformes plusieurs fois par jour. Ceci confirme bien la littérature scientifique et la notion du Privacy Paradoxe (Barnes 2006).

En ce qui concerne les enseignants, les résultats de l'enquête quantitative montrent que seulement 25,6% pensent avoir les connaissances nécessaires pour sensibiliser les élèves à la protection de leurs données personnelles. Et seulement 20% d'entre eux se sentent capables d'expliquer aux élèves comment protéger ses données personnelles. Pourtant, ils étaient 95,3% à savoir que leurs données étaient collectées sans leur réel consentement et ensuite utilisées à des fins publicitaires, par exemple.

Malgré ce constat, selon Thomas Jadin, directeur d'une école secondaire, les enseignants sont sensibilisés à la question puisqu'en début d'année, notamment, ils signent une adhésion à certains articles du RGPD. Toujours selon ce directeur, ils abordent cette problématique dans leurs cours. Les élèves ont confirmé, pour la plupart, avoir déjà discuté de ce sujet pendant les cours, sans avoir une réelle activité consacrée à cela. Les résultats de l'enquête quantitative indiquent un résultat semblable. En effet, plus de la moitié des professeurs ont déjà discuté de cette problématique avec leurs élèves et parmi eux, 66% l'ont fait par hasard, au détour d'une conversation. Toujours selon les élèves, bien qu'ils en discutent, les connaissances des enseignants sont cependant limitées et ils n'apprennent pas le fond du problème. Les résultats de l'enquête quantitative présentés plus haut confirment les dires des élèves.

Virginie Tyou, l'auteure et conférencière, confirme que les enseignants n'ont pas les connaissances requises pour enseigner le numérique. Selon elle, il leur manque deux éléments importants. D'une part, les enseignants ne sont pas nés dans l'ère numérique, ils ont donc des lacunes technologiques. D'autre part, le numérique ne s'enseigne pas de la même façon que les autres matières du programme scolaire, il ne s'apprend pas avec des règles mais plutôt par de la pratique. Les enseignants doivent donc développer de nouvelles méthodes d'apprentissage

pour former les élèves au numérique. Il leur manque donc également les compétences psychopédagogiques et il est important de les former à cela. La littérature confirme cela. Les enseignants n'ont en effet pas toutes les compétences requises pour enseigner le numérique. Selon Bruillard et Baron (2006), l'enseignement du numérique repose sur trois compétences : la technique, la didactique et la pédagogie. Les enseignants doivent accompagner les élèves dans le changement, compétence à laquelle ils ne sont pas formés à la base. Pour pouvoir enseigner le numérique correctement, les profs souhaitent se former, mais pas uniquement sur les aspects techniques (Dioni 2008).

En ce qui concerne les formations sur cette thématique, certains d'entre eux ont déjà eu l'occasion d'y participer mais malheureusement, aucun lien significatif n'a pu être établi entre le fait d'être capable d'expliquer aux élèves comment protéger ses données personnelles et le fait d'avoir participé à des formations. Il est donc important de noter que, pour le moment, les formations ne sont pas efficaces.

Tous ces arguments, permettent de confirmer que les enseignants manquent en effet de connaissances, tant techniques que psychopédagogiques, pour enseigner le numérique et tous les risques qui l'accompagnent aux élèves. **L'hypothèse 1a est donc rejetée.** Cependant, un bon nombre d'enseignants est conscient de cette problématique et tente, malgré les lacunes dans ce domaine, d'en parler aux élèves pour les y éveiller.

Aborder le numérique au détour de discussions est une preuve que les enseignants pensent avoir un rôle à jouer dans l'éducation au numérique. 97% des professeurs interrogés ont d'ailleurs répondu positivement à cette question. Le directeur, Thomas Jadin, a affirmé que l'éducation au numérique devrait se trouver dans les grilles horaires. Pour lui, nul doute que l'école a un rôle à jouer. La seconde intervenante, Virginie Tyou, ajoute même qu'il faudrait commencer à éduquer les élèves dès l'âge de 8 ou 9 ans, donc à l'école primaire. En discutant avec les élèves, ceux-ci ont également confirmé que l'école avait un rôle à jouer. Selon eux, l'école aurait beaucoup plus d'impact que les parents dans l'éducation au numérique. Les propos des différents intervenants sont en lien avec la littérature. En effet, les enseignants reconnaissent l'influence des technologies sur les enfants et assument leur rôle à jouer dans l'apprentissage de l'utilisation appropriée de ces nouvelles technologies (Lauricella et al. 2010).

Tous les intervenants et les résultats de l'étude quantitative auprès des enseignants confirment donc que l'école a bien un rôle clé à jouer dans l'éducation au numérique et **l'hypothèse 1b n'est donc pas rejetée.**

Différents moyens peuvent être mis en place pour intégrer l'éducation au numérique dans les écoles. Les élèves du secondaire interrogés suggèrent, par exemple, qu'un intervenant externe, puisque selon eux les professeurs n'ont pas les connaissances requises, organise des activités autour de cette thématique quelques fois sur l'année. Selon Virginie Tyou et le Thomas Jadin, il faudrait même instaurer un cours à ce sujet dans le programme scolaire car étant dans l'ère numérique, cette problématique est de plus en plus importante, comme tout ce qui touche au numérique. La littérature scientifique a d'ailleurs souligné le manque de cyberculture des utilisateurs pour toutes les questions relatives à la protection des données personnelles mais aussi aux notions de hacking, par exemple (Chan & Virkki, 2014). La question des méthodes à mettre en place pour éduquer les jeunes a également été posée aux enseignants lors de l'enquête. C'est la mise en place d'activités ludiques à l'école qui a remporté le plus de suffrages (86%) et même l'unanimité chez les professeurs de primaire. 62% des répondants pensent qu'il faut intégrer l'éducation le numérique dans un cours donné à tous les élèves et 48,8% suggèrent des conférences données à l'école par des professionnels.

En ce qui concerne les connaissances des parents, il a été relevé précédemment que la grande majorité d'entre eux utilisait plusieurs fois par jour les grandes plateformes et savait que celles-ci collectaient et utilisaient leurs données. Pourtant, un quart (26,25%) seulement a les connaissances nécessaires pour conscientiser leurs enfants à la protection de leurs données personnelles. Ceci est approuvé par la littérature scientifique. En effet, les parents actuels sont sans doute la première génération de parents à devoir faire face à une aussi grande évolution des technologies et ils n'ont pas toujours les connaissances requises (Dioni 2008). Les enseignants ont également eu l'occasion de donner leur avis à propos des connaissances des parents et 97% d'entre eux affirment que ceux-ci n'ont pas les connaissances à ce sujet. Les adolescents interrogés confirment ces dires en appuyant que leurs parents n'y connaissent pas grand-chose, certains allant même jusqu'à dire qu'ils apprennent eux-mêmes certaines notions à leurs parents concernant les risques liés à cette problématique. Virginie Tyou, l'auteure, a également remarqué que certains jeunes avaient plus de connaissances que leurs parents, qui ne sont pas nés dans l'ère du numérique.

Les connaissances des parents et leur capacité à expliquer et montrer à leurs enfants comment protéger leurs données sont liées à leur niveau d'éducation. En effet, les résultats de l'étude quantitative l'ont prouvé. Les parents ayant un diplôme universitaire de type long sont les plus nombreux à avoir des connaissances tandis que ceux n'ayant qu'un diplôme de secondaire sont très peu à affirmer cela. L'auteure et conférencière Virginie Tyou a elle-même constaté que les parents « éduqués » connaissent mieux les risques. La littérature confirme aussi ces propos. Selon Zhang, Chen et Lee (2013), les personnes bénéficiant d'un niveau d'éducation élevé ont plus de connaissances liées au numérique et peuvent ainsi plus facilement percevoir les risques. De nombreuses preuves démontrent que le niveau d'éducation a un lien avec les connaissances. Cet argument renforce l'hypothèse qui affirme que l'école a un rôle à jouer dans l'éducation au numérique. En effet, puisque les parents n'ont pas les connaissances et n'ont pas tous la même éducation, l'école a donc le rôle d'éduquer en mettant tout le monde sur le même pied d'égalité. Cet argument est appuyé par la littérature et la notion de « fracture numérique » (Rizza 2006) qui touche certaines familles n'ayant pas les mêmes droits et accès aux technologies numériques.

Les connaissances des parents sont également liées à leur métier. Les études qualitatives et quantitatives réalisées ont prouvé que le peu de parents qui avait des connaissances les avait généralement acquises grâce à leur métier. En effet, les adolescents ayant témoigné que leurs parents avaient des connaissances sur les risques liés aux données personnelles ont expliqué qu'ils les avaient acquises par le biais de leur métier. Le directeur d'école secondaire interviewé a également souligné que grâce à son métier de directeur, il avait des connaissances à ce sujet. Les résultats de l'enquête quantitative ont aussi démontré qu'il y avait un lien entre le métier et le fait d'avoir des connaissances et d'être capable d'expliquer à ses enfants comment protéger ses données personnelles. Les dirigeants d'entreprise, par exemple, sont bien plus nombreux à avoir des connaissances à ce sujet que les employés. De plus, bien qu'ils soient très peu nombreux à avoir répondu au questionnaire et que le résultat n'est peut-être donc pas très significatif, tous les professeurs d'informatique ayant répondu disent avoir les connaissances et la capacité d'expliquer cette problématique à leurs élèves.

Les connaissances des parents ne semblent pas être liées au genre ni à l'âge, d'après les résultats de l'enquête quantitative. Les parents des adolescents, un peu plus âgés, n'ont pas les connaissances nécessaires et, selon Virginie Tyou, les parents qu'elle rencontre, principalement des parents d'enfants du primaire donc un peu plus jeunes, ne les ont pas non plus.

Malgré le peu de connaissances, 61% des parents ont répondu avoir déjà sensibilisé leurs enfants à ce sujet. La peur est d'ailleurs liée à cette variable. Les adolescents confirment tous cela, leurs parents leur en ont déjà parlé, mais de manière très globale puisqu'ils n'y connaissent pas grand-chose. Les parents leur disent de faire attention mais sans leur expliquer pourquoi puisqu'eux-mêmes ne le savent pas. Virginie Tyou contredit cet argument. Selon elle, les parents ne conscientisent pas leurs enfants et ne parlent pas du tout de ce problème avec eux. En effet, aucun enfant interrogé dans les écoles primaires ne sait répondre à la question « qu'est-ce qu'une donnée personnelle ? ».

Tous les arguments cités précédemment confirment que les parents n'ont ni les connaissances ni les compétences pour conscientiser leurs enfants à la protection des données personnelles. **L'hypothèse 2a est donc rejetée.**

Bien qu'ils n'ont pas les connaissances liées au numérique, les parents craignent les dangers auxquels peuvent être confrontés leurs enfants en utilisant internet. La littérature scientifique confirme les résultats ci-dessus (Livingstone 2002). La peur concernant la vie privée de leur enfant est liée à plusieurs variables. Les parents ayant peur sont plus nombreux à avoir déjà sensibilisé leur enfant à ces risques et à avoir mis en place un contrôle parental.

Le contrôle parental et autres contrôles concernant le temps d'écran, les réseaux sociaux ou encore les sites fréquentés ne semblent pas liés significativement au niveau d'éducation selon l'enquête quantitative. Pourtant, Virginie Tyou affirme que les parents plus éduqués contrôlent plus leurs enfants. Elle insiste d'ailleurs sur ce point en expliquant que les contrôles sont très importants pour que les enfants fassent attention à la manière dont ils utilisent internet. La littérature confirme cela en mentionnant par exemple qu'un jeune n'ayant reçu aucune supervision et aucune règle utilise internet sans se soucier de la protection de sa vie privée et de ses données personnelles (Feng & Xie, 2014).

Malheureusement, les parents ne contrôlent pas assez ce que font par leurs enfants sur leur ordinateur ou téléphone. En effet, deux tiers des répondants n'ont pas mis en place de contrôle parental. Quant aux contrôles des réseaux sociaux, des achats en ligne, des sites fréquentés et du temps d'écran, les résultats divergent entre ce qu'ils considèrent comme important à contrôler et ce qu'ils contrôlent vraiment.

Tous ces arguments entraînent **le rejet de l'hypothèse 2b** : les parents ne contrôlent pas assez l'utilisation du numérique chez leur enfant.

4.2. Recommandations

Suite aux nombreuses recherches et à l'analyse des résultats obtenus lors des enquêtes qualitatives et quantitatives, je souhaite faire certaines recommandations.

Premièrement, il est essentiel de mettre rapidement en place des actions pour apprendre aux utilisateurs à protéger leurs données personnelles car j'ai constaté, tant dans la littérature que dans les résultats des enquêtes, que les gens continuent à utiliser quotidiennement les plateformes tout en sachant que leurs données sont collectées et utilisées par la suite.

D'autre part, je pense qu'il serait essentiel de mettre en place, dans les programmes scolaires, un cours sur le numérique accessible à tous les élèves. Dans l'école secondaire d'une des élèves interrogées, un cours sur la transition écologique a vu le jour cette année. Cela laisse entrevoir la possibilité d'ajouter au programme scolaire des cours liés et adaptés à des thématiques actuelles. Ce cours sur le numérique devrait bien-sûr aborder les questions d'éthique sur internet, les mécanismes de collecte et de traitement des données ainsi que la protection de ses données personnelles. Ce cours pourrait aussi couvrir d'autres sujets liés au numérique tels que le cyber-harcèlement, les algorithmes, le hacking, ... En effet, nous sommes confrontés quotidiennement à tous ces risques mais nous n'avons pas suffisamment de connaissances sur ces sujets. Comme relevé dans la littérature, les utilisateurs manquent de cyberculture (Zeebaree et al. 2020). Il est primordial d'éduquer la population au numérique et aux risques qui en découlent et ce, dès le plus jeune âge. Comme constaté tout au long de ce travail de recherche, les enfants sont exposés aux dangers du numérique très jeunes, il faut donc les éveiller aux risques qu'ils encourent.

Un cours à intégrer dans les programmes scolaires serait donc primordial. Pour le primaire, ce cours devrait être abordé de façon ludique, comme l'ont recommandé à l'unanimité les enseignants du fondamental. En ce qui concerne les secondaires, il pourrait s'agir, dans un premier temps, de formations ou d'activités régulières. Cependant, pour cette option-là, la formation devrait être ludique, animée par un intervenant formé et se baser sur des cas pratiques, des exemples concrets, en faisant participer les élèves. De plus, la formation devrait se dérouler

durant au moins une demi-journée ou plusieurs périodes de cours. Ceci permettrait d'aborder le problème en profondeur et de les amener à comprendre le processus de récolte et de gestion des données afin de les conscientiser de la meilleure des façons.

Un autre constat, les formations actuelles adressées aux enseignants ne sont pas assez qualitatives. En effet, d'après les résultats, la plupart des enseignants ayant suivi une formation consacrée à ce sujet ont répondu ne pas se sentir capable d'expliquer ou de montrer aux élèves comment protéger leurs données personnelles. Pour faire face à ce problème, je suggérerais d'améliorer la formation des enseignants. Comme l'a expliqué Virginie Tyou, le numérique ne s'apprend pas de la même façon que les matières actuelles. La formation visant les enseignants devrait couvrir non seulement les volets techniques et technologiques, mais également le volet psychopédagogique afin de leur inculquer des méthodes d'apprentissages adaptées au numérique. Ces formations ne doivent pas obligatoirement viser tous les enseignants d'une école mais en spécialiser quelques-uns pour commencer.

Une autre recommandation, que suggérerait également le directeur monsieur Jadin, serait d'avoir un référent numérique dans chaque école. Cette personne serait ainsi en charge de tout ce qui est lié au numérique. Elle s'occuperait non seulement de l'aspect technique (comme les plateformes Smartschool, les tableaux interactifs, une aide pour utiliser les outils numériques) mais également de la mise en place d'un cours sur le numérique, de l'organisation d'activités ou de conférences à ce sujet, ...

Enfin, je souhaite conclure ces recommandations en suggérant d'approfondir cette étude qui présente certaines limites, comme évoqué précédemment. L'échantillon étant non-aléatoire et de petite taille, je suggérerais de questionner davantage d'enseignants et de parents, issus de milieux et d'écoles plus diversifiés. Je recommanderais également d'interviewer des personnes issues d'organisations telles que la Commission européenne ou le Conseil européen mais également une personne de la Fédération Wallonie-Bruxelles. Malheureusement, n'ayant reçu aucune réponse de leur part, je n'ai pas eu l'occasion d'interroger ce type de partie prenante qui aurait pu apporter d'autres informations pertinentes au sujet de ma problématique.

CONCLUSION

L'idée que la conscientisation à l'utilisation des données personnelles puisse passer par l'éducation a fait office de ligne directrice de ce travail de recherche.

Il ressort des nombreuses lectures de la littérature relatives à ce sujet et des résultats des différentes enquêtes quantitatives et qualitatives que l'école apparaît comme la solution idéale pour éduquer les utilisateurs européens à la protection de leurs données personnelles. En effet, seule l'hypothèse suggérant que l'école avait un rôle à jouer dans l'éducation au numérique s'est révélée positive.

L'éducation au numérique est une solution à mettre en place dans les écoles et ce dès les primaires. En effet, les enfants sont confrontés de plus en plus jeunes aux risques liés à internet et au numérique. De plus, il est essentiel de les éduquer tôt car des informations expliquées de manière ludique à des enfants restent davantage ancrées quand ils grandissent et ils s'en souviennent mieux. Il est également important de noter que les enfants ont généralement tendance à mieux écouter les adultes (les enseignants dans ce cas-ci) et appliquer leurs conseils que lorsqu'ils sont adolescents.

Cependant, à l'heure actuelle, les enseignants n'ont pas les connaissances techniques et psychopédagogiques nécessaires pour enseigner le numérique aux élèves et les éveiller à la protection de leurs données personnelles. Bien que certains aient suivi des formations à ce sujet, celles-ci ne se sont pas révélées très utiles puisqu'ils ne se sentent pas capables d'expliquer aux élèves comment protéger leurs données.

L'école serait une solution pour conscientiser les élèves. En effet, les méthodes mises en place à l'heure actuelle, comme les campagnes organisées par Child focus ou les minis formations d'une heure organisées dans les écoles, sont plutôt destinées à la prévention. Elles ne sont donc pas suffisantes pour faire prendre conscience aux jeunes des dangers du numérique.

En ce qui concerne les parents, ceux-ci n'ont pas les connaissances nécessaires pour éduquer leur enfant au numérique. Cela renforce l'hypothèse que l'école a un rôle essentiel à jouer. De plus, certaines familles sont touchées par la fracture numérique et cet écart ne cesse de grandir.

L'école permettrait en outre de réduire cet écart puisque les enfants auraient tous droit à une formation continue à ce sujet.

Enseigner le numérique à l'école permettrait aussi de former indirectement les parents des élèves. En effet, les enfants vont acquérir des connaissances et des compétences relatives au numérique. Ils pourront ainsi en parler dans leur famille et les appliquer chez eux. Il y aurait donc une transmission de savoirs des enfants vers les parents qui pourraient à leur tour appliquer les conseils reçus via l'école et être davantage informés des risques liés au numérique.

L'école est donc la clé pour éduquer les jeunes à la protection de leurs données personnelles et à tous les risques liés au numérique. Dans cette perspective, il serait intéressant de mettre en place, dans les programmes scolaires et ce, dès l'école primaire, un cours où certains enseignants pourraient inculquer aux élèves, de façon ludique et la plus pédagogique possible, les différents aspects des technologies numériques. Cela leur permettrait d'apprendre aux jeunes à gérer leurs données personnelles et à protéger leur vie privée, mais aussi de les sensibiliser au cyber-harcèlement ou aux algorithmes. A cette fin, la formation des enseignants devrait être repensée afin de leur transmettre les compétences clés liées au numérique, tant au niveau technique que psychopédagogique.

BIBLIOGRAPHIE

A. Articles Scientifiques

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54(2), 442-492. <https://doi.org/10.1257/jel.54.2.442>
- Attour, A., & Longhi, C. (2009). Fracture numérique, le chaînon manquant. *Les Cahiers du numerique*, 5(1), 119-146.
- Barnes, S. B. (2006). A privacy paradox : Social networking in the United States. *First Monday*. <https://doi.org/10.5210/fm.v11i9.1394>
- Batra, S., & Tyagi, C. (2012). *Comparative Analysis of Relational And Graph Databases*. 2(2), 4.
- Belleflamme, P. (2017). *LES PLATEFORMES DE L'ECONOMIE COLLABORATIVE : FONCTIONNEMENT ET ENJEUX*. <https://doi.org/10.3917/dbu.decro.2017.01.0221>
- Benamar, L., Balagué, C., & Zhong, Z. (2020). Internet of Things devices appropriation process : The Dynamic Interactions Value Appropriation (DIVA) framework. *Technovation*, 89, 102082. <https://doi.org/10.1016/j.technovation.2019.06.001>
- Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents – Privacy Concerns – Outcomes model. *Journal of Information Science*, 43(5), 583-600. <https://doi.org/10.1177/0165551516653590>
- Bourreau, M., & Perrot, A. (2020). Plateformes numériques : Réguler avant qu'il ne soit trop tard. *Notes du conseil danalyse economique*, 60(6), 1-12.
- Brenner, S. (2001). *Cybercrime Investigation and Prosecution : The Role of Penal and Procedural Law*.
- Britten, N. (1995). Qualitative Research : Qualitative interviews in medical research. *BMJ*, 311(6999), 251-253. <https://doi.org/10.1136/bmj.311.6999.251>

- Bruillard, E., & Baron, georges-louis. (2006). *Usages en milieu scolaire : Caractérisation, observation et évaluation*.
- Chan, C. K., & Virkki, J. (2014). Perspectives for Sharing Personal Information on Online Social Networks. *Social Networking, 2014*. <https://doi.org/10.4236/sn.2014.31005>
- Chatellier, R., Delcroix, G., & Hary, E. (2019). *La forme des choix—Données personnelles, design et frictions désirables—CAHIERS IP INNOVATION & PROSPECTIVE N°06—CNIL* [Research Report]. CNIL. <https://hal.archives-ouvertes.fr/hal-02181440>
- Codron, C. (s. d.). *La surveillance diffuse : Entre Droit et Norme*. 575.
- Combs-Ronto, L. A., Olson, S. L., Lunkenheimer, E. S., & Sameroff, A. J. (2009). Interactions Between Maternal Parenting and Children’s Early Disruptive Behavior : Bidirectional Associations across the Transition from Preschool to School Entry. *Journal of Abnormal Child Psychology, 37*(8), 1151-1163. <https://doi.org/10.1007/s10802-009-9332-2>
- Darnault, C. (2021). *La protection des données personnelles : Présentation des approches européennes et américaines*. 3, 153-176.
- Dioni, C. (s. d.-a). *Métier d’élève, métier d’enseignant à l’ère numérique*. 29.
- Dioni, C. (s. d.-b). *Métier d’élève, métier d’enseignant à l’ère numérique*. 29.
- Ert, E., Fleischer, A., & Magen, N. (2016). Trust and reputation in the sharing economy : The role of personal photos in Airbnb. *Tourism Management, 55*, 62-73. <https://doi.org/10.1016/j.tourman.2016.01.013>
- Feng, Y., & Xie, W. (2014). Teens’ concern for privacy when using social networking sites : An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior, 33*, 153-162. <https://doi.org/10.1016/j.chb.2014.01.009>
- Fluckiger, C. (s. d.). *La culture numérique adolescente*. 13.

- Forsé, M. (2008). Définir et analyser les réseaux sociaux. *Informations sociales*, 147(3), 10-19.
- Galley, P. (s. d.). *Terrorisme informatique : Quels sont les risques ?* 34.
- Hassani, N. (2019). Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations. *Terminal. Technologie de l'information, culture & société*, 124, Article 124. <https://doi.org/10.4000/terminal.4040>
- Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9), 1277-1288.
<https://doi.org/10.1177/1049732305276687>
- Jean-Marc Deltorn. (2017). » *La protection des données personnelles face aux algorithmes prédictifs* | *Revue des droits et libertés fondamentaux*. <http://www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/>
- Lancelot Miltgen, C. (2003). Vie privée et Internet : Influence des caractéristiques individuelles et situationnelles sur les attitudes et les comportements des internautes face à la collecte de leurs données personnelles. *Congrès International de l'Association Française du Marketing*, 1-30. <https://hal.archives-ouvertes.fr/hal-00457867>
- Lauricella, A. R., Herdzina, J., & Robb, M. (2020). Early childhood educators' teaching of digital citizenship competencies. *Computers & Education*, 158, 103989.
<https://doi.org/10.1016/j.compedu.2020.103989>
- Les français et la protection des données personnelles*. (s. d.). 13.
- Lesteven, G., & Godillon, S. (2017). Les plateformes numériques révolutionnent-elles la mobilité urbaine ? *Netcom. Réseaux, communication et territoires*, 31-3/4, 375-402.
<https://doi.org/10.4000/netcom.2756>

- Livingstone, S. (2002). *Young People and New Media : Childhood and the Changing Media Environment* / S. Livingstone.
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (s. d.). *The perspective of European children*. 171.
- Maurel, L. (2019). Contre le pouvoir des plateformes, établir une portabilité sociale des données ? In *Rapport annuel OPTIC "ETHICS & TECH 2019"—(Re)construire la confiance dans les technologies*. <https://hal.archives-ouvertes.fr/hal-02144473>
- Medhi, S., & Baruah, H. (2017). Relational database and graph database : A comparative analysis. *Journal of Process Management. New Technologies*, 5(2), 1-9.
<https://doi.org/10.5937/jouproman5-13553>
- Miller-Lewis, L. R., Baghurst, P. A., Sawyer, M. G., Prior, M. R., Clark, J. J., Arney, F. M., & Carbone, J. A. (2006). Early Childhood Externalising Behaviour Problems : Child, Parenting, and Family-related Predictors Over Time. *Journal of Abnormal Child Psychology*, 34(6), 886-901. <https://doi.org/10.1007/s10802-006-9071-6>
- Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns : A qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), 103-125. <https://doi.org/10.1057/ejis.2013.17>
- NixonGiuffridaCCIPaper.pdf*. (s. d.). Consulté 3 janvier 2022, à l'adresse
<https://covacci.org/wp-content/uploads/2021/03/NixonGiuffridaCCIPaper.pdf>
- Ou, C. X. J., Davison, R. M., & Cheng, N. C. K. (2011). Why Are Social Networking Applications Successful : An Empirical Study Of Twitter. *PACIS 2011 Proceedings*.
<https://aisel.aisnet.org/pacis2011/145>
- Rallet, A. (2018). *Valoriser ses données personnelles ? 3 scénarios*. <https://hal.archives-ouvertes.fr/hal-01909650>

- Reitz, E., Deković, M., & Meijer, A. M. (2006). Relations between parenting and externalizing and internalizing problem behaviour in early adolescence : Child behaviour as moderator and predictor. *Journal of Adolescence*, 29(3), 419-436.
<https://doi.org/10.1016/j.adolescence.2005.08.003>
- Rizza, C. (2006). The digital divide, paradox of the Net generation. *Hermes, La Revue*, 45(2), 25-32.
- Schlagwein, D., Schoder, D., & Spindeldreher, K. (2020). Consolidated, systemic conceptualization, and definition of the “sharing economy”. *Journal of the Association for Information Science and Technology*, 71(7), 817-838.
<https://doi.org/10.1002/asi.24300>
- Sechrest, L., & Sidani, S. (1995). Quantitative and qualitative methods : Is There an Alternative? *Evaluation and Program Planning*, 18(1), 77-87.
[https://doi.org/10.1016/0149-7189\(94\)00051-X](https://doi.org/10.1016/0149-7189(94)00051-X)
- Smyrnaio, N. (2016). L’effet GAFAM : Stratégies et logiques de l’oligopole de l’internet. *Communication langages*, 188(2), 61-83.
- Suarez-Herrera_(2012)_- _Livre_ACFAS-with-cover-page-v2.pdf. (s. d.). Consulté 2 janvier 2022, à l’adresse [https://d1wqtxts1xzle7.cloudfront.net/31310675/Suarez-Herrera_\(2012\)_- _Livre_ACFAS-with-cover-page-v2.pdf?Expires=1641165235&Signature=EPY7v-ORF5G5MBt~Tsw4CbLO3Qow~O2h7e~QD~KOV9kI7w~Nn1UO6POze4nIsAhzHV~On8oAQAGJs-EG2VdFucUJHdhXQE9Vk681lVPdBWK3nv~YjWPOk5UiRdHcNwZ5HETl117ND1-I5POrrrYZzy7kXDBBuXX6hKEICT15Yy9Ghzddd6br3gWwpCBeGj-Io6GXXS1gO4o8Gf6njrtBTesR7pLZddemFaDSSNIXjAfZnBTh6w7gXU3DMPisdvKyRMSVIMn1dxAVE21rlbQKoQuhcEdSeL6lf4cIq5lTtHHsi7c3R1Cun1mmyog2XE](https://d1wqtxts1xzle7.cloudfront.net/31310675/Suarez-Herrera_(2012)_- _Livre_ACFAS-with-cover-page-v2.pdf?Expires=1641165235&Signature=EPY7v-ORF5G5MBt~Tsw4CbLO3Qow~O2h7e~QD~KOV9kI7w~Nn1UO6POze4nIsAhzHV~On8oAQAGJs-EG2VdFucUJHdhXQE9Vk681lVPdBWK3nv~YjWPOk5UiRdHcNwZ5HETl117ND1-I5POrrrYZzy7kXDBBuXX6hKEICT15Yy9Ghzddd6br3gWwpCBeGj-Io6GXXS1gO4o8Gf6njrtBTesR7pLZddemFaDSSNIXjAfZnBTh6w7gXU3DMPisdvKyRMSVIMn1dxAVE21rlbQKoQuhcEdSeL6lf4cIq5lTtHHsi7c3R1Cun1mmyog2XE)

4znBbYLtBQl666uJdcqWAg__&Key-Pair-

Id=APKAJLOHF5GGSLRBV4ZA#page=136

Sylvestre, G. (2017). Les types de failles et de risques sécurité. *I2D - Information, donnees documents*, 54(3), 30-31.

Symantec. (2015). *State of Privacy Report 2015*.

<https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/state-of-privacy-report-en-2015.pdf>

The Common Sense Census : Media Use by Tweens and Teens. (s. d.). 104.

Tussyadiah, I. P. (2015). An Exploratory Study on Drivers and Deterrents of Collaborative Consumption in Travel. In I. Tussyadiah & A. Inversini (Éds.), *Information and Communication Technologies in Tourism 2015* (p. 817-830). Springer International Publishing. https://doi.org/10.1007/978-3-319-14343-9_59

Umhoefer, C., Rofé, J., Lemarchand, S., Piper, D., Baltassis, E., Stragier, F., & Telle, N. (s. d.). *Le Big Data face au défi de la confiance*. 24.

Viossat, L.-C. (2018). Les plateformes, un modèle en voie de régulation. *Constructif*, 50(2), 40-43.

Zeebaree, S., Ameen, S., & M.Sadeeq, M. (2020). *Social Media Networks Security Threats, Risks and Recommendation : A Case Study in the Kurdistan Region*. 13, 349-365.

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile Commerce and Consumer Privacy Concerns. *Journal of Computer Information Systems*, 53(4), 31-38.
<https://doi.org/10.1080/08874417.2013.11645648>

B. Ouvrages de référence

- Denzin, N. K. (2017). *The Research Act : A Theoretical Introduction to Sociological Methods*. Transaction Publishers.
- Henderson, A. T., Berla, N., & National Committee for Citizens in Education (Éds.). (1994). *A new generation of evidence : The family is critical to student achievement*. National Committee for Citizens in Education.
- La sociologie des réseaux sociaux*. (s. d.). Consulté 3 janvier 2022, à l'adresse <https://www.cairn.info/la-sociologie-des-reseaux-sociaux--9782707188885.htm>
- Lemieux, V. (1999). *Les réseaux d'acteurs sociaux*. Presses Universitaires de France.
- Morgan, D. L. (1996). *Focus Groups as Qualitative Research*. SAGE Publications.
- Sterling, B. (2020). *The Hacker Crackdown : Law and Disorder on the Electronic Frontier*. Open Road Media.
- Vandercammen, M., & Gauthy-Sinéchal, M. (2014). *Etudes de marchés : Méthodes et Outils* (4^e éd.). De Boeck Supérieur.
- Wall, D. (2007). *Cybercrime : The Transformation of Crime in the Information Age*. Polity.
- Weber, R. P. (1990). *Basic Content Analysis*. SAGE.

C. Sites internet

- (8) (PDF) *Cybercrime Investigation and Prosecution : The Role of Penal and Procedural Law*. (s. d.). Consulté 3 janvier 2022, à l'adresse https://www.researchgate.net/publication/240610895_Cybercrime_Investigation_and_Prosecution_the_Role_of_Penal_and_Procedural_Law
- Auteure, conférencière et hypnothérapeute*. (s. d.). Virginie Tyou. Consulté 3 janvier 2022, à l'adresse <https://www.virginietyou.com/>
- BOITMOBILE. (s. d.). *Courtier en données—Définitions Marketing » L'encyclopédie*

illustrée du marketing. Consulté 3 janvier 2022, à l'adresse <https://www.definitions-marketing.com/definition/courtier-en-donnees/>

Cambridge Analytica : 87 millions de comptes Facebook concernés. (2018, avril 4). *Le Monde.fr*. https://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptes-facebook-concernees_5280752_4408996.html

Camgirl—2 définitions—Encyclopédie.fr. (s. d.). Consulté 3 janvier 2022, à l'adresse <https://www.encyclopedia.fr/definition/Camgirl>

CHAPITRE I - Dispositions générales | CNIL. (s. d.). Consulté 27 décembre 2021, à l'adresse <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4>

CHAPITRE II - Principes | CNIL. (s. d.). Consulté 27 décembre 2021, à l'adresse <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article9>

Cimpanu, C. (s. d.). *Australian tech unicorn Canva suffers security breach*. ZDNet. Consulté 2 janvier 2022, à l'adresse <https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/>

CNIL |. (s. d.). Consulté 2 janvier 2022, à l'adresse <https://www.cnil.fr/>

Consumers Around the Globe Worried About How Much Personal Information They Share Online; Survey Reveals Need for More Education and Transparency | ForgeRock. (2018, mars 5). <https://www.forgerock.com/about-us/press-releases/consumers-around-globe-worried-about-how-much-personal-information-they>

Cookie | CNIL. (s. d.). Consulté 3 janvier 2022, à l'adresse <https://www.cnil.fr/fr/definition/cookie>

Cybercriminalité : Définition de « cybercriminalité ». (s. d.). La langue française. Consulté 3 janvier 2022, à l'adresse <https://www.lalanguefrancaise.com/dictionnaire/definition/cybercriminalite>

Cyberculture : Définition de « cyberculture ». (s. d.). La langue française. Consulté 3 janvier

2022, à l'adresse
<https://www.lalanguefrancaise.com/dictionnaire/definition/cyberculture>

Cyberespace : Définition simple et facile du dictionnaire. (s. d.). Consulté 3 janvier 2022, à l'adresse <https://www.linternaute.fr/dictionnaire/fr/definition/cyberespace/>

Cyberharcèlement : Définition, sanctions, précautions - Ooreka. (s. d.). Ooreka.fr. Consulté 3 janvier 2022, à l'adresse [//justice.ooreka.fr/astuce/voir/599421/cyberharcèlement](https://justice.ooreka.fr/astuce/voir/599421/cyberharcèlement)

Définition du NoSQL (Not Only SQL database). (2020, mars 27). *Actualité Informatique*.
<https://actualiteinformatique.fr/data/definition-nosql-not-only-sql-database>

Définition du SQL (Structured Query Language). (2020, mars 27). *Actualité Informatique*.
<https://actualiteinformatique.fr/data/definition-sql-structured-query-language>

Définitions des microdonnées et des données agrégées—Service des bibliothèques et archives—Université de Sherbrooke. (s. d.). Consulté 3 janvier 2022, à l'adresse
<https://www.usherbrooke.ca/biblio/trouver-des/donnees-statistiques/definitions-des-microdonnees-et-des-donnees-agregees>

Domaine de compétences numériques. (s. d.). Education à la citoyenneté numérique (ECN). Consulté 2 janvier 2022, à l'adresse <https://www.coe.int/fr/web/digital-citizenship-education/digital-citizenship-domains>

Donnée sensible | CNIL. (s. d.). Consulté 27 décembre 2021, à l'adresse
<https://www.cnil.fr/fr/definition/donnee-sensible>

Données personnelles. (s. d.). La Quadrature du Net. Consulté 3 janvier 2022, à l'adresse
https://www.laquadrature.net/donnees_perso/

Données personnelles | CNIL. (s. d.). Consulté 27 décembre 2021, à l'adresse
<https://www.cnil.fr/fr/donnees-personnelles>

Hacking | Besafe. (s. d.). Consulté 3 janvier 2022, à l'adresse
<https://www.besafe.be/fr/themes-de-securite/cybersecurite/cybercriminalite/hacking>

Home—BIK Portal—BIK Community. (s. d.). BIK Portal. Consulté 2 janvier 2022, à l'adresse <https://www.betterinternetforkids.eu>

illustradata. (2016, novembre 8). Que sont les bases NoSQL orientées graphes et à quoi servent-elles ? *IllustraData*. <http://www.illustradata.com/bases-nosql-orientees-graphes-a-quoi-servent/>

Internet et les réseaux sociaux : Utilisation des 8 - 11 ans en chiffres. (2021, avril 12).

THEMIS. <https://www.themis.asso.fr/internet-et-les-reseaux-sociaux-utilisation-des-8-11-ans-en-chiffres/>

Je décide de ce qui concerne ma vie privée | Je Decide. (s. d.). Consulté 2 janvier 2022, à l'adresse <https://www.jedecide.be/>

Jean-Marc Deltorn. (2017). » *La protection des données personnelles face aux algorithmes prédictifs | Revue des droits et libertés fondamentaux*. <http://www.revuedlf.com/droit-ue/la-protection-des-donnees-personnelles-face-aux-algorithmes-predictifs/>

La CNIL publie son rapport d'activité 2020 | CNIL. (s. d.). Consulté 3 janvier 2022, à l'adresse <https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2020>

Larousse, É. (s. d.). *Définitions : Agrégateur - Dictionnaire de français Larousse*. Consulté 3 janvier 2022, à l'adresse <https://www.larousse.fr/dictionnaires/francais/agr%C3%A9gateur/187978>

Le référentiel CNIL de formation des élèves à la protection des données personnelles. (s. d.). éducol | Ministère de l'Éducation nationale, de la Jeunesse et des Sports - Direction générale de l'enseignement scolaire. Consulté 2 janvier 2022, à l'adresse <https://eduscol.education.fr/574/le-referentiel-cnil-de-formation-des-eleves-la-protection-des-donnees-personnelles>

L'éducation à la citoyenneté numérique. (s. d.). Education à la citoyenneté numérique (ECN). Consulté 2 janvier 2022, à l'adresse <https://www.coe.int/fr/web/digital-citizenship->

education/digital-citizenship-education-project

Les audiences numériques augmentent, mais les problèmes arrivent... (2021, juillet 21). We

Are Social France. <https://wearesocial.com/fr/blog/2021/07/les-audiences-numeriques-augmentent-mais-les-problemes-arrivent/>

Page d'accueil citoyen | Autorité de protection des données. (s. d.). Consulté 2 janvier 2022, à l'adresse <https://www.autoriteprotectiondonnees.be/citoyen>

Qualitative Data : An Introduction to Coding and Analysis—Carl Auerbach, Louise B.

Silverstein—Google Livres. (s. d.). Consulté 2 janvier 2022, à l'adresse

[https://books.google.be/books?hl=fr&lr=&id=zclS-vzxsysC&oi=fnd&pg=PP7&dq=\(Auerbach,+Silverstein,+2003\)&ots=GrEoHPT6wj&sig=Rl7YwP199KpcHB2htqnrsnkRB9I#v=onepage&q=\(Auerbach%2C%20Silverstein%2C%202003\)&f=false](https://books.google.be/books?hl=fr&lr=&id=zclS-vzxsysC&oi=fnd&pg=PP7&dq=(Auerbach,+Silverstein,+2003)&ots=GrEoHPT6wj&sig=Rl7YwP199KpcHB2htqnrsnkRB9I#v=onepage&q=(Auerbach%2C%20Silverstein%2C%202003)&f=false)

Qu'est-ce qu'une base de données relationnelle. (s. d.). Oracle France. Consulté 1 janvier

2022, à l'adresse <https://www.oracle.com/fr/database/base-de-donnees-relationnelle-definition.html>

strategie.agency. (s. d.). *Safer Internet Day*. Consulté 2 janvier 2022, à l'adresse

<https://saferinternetday.be/home/saferinternetday.be/>

Study : Hackers Attack Every 39 Seconds. (s. d.). Consulté 3 janvier 2022, à l'adresse

<https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>

The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors -

ProQuest. (s. d.). Consulté 2 janvier 2022, à l'adresse

<https://www.proquest.com/docview/195919282?accountid=12156&parentSessionId=1I%2BbwXOO8fVaZtUog5zf0Gm9d90AJY1Xt3RkzHXnjl%3D&pq-origsite=summon>

Tout sur la graph database : La base de données pour une mise en réseau efficace. (s. d.).

IONOS Digitalguide. Consulté 1 janvier 2022, à l'adresse

<https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/base-de-donnees-orientee-graphe/>

tralalere. (s. d.). *Qui sommes-nous ?* Internet Sans Crainte. Consulté 2 janvier 2022, à

l'adresse <https://www.internetsanscrainte.fr/qui-sommes-nous>

Two-sided markets : A progress report—Rochet—2006—The RAND Journal of Economics—

Wiley Online Library. (s. d.). Consulté 2 janvier 2022, à l'adresse

<https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1756->

[2171.2006.tb00036.x?casa_token=MtSgXLrZ4vQAAAAA:-WmvGlm-](https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1756-2171.2006.tb00036.x?casa_token=MtSgXLrZ4vQAAAAA:-WmvGlm-)

[OPjktL6koFUrn9XZHFnbHhxxRKKBuowHACPDHsI_pszJEMjbU55VhGwmkHMv](https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1756-2171.2006.tb00036.x?casa_token=MtSgXLrZ4vQAAAAA:-WmvGlm-)

[SJawQwHKfZDUzQ](https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1756-2171.2006.tb00036.x?casa_token=MtSgXLrZ4vQAAAAA:-WmvGlm-)

Winder, D. (s. d.). *Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019.*

Forbes. Consulté 3 janvier 2022, à l'adresse

<https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41->

[billion-records-in-first-six-months-of-2019/](https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/)

D. Autres

Mercier, D. (2019). *L'impact du RGPD sur la confiance des consommateurs.*

Pleyers, G. (2020). *Marketing Research LLSMS2000.*

ANNEXES

Annexes 1 : Questionnaires des enquêtes qualitatives

A) Focus group pour les élèves

Bonjour à toutes et à tous,

Merci pour votre présence. Je suis étudiante en sciences de gestion et je réalise un mémoire pour voir si l'éducation au numérique pourrait être une solution pour conscientiser les jeunes à la protection de leurs données personnelles.

1) Tour de table présentation

Chacun se présente

2) Sujet :

Savez-vous ce qu'est une donnée personnelle et ce qu'est une donnée sensible ?

Théo : c'est tout ce qui peut nous concerner de près ou de loin donc ton adresse ton code postal, ton nom et tout ça.

Juliette : je pense que c'est aussi tes recherches, tes favoris etc. Si on va par exemple tout le temps voir un site, c'est une de tes données.

⇒ Une donnée personnelle, c'est « toute information se rapportant à une personne physique identifiée ou identifiable ». Par exemple, nom, prénom, adresse,... Une donnée sensible c'est un type de donnée personnelle. Elles fournissent des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Ces données sont plus privées et doivent être traitées avec plus de sécurité.

Utilisez-vous les grandes plateformes comme Facebook, Google, Amazon, Uber, Airbnb, Netflix,... ? Si c'est le cas, avez-vous déjà remarqué que vos données étaient en quelque sorte volées ? Qu'avez-vous déjà remarqué par rapport à cela ?

Juliette : oui moi tout le temps. A chaque fois que je vais voir un truc sur un site j'ai des pubs. Dernièrement c'est arrivé avec Patagonia.

Sybille : oui j'ai remarqué. Mon papa est fan de vélo et moi pas, mais j'ai déjà eu plein de pubs de vélo car mon papa nous en parle et donc je suis sûre que Google nous écoute. Ma sœur a aussi les pubs de vélo.

Théo : moi aussi j'ai eu l'expérience plusieurs fois.

Vous-êtes vous déjà posé la question de savoir où vont nos données et quels sont les mécanismes derrière tout ça ?

Juliette : je me suis déjà posée plein de fois la question mais alors j'en ai aucune idée, j'ai pas cherché.

Louis : c'est pas les moteurs de recherches qui possèdent tous les sites, comme Facebook qui possède Instagram, What, 'sApp, ils ramènent toutes les données chez lui et puis Facebook les revend à plein d'autres sites.

⇒ Explication en très bref des mécanismes

3) L'éducation à travers les écoles

Une des clés pour vous conscientiser à la protection de votre vie privée, de vos données personnelles et des dangers d'Internet serait l'éducation citoyenne numérique, c'est-à-dire

l'autonomisation des enfants par le biais de l'éducation ou l'acquisition de compétences pour apprendre et participer activement à la société numérique. Il s'agit des connaissances, des aptitudes et de la compréhension nécessaires aux utilisateurs pour exercer et défendre leurs droits et responsabilités démocratiques en ligne et promouvoir et protéger les droits de l'homme, la démocratie et l'État de droit dans le cyberspace.

L'éducation au numérique passerait par l'école. Avez-vous déjà eu des activités, des formations, un cours là-dessus (par exemple en informatique), ou des discussions en classe à ce sujet ? (protection des données personnelles) ?

Théo : je me souviens, déjà en primaire on avait eu des activités. Comme on allait rentrer dans l'adolescence on allait être confronté aux réseaux sociaux et donc c'était fort sur les réseaux. Par exemple, ce qu'on peut et ne peut pas publier sur Instagram, à quel âge on peut faire quoi, où vont nos photos,...

En Secondaire maintenant, les profs de notre école en parlent beaucoup. Ils y font beaucoup allusion. Depuis 5 ans (que je suis dans l'école) on a eu deux activités, avec des gens professionnels qui viennent et qui nous parlent et nous sensibilisent. Cela prend 2h de cours et on fait cela à la place du cours.

Ce sont dans des cours généraux ou c'est par exemple pour le cours d'informatique ?

Théo : c'est dans des cours généraux donc par exemple à la place de deux heures de géo. C'était aussi sur le cyberharcèlement etc mais dans le cyberharcèlement par exemple ils parlaient des données, des photos que certains utilisaient même si on les avait supprimée.

Louis : nous on n'a jamais eu ça au Christ-Roi. Les profs ils en nous en ont déjà parlé comme ça dans une conversation, surtout quand on était en première ou deuxième mais sinon non.

Juliette : Nous en première on a eu un gars de la police qui était venu nous expliquer les dangers d'internet parce que tu t'inscris sur internet. Il disait de faire attention de pas mentir sur son âge et nous a parlé des dangers d'Internet mais pas beaucoup sur les données en tout cas j'ai pas beaucoup de souvenirs. Ils nous parlaient quand même de la vie privée sur les réseaux sociaux comme le fait de pas publier de photos de toi en vacances etc pour les cambrioleurs mais sinon on a jamais rien eu d'autres. De temps en temps les profs quand ils ouvrent un site devant nous et qu'ils voient une page avec les cookies ils dites « oui faites gaffe à ça » vite fait mais j'ai jamais eu d'activité là-dessus ni rien. Ils ne nous apprennent pas beaucoup plus que ce que l'on sait déjà.

Sybille : Nous on a eu aussi une activité de deux heures de cours avec plein de vidéos qui nous sensibilisaient. Je m'en souviens d'une c'était plein de personnes dans des tentes qui travaillent sur des ordinateurs et cela faisait plein de liens entre les personnes et ce qu'on fait sur internet. Ils nous ont expliqué sur Facebook, on n'a plus juste le petit pouce « like », maintenant on a le « j'adore » et d'autres pour encore plus avoir notre avis par rapport aux publications.

Théo : aux AIF en primaire, on a dû lire un livre qui s'appelait « cliki », c'était sur le fait qu'on nous écoutait, cela représentait les dangers d'internet etc. On avait dû faire un exposé, on en avait parlé en classe. A chaque cours de français on parlait du bouquin cela avait pris plusieurs semaines.

Maud : Moi l'année passée, mon examen d'audition de Néerlandais, c'était sur ça. Sur nos données.

Juliette : ah oui nous aussi on a eu un chapitre là-dessus en Néerlandais.

Maud : oui et donc j'ai pas tout compris mais il y avait une vidéo avec et cela m'avait quand même choqué car on comprenait quand même certaines choses sur les données. On voyait qu'une fille écrivait quelque chose et qu'un mécanisme cryptait tous les messages et qu'avec un mot ils reliaient tous tes autres messages. Par exemple si dans les messages il trouvait plusieurs fois le mot pomme t'as une pub sur les pommes. Un autre exemple, via ton google map, ton gps et il va calculer près de quel magasin tu vas passer et du coup il va mettre des pubs des prochains magasins que tu vas croiser dans la rue.

Juliette : ça c'est comme sur Instagram et Tik-tok, il y a des algorithmes pour nous proposer que certaines publications.

Théo : oui Instagram, ils savent tout voir sur nous, si on zoom sur une publication, combien de temps on reste sur telle publication, ça fait trop peur !

Louis : nous dans notre école on parle jamais de ça même en cours de langue etc.

Juliette : moi pareil, j'ai plus appris à l'extérieur en parlant avec des gens plutôt qu'à l'école quoi.

Selon-vous est-ce important d'apprendre ça à l'école ? Et si oui par quels moyens (activité ludique, cours d'informatique, journée de formation) ?

Juliette : on doit pas avoir un cours chaque semaine sur le cyberharcèlement mais par exemple une formation 1 ou 2 fois par an ça serait intéressant

Maud : oui deux fois par an, on nous apprendrait concrètement les choses, pour nous sensibiliser.

Juliette : parce que moi je l'ai appris tard, et encore maintenant je sais qu'il se passe quelque chose mais je ne sais pas quoi.

Maud : mais le pire c'est qu'on continue parce qu'on sait pas comment faire.

Louis : oui cela serait bien qu'on nous explique mieux et qu'on nous dise quelles sont un peu les clés pour se protéger, quels sont les moyens car on ne sait pas comment on doit faire. On voit les pubs sur Facebook après notre recherche sur certains sites mais comment faire pour ne plus avoir ça ? On ne sait pas.

Maud : Pour l'école, quand on était petit en primaire, on devait taper des livres pour s'entraîner à taper sur un ordinateur, cela serait beaucoup plus intéressant de sensibiliser les enfants au cyberharcèlement, aux données personnelles et à tous les dangers d'internet plutôt que de bêtement taper un livre.

Théo: surtout si c'est un professionnel qui vient, nos parents ils nous disent fait attention mais sinon ils connaissent pas plus.

Juliette : aussi ça serait bien de faire des activités en mode plus ludique et pas une personne qui parle 2 h en monologue

Louis : j'ai l'impression aussi que certaines personnes de notre âge elles s'en fichent un peu. L'autre jour on discutait de ça dans mon groupe d'ami une a dit « j'ai tout le temps des pubs pour des chaussures, ça revient tout le temps » et un autre ami disait « bah c'est normal et en soi c'est pas grave ».

Maud : oui peut-être que là pour des chaussures on s'en fiche et on se rend pas compte que c'est problématique ou « dangereux » mais si on agit déjà comme ça maintenant, plus tard

quand il y aura des informations plus importantes et plus confidentielles, comme on aura appris à s'en foutre notre attitude ne changera pas.

4) L'éducation à travers les parents :

L'éducation vient aussi de vos parents. Ils ont également un rôle à jouer à vous conscientiser aux dangers d'internet et à la protection de votre vie privée et de vos données personnelles.

Vos parents surveillent-ils ce que vous faites sur les écrans ? Avez-vous un temps d'écran limité ? Contrôlent-ils les sites sur lesquels vous allez ? Avez-vous un logiciel de contrôle parental mis en place chez vous ?

Sybille : pas du tout, je pense que mes parents ne savent même pas qu'on peut contrôler tout ça.

Juliette : pas du tout mais par exemple, au début ou je m'étais inscrite sur les réseaux sociaux, ils m'avaient avertis des dangers mais principalement sur ce que je poste pour ma vie privée, ou certains sites mais pas sur les données personnelles. Par contre, je connais des gens qui ont des contrôles parentaux pour vérifier les sites,...certains sites sont bloqués.

Louis : au début mon frère et moi nos téléphones étaient contrôlés mais maintenant plus. Mon frère il a encore ça quand même sur Apple, quand il veut télécharger des applications il a un mot de passe à mettre qui vient de mes parents et donc ça ils contrôlent.

Juliette : moi j'ai ça pour ma carte bancaire je peux pas acheter en ligne ou faire des versements avant mes 18 ans, sauf si ma maman le fait. Je peux payer en Bancontact mais pas sur internet.

Maud : moi ils ont voulu mettre un logiciel de contrôle parental mais on ne l'a jamais fait. Ils nous suivent sur Instagram pour regarder ce qu'on publie mais c'est tout.

Vous ont-ils déjà expliqué et conscientisé aux dangers d'internet et surtout à la protection de vos données personnelles ? Si oui, que vous ont-ils expliqué ?

Théo oui ils m'en ont déjà parlé, des dangers surtout et un peu des données personnelles sur ce qu'ils savent quoi, mais j'ai l'impression que notre génération est plus instruite que la leur. Mes parents c'est parfois moi qui doit leur dire « fait quand même gaffe »

Juliette : mes parents, ils en savent un peu car il y a déjà eu des reportages, le journal,...ils regardent plus cela que moi. Ils m'en informent mais c'est vraiment les bases.

Maud : mes parents me disent « fais attention à tes informations » mais ils savent pas où vos nos informations. Ils préviennent mais ils comprennent pas les mécanismes. Par exemple, avant ma mère voulait qu'on télécharge une application spéciale qui garde pas nos données mais on

l'a jamais fait. On a une conversation de famille sur what's app et tous les mois elle nous envoie un lien « signal » en nous disant aller sur Signal c'est plus sécurisé mais on l'a jamais fait

Juliette : c'est vrai qu'on sait tous mais sans savoir. On fait rien pour changer cela et protéger nos données car on ne sait pas comment on doit faire, que ce soit nos parents ou nous.

Maud : ma maman elle pense que What's app c'est mieux que Signal pour les données etc donc elle nous dit d'aller dessus mais sans pousser non plus car elle sait même pas trop pourquoi c'est mieux et donc on n'a jamais installé Signal. Elle pense que comme ça n'appartient pas à Facebook il y a moins de dangers.

Juliette : mon oncle nous a envoyé un message sur les paramètres de confidentialité de what'sapp qui avaient été modifiées et donc qu'il fallait aller modifier nous même ces paramètres. C'est un message qui tourne sur Facebook et What'sapp et donc mon oncle nous l'a envoyé et il est noté tout ce qu'il faut changer soi-même dans les paramètres.

Maud : oui ma maman a aussi reçu ce message et c'est entre autre pour ça qu'elle voulait changer.

Louis : mon papa sait des choses grâce à son travail car il doit contrôler le trafic de certaines choses qui se fait sur internet et donc il sait ça. Par contre ma maman, elle apprend en même temps que nous.

Théo : mon parrain fait partie de la sécurité et m'avait dit qu'il ne publiait jamais des photos de ses enfants surtout en bas page car elles pourraient être réutilisées sur des sites illégaux, etc. Il a averti mes parents mais mes parents ne le font pas car comme nous, on se dit que c'est « impensable » de faire ça, on ne se rend pas compte de tout ce qui tourne derrière les écrans et on comprend pas les mécanismes.

5) Autre

Il existe de nombreux sites internet qui proposent des formations en ligne pour les parents, les enseignants mais aussi les enfants et les adolescents. (Via la commission européenne, l'autorité de la protection des données etc) Prendriez-vous le temps d'aller faire des petites formations en ligne maintenant que vous savez que cela existe ?

Tout le monde la même réponse : jamais

Louis : et même si on avait envie de le faire on est même pas au courant que cela existe.

Selon vous, est-ce l'école, vos qui auront le plus d'impact à vous conscientiser à la protection de vos données personnelles ?

Juliette : l'école ça serait le mieux mais aussi sur internet

Louis : oui l'école serait le mieux et internet c'est vrai que c'est paradoxal.

Maud : des Youtubeurs ont déjà fait des codes promos pour des logiciels/ application de sécurité de données. C'était payant donc les gens vont pas payer mais bon.

Mis à part les parents et l'école, pensez-vous pouvoir vous sensibiliser à cela par d'autres moyens ? Par exemple, via les médias, le bouche-à-oreille, des documentaires, des minis formations en ligne. Pensez-vous que cela aura le même impact ?

Juliette : peut-être des pages Instagram qui pourraient sensibiliser car on est beaucoup là-dessus et certains comptes Instagram sont très instructifs mais c'est un peu paradoxal de s'instruire de ça sur les réseaux.

Maud : pour les jeunes, un Youtubeur super connu, qui fait toujours des milliers de vues, que les gens croient (il raconte pas n'importe quoi dans ses autres vidéos) que tout le monde regarde, qui fait une vidéo avec un expert sur ça cela pourrait sensibiliser plein de jeunes. Et c'est une plus chouette façon d'être conscientisé et comme c'est un Youtubeur qu'on regarde souvent et qui est réputé pour ne pas dire de connerie les gens auraient confiance en ses propos.

Juliette : Je pense que c'est une bonne idée et à l'école aussi car déjà sur internet y'a beaucoup de fake news. Mais à l'école ça serait bien d'avoir un professionnel qui vient et qui fait des chouettes activités, qui est calé là-dedans, cela aura plus d'impact que si c'est notre prof de français qui nous parle 10 minutes de ça pendant son cours.

Maud : oui à l'école ça serait top, comme on a les formations du planning familial il faudrait avoir une fois par an une formation sur tout le numérique avec le cyberharcèlement, les données personnelles,...

Juliette : oui je suis d'accord, plus pour sensibiliser que d'avoir un cours là-dessus.

Sybille :cette année une nouvelle option a ouvert, sur l'écologie et la transition, donc pourquoi pas ouvrir un cours lié à ça et sur l'informatique mais aussi l'éthique de tout ça.

Juliette : oui mais alors si c'est une option tout le monde n'aura pas accès alors que si c'est des formations comme on a le planning familial, tout le monde peut y avoir droit.

B) Entretien semi-directif avec un directeur d'école

1) Introduction :

Etudiante en Sciences de Gestion à l'UCL, je rédige actuellement mon mémoire qui porte sur la problématique des données personnelles. Je souhaite voir si l'éducation à la citoyenneté numérique pourrait être une solution pour conscientiser les jeunes à la protection de leurs

données personnelles. L'éducation pourrait passer par l'école et il serait intéressant d'avoir votre point de vue à ce sujet.

2) Sujet général :

Avant toute chose, savez-vous ce qu'est une donnée personnelle et une donnée sensible ? Êtes-vous au courant que les données personnelles sont collectées, bien souvent sans le consentement réel des utilisateurs ? Vous avez sûrement déjà remarqué les bannières publicitaires etc.

Alors oui, comme directeur j'ai à traiter des données qualifiées de données personnelles qui sont sujettes au RGPD. Comme directeur d'école, je dois prendre toute une série de disposition afin d'en garantir la sécurité. Sur internet, comme tout citoyen, j'ai conscience des potentiels dangers de fuites de données à des fins marketing ou autre.

3) Enseignants:

Pensez-vous que les professeurs actuellement parlent à leurs cours de ces dangers ? Les enseignants ont-ils actuellement les connaissances nécessaires pour pouvoir informer et conscientiser les élèves à protéger leurs données personnelles et à agir en bon citoyen numérique ?

Oui, très certainement. Il faut savoir que tous les enseignants, tous les membres du personnels ont accès à des données dites confidentielles et ils sont donc tenus à un certain secret professionnel qui existait bien avant le RGPD mais aujourd'hui, l'enseignant a des informations qui relèvent de l'intimité dans certaines familles donc ils sont très sensibilisés à cela. En début d'année, dans toutes les écoles, tous les enseignants signent une adhésion à certains articles du RGPD disant « je m'engage à respecter telle et telle chose ». Le texte est très long donc nous l'avons résumé en une dizaine d'article. Chaque membre du personnel est donc sensibilisé à la question et d'une manière ou d'une autre cela va transparaître à travers les cours. Certains cours plus que d'autres bien entendu. Un cours de français ou de religion fera plus de places aux questions éthiques que le cours de math mais certainement oui.

Ces questions n'interviennent pas dans les programmes et les référentiels de cours mais les enseignants ont bien conscience qu'ils ont un rôle d'accompagnement de la jeunesse bien plus large que le contenu des programmes et donc ces questions-là sont bien présentes dans les cours. Mais tel quel il n'y a pas de prof désigné pour sensibiliser les élèves à ces questions-là.

Avez-vous déjà organisé des formations pour les élèves ? Par exemple, l'intervention d'une personne extérieure formée à ce sujet qui est venue parler de la problématique aux élèves ?

Oui, dans l'école, il y a toute une série d'animation et de partenaires extérieurs qui viennent traiter des questions au sens large de communication aux élèves. En première par exemple, le service jeunesse de la police fédérale est venu expliquer à nos élèves ce qu'était le droit à l'image, le droit à l'intimité, au respect de la vie privée, aux menaces et dangers des réseaux sociaux. On peut partager des choses sans l'accord de l'autre,...L'importance de ce rôle, c'est que la police se montre partenaire dans un rôle pédagogique et pas répressif et ouvre les yeux de nos élèves sur les potentiels dangers, y compris au niveau pénal. Il éduquer et pour cela nous avons des partenaires extérieurs dont la police.

On a eu jusqu'à avant le covid avec une ASBL qui s'appelle ACBJ, agréée par la Fédération Wallonie-Bruxelles qui est venue elle aussi informer nos élèves. Ils venaient en 5^{ème} pour parler notamment des droits d'auteurs et de la problématique de plagiat par exemple lors de la rédaction des travaux de fin d'étude. C'est une question un peu nouvelle dû au déploiement du numérique ces dernières années.

Pour résumer, on a donc des partenaires extérieurs, les profs en interne également mais nous n'avons pas un programme de cours tel quel pour cela.

Les enseignants ont-ils déjà assisté à des formations à ce sujet ou pris part à des activités dans le cadre de l'école ? (lors d'une journée pédagogique par exemple) Si oui, pouvez-vous m'en dire plus ? Par qui était-ce donné ? Etait-ce adressé à tous les enseignants ?

Non, pas spécifiquement sur ces questions là.

Pensez-vous qu'il serait intéressant de former les enseignants à ce sujet ? Pourquoi ?

Cela se fait un peu de manière incidente. Il faut savoir que comme dans beaucoup d'écoles, on déploie ici le recours à une plateforme numérique, Smartschool, outil de communication extraordinaire qui permet interactions entre élèves, professeurs, parents, directeurs, éducateurs donc c'est super. Mais, à chaque fois qu'on active de nouveaux modules ou fonctionnalités, on se rend compte qu'il y a des questions d'ordre éthiques qui se posent. Un prof de math peut-il avoir accès aux commentaires du commentaires de NDLS de son enfant qui est élève dans l'école, ou d'un autre enfant. Comment réguler cela ? Comment faire en sorte que la plateforme ne devienne pas un Facebook local ? Donc il a fallu, là aussi, faire adhérer l'ensemble de la communauté scolaire à des règles. Cette plateforme elle relève du Pédagogique, au sens large bien-sûr. L'outil nous a été très utile surtout lorsqu'on est passé à l'enseignement hybrid. On

avait déjà déployé cet outil, et on a fait un bon en avant dans le numérique tant au niveau éthique que technique. On a dû rappeler aux parents et aux élèves les règles et rappeler que c'est un outil pédagogique et éducatif.

4) Les élèves et l'école

Pensez-vous que l'école à un réel rôle à jouer dans l'éducation des enfants et adolescents concernant le numérique ?

Bien-sûr ! On constate un sacré retard dans la fédération Wallonie Bruxelles. Par exemple, notre coordinateur informatique, certaines semaines il fait 70h alors qu'il n'a qu'une 20aine d'heure de cours d'informatique. et la fédération ne donne aucun moyen aux écoles pour encadrer ce déploiement numérique. Tout directeur doit s'adapter, et par exemple trouver un prof d'informatique qui n'a pas un horaire complet, lui donner quelques heures non chargées de cours. Souvent ce sont des gens passionnés, qui aiment ça mais on n'a pas de moyen humain pour accompagner ce virage numérique dans les écoles. Quant à l'intégrer dans les programmes de cours, là non plus ce n'est pas là, la Fédération dit « on ne va pas faire ça maintenant, on va attendre l'arrivée du tronc commun, nouveau diplôme qui interviendra à 15 ans et non plus en fin d'école primaire, on va intégrer tout ça mais ça viendra plus tard. Mais le changement il est là maintenant. Donc il y a un décalage, un manque de réactivité par rapport à la réalité que vivent les écoles parce que le virage numérique on est en plein dedans. Nous ici notre école ça va on a su anticiper mais je connais plein d'écoles qui sont complètement à la traine au point d'envoyer encore des e-mails généraux pour communiquer avec les parents par exemple.

Pensez-vous qu'il devrait être obligatoire de former les élèves et les enseignants à cette problématique, ou du moins de tenter de les conscientiser ?

La révolution numérique qu'on est en train de vivre mériterait sans doute que l'école se dote de programmes de cours et de contenu. Je crois que cela manque. Au niveau des référentiels et des programmes par exemple en informatique, c'est la suite office et les choses basiques, un peu de codage, mais ce sont des programmes déjà anciens alors qu'il y a des tous nouveaux logiciels. Mais avant que ces nouveaux logiciels entrent dans les programmes, on sera déjà passé à autre chose car justement ce sont des matières dans lesquelles on a du mal à suivre tellement cela va vite. Donc je pense que éduquer au numérique devrait être présent dans les grilles horaires de tous nos élèves. A travers quels cours, pas nécessairement l'informatique mais de fait il y a un déficit d'accompagnement ou chacun se débrouille un peu avec les moyens qu'il a.

5) Projets futurs

Y-a-t-il des projets futurs de la part de la fédération Wallonie Bruxelles ou même de la ministre à mettre en place concernant l'éducation au numérique ?

Par rapport aux cours, non je sais qu'il n'y a rien. Par rapport à l'accompagnement en personne, en ressource humaines, je sais qu'il n'y a rien, et nous directeur on se bagarre pour qu'il y ait enfin la reconnaissance d'un référent numérique dans chaque école. En fait en fonction de ton nombre d'élèves, tu as droit à autant d'éducateurs, autant de profs, une ou deux secrétaire etc mais au niveau du numérique il n'y a rien. Et on en a besoin absolument. Ici moi je me débrouille, j'ai des équipes en or et on arrive à s'en sortir pour le moment mais dans certaines écoles c'est la galère totale et où ça n'avance pas donc l'école accentue son décalage face au monde qui n'arrête pas de changer et qui change de plus en plus vite. Donc je sais qu'au niveau des programmes il n'y a rien de prévu sauf avec l'arrivée du tronc commun mais cela arrivera pour les premières années en 2026 donc dans 5 ans au regard de l'évolution numérique, on sera déjà dans un autre monde. Au niveau des ressources humaines, on réclame, insiste auprès de la ministre.

On est demandeur et on ne reçoit pas assez.

C) Entretien semi-directif avec Virgie Tyou

Bonjour Virginie,

Je me présente, je suis étudiante en sciences de Gestion à l'UCL, je termine mon mémoire. Je réalise mon mémoire sur tout ce qui touche au numérique. La problématique de mon mémoire est de voir si l'éducation à la citoyenneté numérique peut être une solution à long terme pour conscientiser les jeunes à protéger leurs données personnelles. En discutant avec ma marraine, enseignante, elle m'a transmis vos coordonnées puisque vous êtes déjà intervenue dans son école.

Pouvez-vous vous présenter en quelques mots ?

Bonjour, je m'appelle Virginie Tyou, je suis auteure, conférencière formatrice et Hypnothérapeute. Je fais des formations sur le numérique dans les écoles, pour les élèves et les enseignants et je commence aussi à organiser cela pour les parents. J'ai écrit plusieurs livres sur le numérique qui s'appellent « Cliky » Cliky, le personnage principal, est une donnée personnelle.

Avant toute chose, je tenais à vous dire que j'ai réalisé des petits entretiens avec des élèves, qui ont maintenant 15 ans mais qui ont eu la chance de participer à une de vos formations et ils m'en ont parlé, ça les a marqués.

Cela me fait doublement plaisir car mon idée est qu'il fallait intervenir bien avant qu'ils soient adolescents donc pour moi l'idée de la protection des données personnelles etc, c'est l'idée de la protection de la vie privée, et si on creuse un peu plus c'est la protection de l'intimité. J'ai terminé un mémoire universitaire l'année derrière en hypnose thérapeutique ou j'ai travaillé sur la notion de l'intimité, si celle-ci pouvait se développer chez les enfants à partir de 8 ans et donc est-ce que cela avait un impact sur leur niveau de connexion. La réponse était oui. En même temps j'ai étudié de manière théorique le fait que d'après les pédopsychiatres, le rapport à l'intimité se construit à partir de 8 ans chez les êtres humains et puis ce n'est pas linéaire, il y a des phases en dangers qui correspondent à l'adolescence, et ces mises en dangers dans le monde physique comme avant, on a tous déjà fait cela. On fait quelques conneries et puis on se dit qu'on ne le fera plus et cela ne porte pas en conséquence. Seulement dans le monde numérique, cela porte en conséquence car tout ce qui est diffusé de soi n'est jamais effacé. On a donc un vrai problème. Donc pour moi c'était une évidence qu'il fallait parler aux enfants du numériques avant qu'ils soient adolescents. L'idée derrière était que, quand ils ont 8-9 ans, on va les familiariser à la protection de leur intimité. Qu'est-ce que c'est l'intimité ? Qu'est-ce que c'est ma vie privée ? Qu'est-ce qui est secret ? Qu'est-ce qui ne l'est pas ? Qu'est-ce que j'ai envie de garder ma vie pour moi ? L'idée est de travailler cela avec les enfants et avec Cliky, le personnage du livre. On les fait déjà réfléchir sur ce qu'est une donnée personnelle. Je peux vous dire que cela fait 6 ans que je fais ça et que ça fait 6 ans qu'aucun enfant sait au départ ce que c'est. Mon intention par la suite, c'est que quand on a appris grâce au livre, avec Cliky, cette petite boule jaune « mascotte », un personnage sympa, c'est quelque chose qui reste même quand on devient adolescent. C'est sous-forme imagée et on s'en souvient bien mieux car il y a de l'affectif, de l'imaginaire et de l'émotionnel.

Quel est votre objectif avec Cliky ?

Mon objectif c'est qu'à un moment donné cela prenne la place dans l'école primaire. Avec cliky, on peut faire des stats, peut travailler dans le cadre du calcul, par exemple faire des pourcentages des enfants qui ont un ordinateur chez eux, une tablette, un smartphone. On peut travailler tout ce qui est compétence émotionnelle, intimité,... On peut lire d'autres choses là dessus. Dans une école à Vervier, Cliky est pendant les classes. Ils ont créé un immense Cliky. Le livre une fois qu'il est lu il est lu mais là ils l'ont installé et cela permet aux enseignants de revenir à chaque fois là-dessus lorsqu'il y a un souci ou une discussion autour du numérique.

On revient donc à Cliky, qui est l'essence d'internet, la data. Et donc quand ils partent dans le secondaire, ils partent avec un bagage. L'adolescence c'est à ce moment-là qu'on ferme ses oreilles, on n'a plus envie d'écouter les bons conseils des parents et des enseignants. Si l'essentiel est déjà en eux avant d'arriver dans le secondaire, il y aura moins de problèmes.

Pour moi l'essentiel du travail de l'éducation à la donnée personnelle doit se faire déjà en primaire.

J'ai observé également que plus vous allez à la campagne, dans des petites écoles, plus ils sont connectés. Le niveau de connexion dépend du niveau socio-culturel des parents. Donc plus il est bas, plus les enfants sont connectés alors qu'on pourrait croire que c'est le contraire. Quand vous êtes dans une grande ville ou dans un grand village comme celui de l'école de ta marraine, vous aurez beaucoup moins d'enfants sur Tik-tok que si vous faites la même enquête à Marche-en-Famenne à la campagne car les parents éduqués connaissent mieux les risques et ont une réflexion par rapport aux écrans donc il y a une règle qui est installée. Les écrans marchent tout le temps, la télé aussi et ce n'est pas parce qu'on est à la campagne qu'on est plus dehors. Je l'ai vérifié en France aussi et c'est pire en France. Dans le Sud de La France, en CE1 ils ont 8 ans dans des petits villages, les $\frac{3}{4}$ de la classe ont un smartphone. J'aurais aussi pensé le contraire, que c'est dans les milieux aisés qu'on donnerait une tablette à l'enfant mais non. Cela veut dire que pour moi, c'est encore plus essentiel que cela soit traité à l'école primaire, qui est l'école pour tous, pour donner une chance à tous les enfants de s'éveiller à une certaine conscience. D'ailleurs, je travaille aussi dans le sud de la France avec une association qui s'appelle « Peps aude », et la directrice de cette association travaille dans un centre de parentalité et d'éducation périscolaire avec des enfants plutôt défavorisés, et un petit lui a dit « en fait cliky, j'ai appris que c'était la conscience d'internet et je ne savais pas qu'il fallait avoir une conscience de cela ».

Quand j'étais petite, j'ai 52 ans, à l'école primaire il y avait des cours d'hygiène corporelle. On nous apprenait qu'il fallait se laver les mains après avoir été aux toilettes, qu'il fallait prendre une douche tous les jours. Je dis qu'aujourd'hui, il faudrait des cours de base numérique. Cela commence par savoir comment cela fonctionne, pourquoi on doit se protéger,....

En primaire on a des cours d'informatique pour tous les élèves, en secondaire ce n'est qu'une option, mais on apprend pas l'éthique, comment se comporter. Effectivement on n'apprend aucune réflexion. On oublie le volley émotionnel et éducatif. Qu'est-ce que c'est une donnée personnelle ? Qu'est-ce que je garde ? Comment ce monde fonctionne ? Simplement les règles de base. C'est un monde qui fonctionne sur de la data, tout est fonction de ça.

Selon, vous cela serait plus intéressant de mettre en place un cours consacré à toutes les thématiques liées au numériques, ou l'intégrer à un cours actuel comme le cours d'informatique, ou autre chose ?

Ils veulent faire des cours de cyber-citoyenneté mais si vous le faites comme à l'ancienne, c'est-à-dire avec des règles à apprendre, sans conscience et sans émotionnel, avec le numérique cela ne fonctionne pas. Les enfants y sont déjà et aiment beaucoup ça. Cela a beaucoup d'impact sur nous, sur notre cerveau, sur nos émotions. Donc, selon mon avis, on ne peut pas éduquer les enfants comme avant. Cela doit venir d'eux. Il faut qu'ils sentent les choses, réfléchir, pourquoi on dit que je ne peux pas donner mon adresse mail à tout le monde ou que je ne peux pas dire où j'habite ? Pourquoi Finalement ? Il faut qu'il y ait le « pourquoi » et le « qu'est-ce que cela a comme impact. Et pas juste la petite phrase « sécurisez cela, faites attention à cela » car ça ce sont juste des gens qui vont se dire ok je dois pas le faire mais pour rentrer sur Tiktok je dois les donner donc tant pis je les donne. Ou pour aller sur ce site je dois accepter cela donc j'accepte tout. Cela a un tel impact dans notre vie, il faut donc d'abord que l'enfant ait un intérêt à respecter ces règles-là.

Bien sûr il faut commencer par former les enseignants. Vous avez dit au début de l'interview que vous formiez les enseignants. Comment cela se passe ?

Oui, j'ai commencé à le faire. Cela prend bien par exemple en France. Ce qui m'embête c'est que c'est souvent des professeurs de collège donc l'équivalent de la 6^{ème} primaire chez nous, mais j'essaye de pousser que ça soit en primaire mais plus tôt. Mais c'est compliqué car on est dans une politique où c'est quand il y a les crashes qu'on met quelque chose en place. Les crashes ils arrivent vers 13-14 ans donc on se dit on va les former à cet âge-là mais si on veut qu'il n'y ait pas de problème à 13 ans il faut commencer à les former à 8 ans.

Et c'est vrai qu'il faut former les enseignants car il leur manque deux choses. 1) ce n'est pas des pros du net, et c'est logique. 2) il y a tout le volet psychologique et psychopédagogique qui doit être changé aussi. Apprendre le numérique avec des règles, cela ne marche pas. Ça c'est l'enseignement d'avant. C'est quelque chose qui doit être beaucoup plus en pratique. Cliky doit repartir dans les familles. Je travaille dans les écoles et j'essaye que dans les écoles, ils fabriquent un cliky qui va repartir dans les familles pour voir comment les familles vont s'acclimater elles-mêmes. Alors attention un autre point par rapport à cela, les enfants savent généralement bien plus que leurs parents car les parents sont au courant de rien, donc c'est bien aussi qu'il y ait une transmission de l'enfant vers son parent car cela permet aussi qu'il y ait un vrai dialogue entre enseignant parent et enfant. C'est essentiel ce dialogue et c'est plus facile à l'école primaire. Mais pour cela, oui il faut une formation des enseignants. J'essaye pour le

moment de la limiter à deux jours mais pour bien faire il faudrait des séminaires d'une semaine pour vraiment aller dans tous les volets que ça soit technologique mais aussi philosophique et psychologique. Et là c'est parfois compliqué avec certains enseignants car ils ont été formé à éduquer mais ils disent qu'ils ne font pas de psychologie et ils disent qu'on accompagne pas. Sauf que avec le numérique, des nouvelles compétences doivent être mises en place.

Maintenant on me demande de former également certains thérapeutes, psychomotriciennes, logopèdes, neuropsychologues car ils commencent à avoir des soucis en cabinet. Il y a de plus en plus de demande pour des retards de langage, des soucis de concentration directement liés à l'utilisation des écrans. Ils ne sont pas des pros du net non plus. Alors d'un côté quand on leur parle d'intimité, d'empathie, ça ça leur parle évidemment plus que des profs mais pas le volet numérique. Il y a un manque de connaissance et de conscientisation et on s'y prend trop tard.

Pour vous, les formations sont essentielles ? Plus que des campagnes de prévention par exemple ?

Je ne suis pas du tout contre les campagnes de prévention de Child focus ou autre mais ce n'est pas de l'éducation au numérique. C'est de la prévention, des animations d'une heure dans une école, que voulez-vous que ça change ? En plus ils forcent le trait pour attirer l'attention des adolescents sauf qu'en faisant cela, les adolescents qui sont sur internet et c'est leur quotidien, ils n'ont pas du tout envie d'entendre ça. Justement une des choses qui a fait que je me suis lancée c'est que ma fille a eu un jour ça à l'école elle m'a dit « maman on a eu une cyber animation c'était tellement horrible ce qu'ils racontaient sur les réseaux, que des gens derrière nous observaient etc qu'en fait on s'est tous dit on écoute rien du tout ». Cela durait 50 minutes ! Les pouvoirs publics avec cela ils se disent qu'ils ont la conscience tranquille, les jeunes ont eu l'info mais non.

Les écoles souhaitent avec des formations à ce sujet ? Avez-vous beaucoup de demandes ?

Quand j'avais commencé en 2015, j'avais rencontré un éditeur qui m'avait dit 'publier un truc sur internet non, c'est juste une mode ». Donc en 2015 certains pensaient encore qu'internet était une mode lors que c'est une révolution complète de notre monde, de nos pratiques et presque de notre manière d'exister.

Quand j'ai commencé dans certaines écoles, certaines étaient vraiment précurseur là-dessus mais d'autres écoles, elles me disaient en 2015 « ah non non faut surtout pas leur parler de ça hein, vous allez les inciter à aller dessus ». Maintenant cela change, je suis bien occupée avec ça et beaucoup d'écoles souhaitent se former mais j'aimerais bien former les enseignants et qu'ils soient à l'aise pour en parler. Ca c'est vraiment la prochaine étape. Et j'ai même certaines demandes des maternelles ! Les maternelles parce que les rentrées scolaires sont de plus en plus

connectées, c'est-à-dire que certains parents qui arrivent et qui expliquent que si l'enfant pleure, la tablette est dans le sac à dos. Ou à la récréation, il ne mange que s'il regarde quelque chose. Et les enseignantes maternelles, elles me demandent, votre cliky, quand est-ce que vous allez faire un livre jeunesse. Moi je suis un peu entre les deux, je me dis que 8 ans c'est déjà bien mais voilà.

Organisez-vous également des formations pour les parents ?

Je fais des ateliers pour les parents, dans des centres pluridisciplinaires où il y a des logopèdes etc. je commence à donner des formations pour qu'elles puissent donner des ateliers cliky. Car les parents et les enfants sont trop connectés. Il faut savoir qu'il y a des familles où ils ne parlent plus car ils sont tous sur les écrans tout le temps, même en mangeant. Et donc il y a des retards, des petits bouts de deux ans qui ne parlent pas car leur parents ne leur parlent pas. Donc les personnes qui bossent dans ces centres veulent créer des ateliers parentaux pour que les parents changent leur pratique.

Les parents n'ont pas les connaissances, ils n'ont pas idées. En France, ce qui marche bien c'est dans les médiathèques. Je fais une tournée des écoles et fin de journée, quand les parents viennent rechercher leurs enfants, je suis à la médiathèque, il y a des cakes, à boire,...et les parents sont accueillis et peuvent poser toutes leurs questions. Ils ne sont pas jugés dans leurs démarches. J'ai créé une association justement et l'idée c'est de créer des tiers lieux ouverts, donc des petits espaces cliky, dans les écoles ou médiathèques ou autre et qu'il y ait une personne relais qui serait formée pour avoir quelques heures par mois d'ouverture aux parents qui auraient des questions. Même pour les grand-parents ou les enfants. « mon enfant me demande a, est-ce une bonne idée » « combien de temps d'écran ». La personne relais ne doit pas tout savoir et ne répondra peut-être pas mais aura été formée à réceptionner les questions des parents en tout cas. Cela devrait se faire dans les écoles, mais aussi dans les espaces de culture, centre pédiatriques, association périscolaire. Un espace ouvert où on peut commencer à se renseigner.

L'enseignant avant on lui apprenait à tout savoir sur un sujet, il maîtrisait parfaitement sa matière et il avait le savoir. Sauf que avec le numérique, il y a tous les 6 mois quelque chose de nouveau. Donc c'est important de savoir, se poser une question et essayer de chercher la meilleure info possible. C'est une démarche action-recherche. Donc cela change la position de l'enseignant. C'est pour aussi qu'il y avait un frein au début. J'ai voulu tester quand j'ai lancé cliky, dans la classe de ma fille. C'était une enseignante proche de la retraite et quand j'ai été la voir pour lui présenter le projet elle m'a dit « c'est sur quoi ? » je lui ai dit « sur le

numérique », elle m’a répondu « oh non non ça je ne peux pas je me sens pas à l’aise. » Et je lui ai dit justement vous êtes la personne idéale, le but n’est pas que vous sachiez mais que vous trouviez ensemble, que vous ameniez les enfants dans le questionnement. Finalement elle était ok, elle a même changé sa démarche d’enseignement elle ne se mettait plus devant la classe mais au centre avec les enfants pour avoir une réelle réflexion.

L’approche entre les parents et les enseignants est-elle différente ?

Oui, les parents c’est plutôt autour de la gestion de l’écran, et comment ça fonctionne, car ils n’ont vraiment aucune connaissance. Je fais des ateliers d’une heure une heure et demi max alors que la formation des enseignants c’est différent j’explique vraiment le concept, on détaille Cliky. Je travaille vraiment sur le processus d’apprentissage. J’essaie de parler avec leur langage à eux. Ce sont des pédagogues, ils ont les clés de l’apprentissage et je leur montre que le pour le moment le numérique se situe au stade 4 dans la consolidation. Pour le moment, l’apprentissage du numérique à l’école on utilise le stade 4 et on oublie les 3 premiers stades qui sont, si je me souviens bien :

- 1) L’attention qu’on porte à une matière
- 2) L’implication, donc « je m’implique, cela me concerne »
- 3) Le retour sur erreur, c’est-à-dire la permission que les enfants pourraient avoir de dire « oulala moi là j’ai bien déconné sur ce site-là »

Et puis grâce à ce retour sur erreur, on peut se dire ah ok « qu’est-ce que tu avais oublié, qu’est-ce que tu n’avais pas compris, qu’est-ce que tu ne savais pas encore ».

⇒ C’est sur base de ces trois étapes là d’apprentissage qu’on peut consolider en disant « qu’est-ce que je vais retenir de tout ça, qu’est-ce qui est essentiel pour moi de savoir »

Et là on peut en tirer des règles, des règles de vie, de comportement.

Mais si on vient directement avec l’étape 4, les règles, sans passer par les trois étapes précédentes, on ne retient rien. Donc On passe une matinée à se demander comment peut-on remettre l’enfant dans un véritable processus d’apprentissage de ce qu’est le numérique. Puis l’après-midi, on travaille sur une des facettes, par exemple les réseaux sociaux, comment cela fonctionne, l’impact que cela a sur notre cerveau, quelles sont nos émotions, qu’est-ce qu’on va rechercher là-dessus. Pourquoi on est si hypnotiser quand on est là-dessus. Puis, un autre volet sur une demi-journée sur l’algorithme, par rapport à tout ce qui est esprit critique car là c’est une catastrophe, je dois expliquer à des adultes que ce qu’ils voient sur Facebook c’est ce que Facebook pense qui va leur plaire. On est renforcer dans nos convictions tout le temps. Et enfin, la dernière demi-journée, c’est vraiment gérer les émotions. Les enfants et internet, c’est que de l’émotionnel. Plus on grandit, plus on va chercher du sensationnel. Ça fait partie de leur

vie, c'est comme ça qu'ils expriment leurs émotions. Comment ça se fait que je peux plus facilement me lâcher devant un écran que si j'étais en face de la personne ? Il faut vraiment intégrer une connaissance de soi. Alors oui ils sont petits mais on n'a pas le choix. L'aspect éducation émotionnelle et connaissance de soi vient plus jeune.

Vous organisez des formations en primaire et en secondaire ?

En France pour les deux car finalement ce sont des profs de collège mais en Belgique je cible les enseignants du primaire même si ça ferait du bien au secondaire. Cela devrait être à tous.

Par rapport à votre rôle d'intervenante, les profs sont pour le moment ne sont pas formés donc c'est vous qui intervenez dans les écoles ?

Oui jusqu'à présent c'est moi mais c'est pour ça que j'ai créé une association, l'idée c'est que moi je continuerai à former des adultes, les enseignants. Et puis eux pourront en parler à leur collègue et pourront faire les animations à ma place. Ce qui me plairait aussi, c'est un projet pour 2022, ce qu'aussi les jeunes enseignants des hautes écoles soient former également. Selon moi c'est super important. Cela fait que se développer ! Par compte, je compte bien garder deux écoles par an que je visiterais car pour moi tout ce que je fais cela vient de ce que j'apprends des enfants, de la manière dont ils le vivent et ça c'est super important de rester tout le temps, comme je dis c'est de la recherche-action. Pas de se dire « parfait j'ai fait une super méthode, j'ai plus besoin d'aller les voir » car cela change tout le temps, il faut évoluer et s'adapter.

Annexes 2 : Questionnaires des enquêtes quantitatives

Questionnaire enseignants :

Enquêtes sur la protection des données personnelles - Enseignants

Bonjour,

Étudiante en Sciences de Gestion à l'UCL, je réalise mon mémoire sur la problématique suivante: "En Europe, l'éducation à la citoyenneté numérique est-elle une solution à long-terme pour conscientiser les utilisateurs à la protection de leurs données personnelles ?". L'école a-t-elle donc un rôle à jouer dans cette éducation? Pourriez-vous prendre quelques minutes de votre temps pour répondre aux questions ci-dessous?

Merci beaucoup!

***Obligatoire**

1. Êtes-vous un enseignant en école primaire ou secondaire ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

Enquêtes sur la protection des données personnelles - Enseignants

Pour les enseignants uniquement

2. Savez-vous ce qu'est une donnée personnelle ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

En Europe, selon Règlement Général de la Protection des Données (RGPD), une donnée personnelle est "toute information se rapportant à une personne physique identifiée ou identifiable". Par exemple, nom, prénom, adresse, plaque d'immatriculation mais également l'opinion politique, les intentions d'achats,...

7. Avez-vous déjà suivi des formations/ conférences sur les dangers d'internet? *

Une seule réponse possible.

- ☐ Oui, dans le cadre de l'école (journée pédagogique,...)
☐ Oui, à titre privé
☐ Non

8. Avez-vous déjà discuté de la protection des données personnelles et de la vie privée sur Internet avec vos élèves? *

Une seule réponse possible.

- ☐ Oui
☐ Non

9. Si oui, dans quelles circonstances?

Une seule réponse possible.

- ☐ "Par hasard", au détour d'une conversation
☐ En organisant une activité/ un cours dans le but de les conscientiser à cela

10. Pensez-vous avoir les connaissances nécessaires pour pouvoir conscientiser les élèves à la protection de leur vie privée et de leurs données personnelles sur Internet? *

Une seule réponse possible.

- ☐ Oui
☐ Non

3. Utilisez-vous les grandes plateformes comme Google, Facebook, Amazon, Airbnb, Uber,...? *

Une seule réponse possible.

- ☐ Oui
☐ Non

4. A quelle fréquence? *

Une seule réponse possible par ligne.

	2,3,4...x/jour	1x/ jour	1 à 2x/semaine	1 à 2x/mois	Jamais
Utilisation	☐	☐	☐	☐	☐

5. Savez-vous que ces plateformes collectent vos données personnelles sans votre réel consentement et que vos données sont ensuite revendues à des entreprises qui les utilisent principalement à des fins publicitaires? *

Une seule réponse possible.

- ☐ Oui
☐ Non

6. Comment savez-vous cela? *

Une seule réponse possible.

- ☐ Via les médias (scandales comme Cambridge Analytica par exemple)
☐ Par le bouche-à-oreille
☐ Depuis l'apparition du Règlement Général de la Protection des données (RGPD)
☐ En surfant sur Internet (pub bannière sur des sujets qui m'intéressent,...)
☐ Je n'étais pas au courant de cela

11. Pensez-vous pouvoir vous-même expliquer et montrer aux élèves les démarches à suivre pour protéger leur vie privée et leurs données personnelles sur Internet? *

Une seule réponse possible.

	1	2	3	4	
Oui, tout à fait	☐	☐	☐	☐	Non, pas du tout

12. Pensez-vous que l'école a un rôle à jouer dans l'éducation au numérique pour les enfants et les adolescents? *

Une seule réponse possible.

- ☐ Oui
☐ Non

13. Pensez-vous que les parents éveillent suffisamment leurs enfants à cette problématique? *

Une seule réponse possible.

- ☐ Oui
☐ Non

14. Qu'est-ce qui devrait être mis en place pour éduquer les élèves à être un bon citoyen numérique? *

Plusieurs réponses possibles.

- ☐ Formation en ligne
☐ Activité ludique à l'école
☐ Sujet à aborder dans le cadre du cours d'informatique
☐ Sujet à aborder dans un cours donné à TOUS les élèves (formation générale)
☐ Conférence à l'école par des professionnels

15. Êtes-vous ? *

Une seule réponse possible.

- ☐ Une femme
☐ Un homme

16. Quel âge avez-vous ? *

Une seule réponse possible.

- ☐ 20 - 30 ans
☐ 31 - 40 ans
☐ 41 - 50 ans
☐ 51 ans et +

17. Êtes-vous enseignant dans une école ? *

Une seule réponse possible.

- ☐ Primaire
☐ Secondaire

18. Êtes-vous prof d'informatique ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

Questionnaire parents :

Enquête sur la protection des données personnelles

Bonjour,

Etudiante en Sciences de Gestion à l'UCL, je réalise mon mémoire sur la problématique suivante: "En Europe, l'éducation à la citoyenneté numérique est-elle une solution à long-terme pour conscientiser les utilisateurs à la protection de leurs données personnelles ?". Les parents ont-ils donc un rôle à jouer dans cette éducation? Pourriez-vous prendre quelques minutes de votre temps pour répondre aux questions ci-dessous?

Merci beaucoup!

*Obligatoire

1. Êtes-vous parent d'un enfant âgé entre 8 et 18 ans ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

2. Possédez-vous un smartphone et/ ou un ordinateur ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

Enquête sur la protection des données personnelles

pour les parents ayant un enfant entre 8 et 18 ans

3. Votre enfant possède-t-il un ordinateur ou un smartphone ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

4. Savez-vous ce qu'est une donnée personnelle ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

En Europe, selon Règlement Général de la Protection des Données, une donnée personnelle est "toute information se rapportant à une personne physique identifiée ou identifiable". Par exemple, nom, prénom, adresse, plaque d'immatriculation mais aussi l'opinion politique, les intentions d'achats,...

5. Utilisez-vous les grandes plateformes comme Google, Facebook, Amazon, Airbnb, Uber,... ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

6. A quelle fréquence ? *

Une seule réponse possible par ligne.

	2,3,4,...x/jour	1x/ jour	1 à 2x/semaine	1 à 2x/mois	Jamais
Utilisation	☐	☐	☐	☐	☐

7. Savez-vous que ces plateformes collectent vos données personnelles sans votre réel consentement et que vos données sont ensuite revendues à des entreprises qui les utilisent principalement à des fins publicitaires ? *

Une seule réponse possible.

- ☐ Oui
☐ Non

8. Comment savez-vous cela? *

Une seule réponse possible.

- ☐ Via les médias (scandales comme Cambridge Analytica par exemple)
- ☐ Par le bouche-à-oreille
- ☐ Grâce à des formations que j'ai suivies
- ☐ Depuis l'apparition du Règlement Général de la Protection des données (RGPD)
- ☐ En surfant sur Internet (pub bannière sur des sujets qui m'intéressent,...)
- ☐ Je n'étais pas au courant de cela

9. Êtes-vous inquiets pour le respect de la vie privée de vos enfants sur Internet? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

10. Avez-vous déjà sensibilisé vos enfants à la protection de leur vie privée et de leurs données personnelles? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

11. Pensez-vous avoir un rôle à jouer dans la conscientisation de vos enfants à la protection de leurs données personnelles? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

16. Si oui, par quel moyen?

Une seule réponse possible.

- ☐ Formation en ligne
- ☐ Formation organisée par l'école pour les parents
- ☐ Formation organisée par des associations ou des organisations
- ☐ Autre : _____

17. Avez-vous mis en place un logiciel de contrôle parental sur un ordinateur ou sur le téléphone de votre enfant? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

18. Quelle importance accordez-vous aux contrôles suivants? *

Une seule réponse possible par ligne.

	Très important	Important	Pas très important	Pas du tout important
Temps d'écran	☐	☐	☐	☐
Sites fréquentés	☐	☐	☐	☐
Réseaux sociaux	☐	☐	☐	☐
Achats en ligne	☐	☐	☐	☐

19. Quel(s) contrôle(s) appliquez-vous réellement? *

Plusieurs réponses possibles.

- ☐ Temps d'écran
- ☐ Sites fréquentés
- ☐ Réseaux sociaux
- ☐ Achats en ligne

12. Pensez-vous avoir les connaissances nécessaires pour éveiller vos enfants à cela? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

13. Pensez-vous pouvoir vous-même expliquer et montrer à vos enfants les démarches à suivre pour protéger leur vie privée et leurs données personnelles sur Internet? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

14. Savez-vous qu'il existe de nombreuses formations en ligne mises en place par des associations ou autres organisations pour s'instruire aux dangers d'Internet (dont le vol des données personnelles)? *

Une seule réponse possible.

- ☐ Oui
- ☐ Non

15. Avez-vous l'intention de vous former pour pouvoir sensibiliser vos enfants? *

Une seule réponse possible.

	1	2	3	4	5	
Absolument	☐	☐	☐	☐	☐	Pas du tout

20. Êtes-vous? *

Une seule réponse possible.

- ☐ Une femme
- ☐ Un homme

21. Quel âge avez-vous? *

Une seule réponse possible.

- ☐ 25 - 35 ans
- ☐ 36 - 45 ans
- ☐ 46 ans - 55 ans
- ☐ + de 55 ans

22. Quel est votre plus haut niveau d'étude? *

Une seule réponse possible.

- ☐ Diplôme primaire
- ☐ Diplôme Secondaire
- ☐ Etudes supérieures de type court
- ☐ Etudes supérieures de type long

23. Quel est votre statut? *

Une seule réponse possible.

- ☐ Indépendant
- ☐ Dirigeant d'entreprise
- ☐ Employé
- ☐ Ouvrier
- ☐ Demandeur d'emploi

Annexe 3 : Plans de codage

Enseignants :

Questions	Valeur dans SPSS	0	1	2	3	4
A	SUIVFORM A		Oui dans le cadre de l'école	Oui à titre privé	Non	
B	CONN	Non	Oui			
C	EXPL		Oui, tout à fait	Oui	Non	Non pas du tout
D	GENRE		Femme	Homme		
E	TYPE		Primaire	Secondaire		
F	AGE		20 – 30 ans	31 – 40 ans	41 – 50 ans	51 ans et +
G	DISCU	Non	Oui			

- A) Avez-vous déjà suivi des formations/ conférences sur les dangers d'internet?
- B) Pensez-vous avoir les connaissances nécessaires pour pouvoir conscientiser les élèves à la protection de leur vie privée et de leurs données personnelles sur Internet?
- C) Pensez-vous pouvoir vous-même expliquer et montrer aux élèves les démarches à suivre pour protéger leur vie privée et leurs données personnelles sur Internet?
- D) Genre
- E) Êtes-vous enseignant dans une école ...
- F) Age
- G) Avez-vous déjà discuté de la protection des données personnelles et de la vie privée sur Internet avec vos élèves?

Parents :

Questions	Valeur dans SPSS	0	1	2	3	4	5
A	CONN	Non	Oui				
B	EXPL	Non	Oui				

C	NIVETUDE		Diplôme secondaire	Etudes supérieures de type court	Etudes supérieures de type long		
D	METIER		Demandeur d'emploi	Ouvrier	Employé	Indépendant	Dirigeant d'entreprise
E	SENSIB	Non	Oui				
F	PEUR	Non	Oui				
G	GENRE		Femme	Homme			
H	AGE		25 – 35 ans	36 – 45 ans	46 – 55 ans	+ de 55 ans	
I	CONTPAR	Non	Oui				
J	IMP		Pas du tout important	Pas très important	Important	Très important	
K	CONTECRA N	Non	Oui				
L	CONTSITE	Non	Oui				
M	CONTRS	Non	Oui				
N	CONTACHA T	Non	Oui				

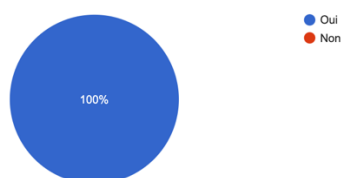
- A) Pensez-vous avoir les connaissances nécessaires pour éveiller vos enfants à cela? D
- B) Pensez-vous pouvoir vous-même expliquer et montrer à vos enfants les démarches à suivre pour protéger leur vie privée et leurs données personnelles sur Internet?
- C) Niveau d'étude
- D) Métier
- E) Avez-vous déjà sensibilisé vos enfants à la protection de leur vie privée et de leurs données personnelles ?
- F) Avez-vous mis en place un logiciel de contrôle parental sur un ordinateur ou sur le téléphone de votre enfant ?
- G) Genre
- H) Âge

- I) Avez-vous mis en place un logiciel de contrôle parental sur un ordinateur ou sur le téléphone de votre enfant ?
- J) Quelle importance accordez-vous aux contrôles suivants?
- K) Appliquez-vous réellement le contrôle du temps d'écran ?
- L) Appliquez-vous réellement le contrôle des sites fréquentés ?
- M) Appliquez-vous réellement le contrôle des réseaux sociaux ?
- N) Appliquez-vous réellement le contrôle des achats en ligne ?

Annexe 4

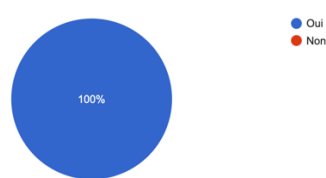
Savez-vous ce qu'est une donnée personnelle ?

43 réponses

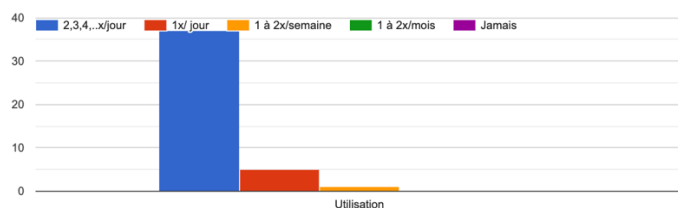


Utilisez-vous les grandes plateformes comme Google, Facebook, Amazon, Airbnb, Uber,...?

43 réponses



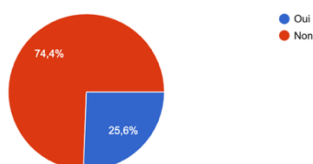
A quelle fréquence?



Annexe 5 :

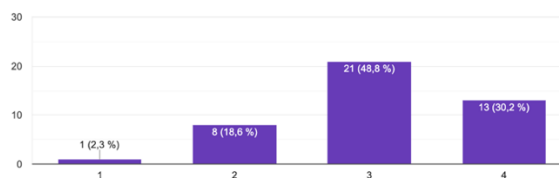
Pensez-vous avoir les connaissances nécessaires pour pouvoir conscientiser les élèves à la protection de leur vie privée et de leurs données personnelles sur Internet?

43 réponses



Pensez-vous pouvoir vous-même expliquer et montrer aux élèves les démarches à suivre pour protéger leur vie privée et leurs données personnelles sur Internet?

43 réponses



Annexe 6 :

Formations - Connaissance

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9,842 ^a	2	,007
Likelihood Ratio	11,051	2	,004
Linear-by-Linear Association	8,986	1	,003
N of Valid Cases	44		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is ,50.

Formation – capacité d'expliquer

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4,447 ^a	6	,616
Likelihood Ratio	5,234	6	,514
Linear-by-Linear Association	,144	1	,705
N of Valid Cases	44		

a. 8 cells (66,7%) have expected count less than 5. The minimum expected count is ,05.

Annexe 7:

Prof info - connaissances

Chi-Square Tests					
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	9,659 ^a	1	,002		
Continuity Correction ^b	5,843	1	,016		
Likelihood Ratio	9,013	1	,003		
Fisher's Exact Test				,012	,012
Linear-by-Linear Association	9,439	1	,002		
N of Valid Cases	44				

a. 2 cells (50,0%) have expected count less than 5. The minimum expected count is ,75.
b. Computed only for a 2x2 table

Prof info - capacité d'expliquer

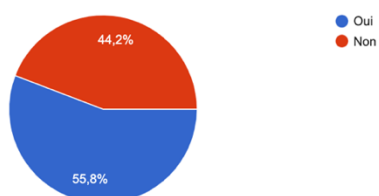
Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	20,390 ^a	3	<,001
Likelihood Ratio	12,907	3	,005
Linear-by-Linear Association	10,967	1	<,001
N of Valid Cases	44		

a. 5 cells (62,5%) have expected count less than 5. The minimum expected count is ,07.

Annexe 8 :

Avez-vous déjà discuté de la protection des données personnelles et de la vie privée sur Internet avec vos élèves?

43 réponses



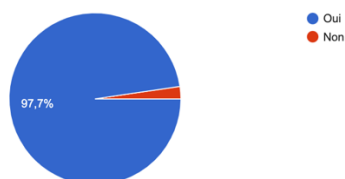
Chi-Square Tests					
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3,736 ^a	1	,053		
Continuity Correction ^b	2,501	1	,114		
Likelihood Ratio	4,028	1	,045		
Fisher's Exact Test				,081	,054
Linear-by-Linear Association	3,651	1	,056		
N of Valid Cases	44				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 4,75.
b. Computed only for a 2x2 table

Annexe 9 :

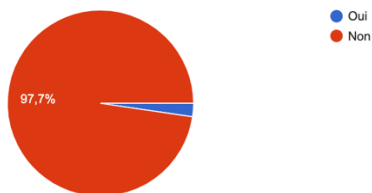
Pensez-vous que l'école a un rôle à jouer dans l'éducation au numérique pour les enfants et les adolescents?

43 réponses



Pensez-vous que les parents éveillent suffisamment leurs enfants à cette problématique?

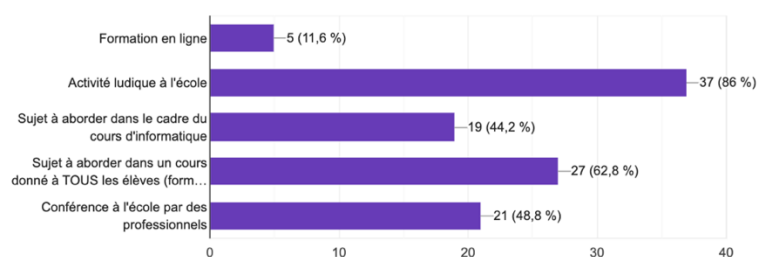
43 réponses



Annexe 10 :

Qu'est-ce qui devrait être mis en place pour éduquer les élèves à être un bon citoyen numérique?

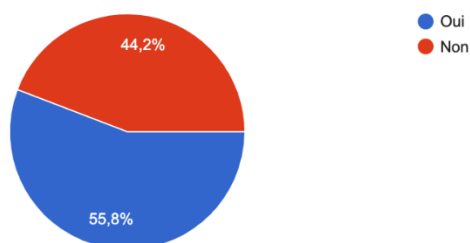
43 réponses



Annexe 11 :

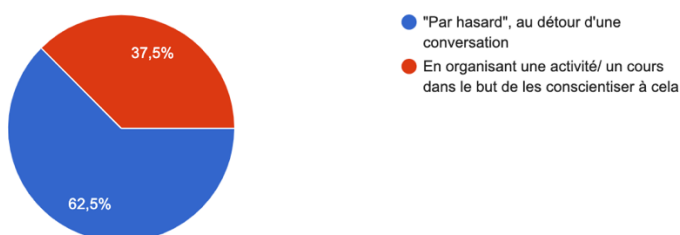
Avez-vous déjà discuté de la protection des données personnelles et de la vie privée sur Internet avec vos élèves?

43 réponses



Si oui, dans quelles circonstances?

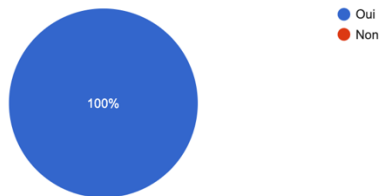
24 réponses



Annexe 12 :

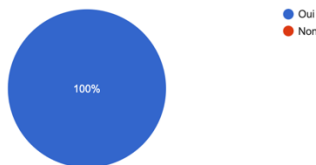
Savez-vous ce qu'est une donnée personnelle ?

68 réponses

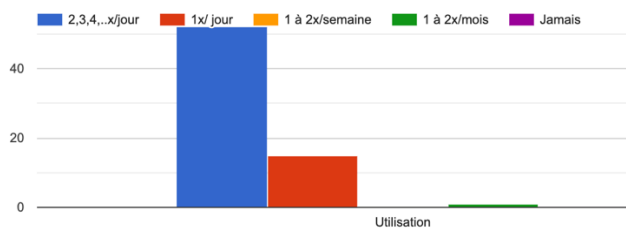


Utilisez-vous les grandes plateformes comme Google, Facebook, Amazon, Airbnb, Uber,...?

68 réponses

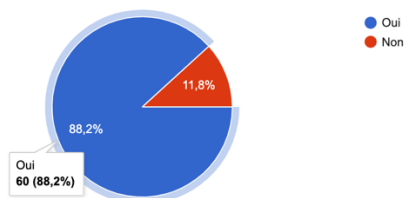


A quelle fréquence?



Savez-vous que ces plateformes collectent vos données personnelles sans votre réel consentement et que vos données sont ensuite revendues à des entreprises qui les utilisent principalement à des fins publicitaires?

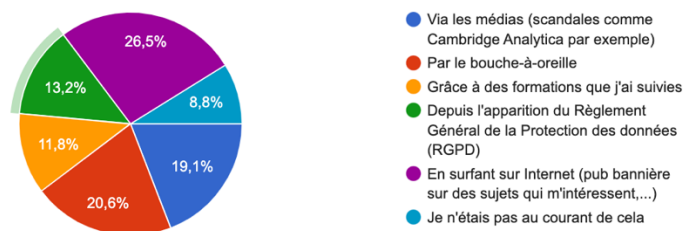
68 réponses



Annexe 13 :

Comment savez-vous cela?

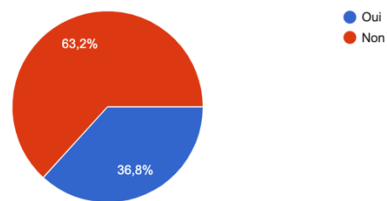
68 réponses



Annexe 14 :

Pensez-vous avoir les connaissances nécessaires pour éveiller vos enfants à cela?

68 réponses



Annexe 15 :

CONN * NIVETUDE Crosstabulation

Count

		NIVETUDE			
		1	2	3	Total
CONN	0	13	18	12	43
	1	3	7	15	25
Total		16	25	27	68

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7,160 ^a	2	,028
Likelihood Ratio	7,260	2	,027
Linear-by-Linear Association	6,508	1	,011
N of Valid Cases	68		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 5,88.

EXPL * NIVETUDE Crosstabulation

Count

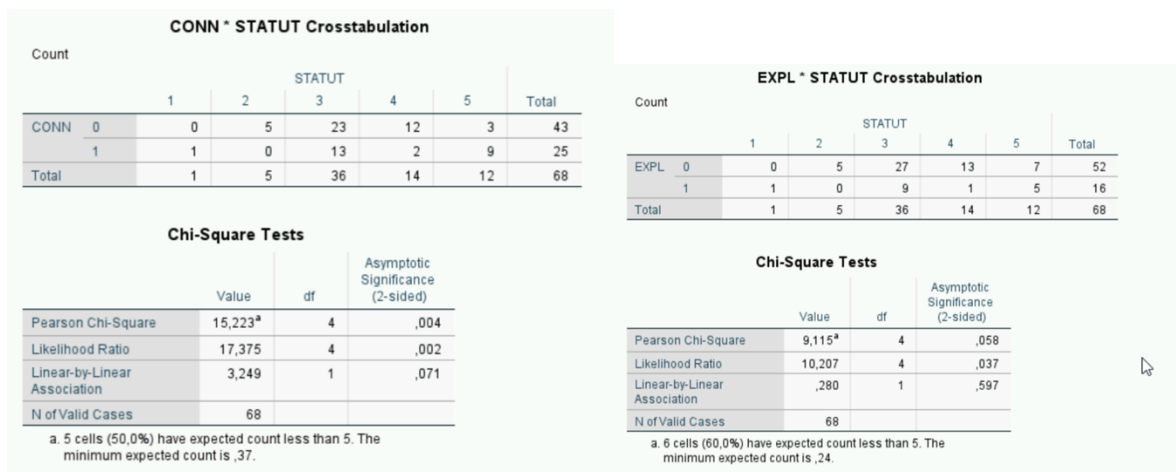
		NIVETUDE			
		1	2	3	Total
EXPL	0	15	20	17	52
	1	1	5	10	16
Total		16	25	27	68

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5,566 ^a	2	,062
Likelihood Ratio	6,105	2	,047
Linear-by-Linear Association	5,461	1	,019
N of Valid Cases	68		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 3,76.

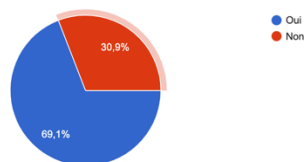
Annexe 16 :



Annexe 17 :

Avez-vous déjà sensibilisé vos enfants à la protection de leur vie privée et de leurs données personnelles ?

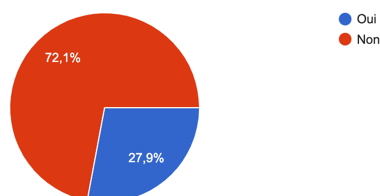
68 réponses



Annexe 18 :

Avez-vous mis en place un logiciel de contrôle parental sur un ordinateur ou sur le téléphone de votre enfant ?

68 réponses



T-Test

Group Statistics					
	CONTPAR	N	Mean	Std. Deviation	Std. Error Mean
AGE	1	19	1,95	,780	,179
	0	49	2,49	,869	,124

Independent Samples Test									
Levene's Test for Equality of Variances					t-test for Equality of Means				
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference Lower Upper
AGE	Equal variances assumed	3,616	,062	-2,374	66	,021	-,542	,229	-,999 -,086
	Equal variances not assumed			-2,491	36,344	,017	-,542	,218	-,984 -,101

Annexe 19 :

PEUR * CONTPAR Crosstabulation				
Count				
		CONTPAR		
		0	1	Total
PEUR	0	16	2	18
	1	33	17	50
Total		49	19	68

Chi-Square Tests				
	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3,444 ^a	1	,063	
Continuity Correction ^b	2,401	1	,121	
Likelihood Ratio	3,904	1	,048	
Fisher's Exact Test				,074
Linear-by-Linear Association	3,393	1	,065	
N of Valid Cases	68			

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 5,03.
b. Computed only for a 2x2 table

Annexe 20 :

1) Temps d'écran

IMPECRAN * CONTECRAN Crosstabulation				
Count				
		CONTECRAN		
		0	1	Total
IMPECRAN	2	13	1	14
	3	10	16	26
	4	1	27	28
Total		24	44	68

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	32,765 ^a	2	<,001
Likelihood Ratio	37,818	2	<,001
Linear-by-Linear Association	31,654	1	<,001
N of Valid Cases	68		

a. 1 cells (16,7%) have expected count less than 5. The minimum expected count is 4,94.

2) Sites fréquentés

IMPSITE * CONTSITE Crosstabulation				
Count				
		CONTSITE		
		0	1	Total
IMPSITE	2	2	0	2
	3	15	9	24
	4	16	26	42
Total		33	35	68

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5,827 ^a	2	,054
Likelihood Ratio	6,634	2	,036
Linear-by-Linear Association	5,644	1	,018
N of Valid Cases	68		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is ,97.

3) Réseaux sociaux

IMPRS * CONTRS Crosstabulation

Count

		CONTRS		
		0	1	Total
IMPRS	1	1	0	1
	2	18	1	19
	3	24	6	30
	4	7	11	18
Total		50	18	68

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	16,493 ^a	3	<,001
Likelihood Ratio	16,681	3	<,001
Linear-by-Linear Association	14,432	1	<,001
N of Valid Cases	68		

a. 3 cells (37,5%) have expected count less than 5. The minimum expected count is ,26.

4) Achats en ligne

IMPACHAT * CONTACHAT Crosstabulation

Count

		CONTACHAT		
		0	1	Total
IMPACHAT	2	1	1	2
	3	14	20	34
	4	7	25	32
Total		22	46	68

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3,099 ^a	2	,212
Likelihood Ratio	3,149	2	,207
Linear-by-Linear Association	2,978	1	,084
N of Valid Cases	68		

a. 2 cells (33,3%) have expected count less than 5. The minimum expected count is ,65.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Louvain School of Management

Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique

www.uclouvain.be/lsm