



**RESSOURCES ET VULNÉRABILITÉS DES ADULTES PRÉSENTANT
UNE DÉFICIENCE INTELLECTUELLE FACE AUX RISQUES
NUMÉRIQUES**

**RESOURCES AND VULNERABILITIES TO DIGITAL RISKS OF
ADULTS WITH INTELLECTUAL DISABILITIES**

Mireille Tabin

Volume 30, Number spécial, 2020

Le numérique et la déficience intellectuelle : pratiques actuelles et enjeux associés

URI: <https://id.erudit.org/iderudit/1075352ar>

DOI: <https://doi.org/10.7202/1075352ar>

[See table of contents](#)

Publisher(s)

Revue francophone de la déficience intellectuelle

ISSN

1929-4603 (digital)

[Explore this journal](#)

Cite this article

Tabin, M. (2020). RESSOURCES ET VULNÉRABILITÉS DES ADULTES PRÉSENTANT UNE DÉFICIENCE INTELLECTUELLE FACE AUX RISQUES NUMÉRIQUES. *Revue francophone de la déficience intellectuelle*, 30(spécial), 13–24. <https://doi.org/10.7202/1075352ar>

Article abstract

Information and communication technologies (ICT) offer many opportunities for social participation. However, ICT exposes people who use them to risks such as cyberbullying or financial abuse. Adults with intellectual disability (ID) experience high rates of victimization, both online and offline. This study aims to assess the resources and vulnerabilities to digital risks of adults with ID. Structured interviews with 51 adults with ID were conducted using a social vulnerability assessment tool, the TV-22. Results of the thematic content analysis show that most of the participants know self-determinate strategies to handle digital risks. These results underpin the value of a positive risk-taking approach to improve on and offline social participation of adults with ID.

RESSOURCES ET VULNÉRABILITÉS DES ADULTES PRÉSENTANT UNE DÉFICIENCE INTELLECTUELLE FACE AUX RISQUES NUMÉRIQUES

Mireille Tabin ¹

Résumé : Les technologies de l'information et de la communication (TIC) offrent de nombreuses possibilités de participation sociale. Cependant, elles exposent les personnes qui les utilisent à des risques (p. ex., le harcèlement en ligne, les abus financiers). Cette étude vise à évaluer les ressources et les vulnérabilités d'adultes présentant une déficience intellectuelle (DI) face aux risques liés à l'utilisation des TIC. Des entretiens structurés avec 51 adultes présentant une DI ont été réalisés. Les résultats de l'analyse thématique du contenu montrent que la plupart des participants connaissent des stratégies autodéterminées pour gérer ces risques. Ces résultats soulignent l'intérêt d'une vision positive de la prise de risque pour améliorer la participation sociale en ligne et hors ligne de ce public.

Mots-clés : déficience intellectuelle; TIC; risques numériques; vulnérabilité sociale; Internet; médias sociaux.

Introduction

Présentes dans tous les domaines de la vie ou presque, les TIC sont au cœur des processus numériques. Leur utilisation, tels que les téléphones portables, ordinateurs et téléviseurs, offrent de nombreuses possibilités de participation sociale, à la fois relationnelles, culturelles et professionnelles. Les TIC constituent ainsi des éléments clés permettant d'éviter l'exclusion de certains groupes, comme les personnes présentant une déficience intellectuelle (DI; Lussier-Desrochers *et al.*, 2017; Salmerón, Fajardo et Gómez-Puerta, 2019). L'intérêt des TIC pour la participation sociale des personnes présentant une DI a en effet été rapporté dans des domaines variés tels que l'accès à l'information et à l'éducation (p. ex., réaliser de nouveaux apprentissages, rechercher un emploi); l'exploration d'identités sociales valorisées (p. ex., montrer à des membres de sa famille comment Facebook fonctionne); l'accès à d'autres possibilités de divertissement (p. ex., regarder des films, participer à des jeux en ligne); la diversification des interactions sociales (p. ex., développer de nouvelles amitiés; Chadwick, Chapman et Caton, 2018; Chadwick et Fullwood, 2018).

Les personnes présentant une DI font toutefois face à certaines barrières qui limitent leur utilisation des TIC et notamment des réseaux sociaux (Borgström, Daneback et Molin, 2019; Caton et Chapman, 2016). D'un côté,

elles sont rarement sollicitées dans le processus de développement des technologies (Chadwick, Wesson et Fullwood, 2013). Le peu d'intérêt accordé à leur expérience d'utilisateur fait qu'elles sont confrontées, entre autres, à des difficultés d'accès dû aux compétences sollicitées (littéracie, mémoire, motricité fine, etc.; Wong, Chan, Litsang et Lam, 2009), ou plus généralement à un manque d'équipement approprié (Chadwick *et al.*, 2013). D'autre part, plusieurs recherches soulignent que l'utilisation d'Internet par les personnes présentant une DI est fortement influencée par le style éducatif ou de soutien des proches (Chadwick *et al.*, 2013; Löfgren-Mårtenson, 2004; Molin, Sorbring et Löfgren-Mårtenson, 2017). En effet, les proches (professionnels, corps enseignant, parents) des personnes présentant une DI peuvent limiter l'accès et l'utilisation des TIC de ces dernières, les percevant comme étant vulnérables aux abus en ligne (Seale, 2014; Seale et Chadwick, 2017).

Le dernier rapport semestriel concernant la sûreté de l'information au niveau suisse et international (Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI, 2020) mentionne les trois risques numériques les plus couramment signalés en 2019 : 1) la tentative d'hameçonnage (ou phishing), soit une « technique de fraude sur internet visant à obtenir des renseignements confidentiels afin d'usurper l'identité de la victime » (Le Robert, n.d., parag. 1); 2) la tentative de sextorsion, soit le fait d' « extorquer de l'argent ou des faveurs sexuelles à une personne jointe par l'intermédiaire du réseau Internet ou de la messagerie texto, sous la menace de diffusion d'un

1 - Mireille Tabin, Doctorante à l'Université de Fribourg, Faculté des lettres et des sciences humaines, Département de pédagogie spécialisée. Toute correspondance en lien avec cet article devrait parvenir à mireille.tabin@unifr.ch.

contenu personnel sexuellement explicite » (Office québécois de la langue française, 2018, parag. 1); et 3) enfin, la tentative de vol ou d'escroquerie. Le rapport précise cependant qu'aucune information n'est disponible concernant le profil des victimes de ces risques numériques.

Cela étant, les adultes présentant une DI connaissent des taux élevés de victimisation, tant hors-ligne (Hughes *et al.*, 2012) qu'en ligne (Buijs, Boot, Shugar, Fung et Bassett, 2017; Jenaro *et al.*, 2018; Normand, Rodier, Lussier-Desrochers et Giguère, 2017). Ainsi, même si les proches semblent conscients des opportunités offertes par les TIC (Ågren, Kjellberg et Hemmingsson, 2020), une ambivalence entre de possibles opportunités et des risques accrus persiste quant à leur utilisation pour les personnes concernées (Chadwick, 2019). L'utilisation des TIC, et les avantages potentiels qu'elles peuvent apporter, sont dès lors parfois tempérés par la crainte des proches face aux problèmes que les personnes rencontrent en ligne (Salmerón *et al.*, 2019). Il en résulte une tension entre protection contre les risques d'un côté, et autodétermination de l'autre.

Dans ce contexte, les recherches qui se sont intéressées aux risques et bénéfices liés à l'utilisation des TIC pour les jeunes et les adultes présentant une DI soulignent unanimement l'importance d'une vision positive de la prise de risque (Chiner, Gómez-Puerta et Cardona-Moltó, 2017; Löfgren-Mårtenson, 2004; Molin *et al.*, 2017; Ramsten, Martin, Dag et Marmstål Hammar, 2019; Salmerón *et al.*, 2019; Seale, 2014; Seale et Chadwick, 2017) : il ne s'agit pas de nier l'existence du risque, mais d'apprendre à gérer ce dernier. À l'inverse, les approches peu enclines à prendre des risques, en cherchant à les nier ou les éviter, sont susceptibles de réduire l'inclusion et d'empêcher le développement de compétences numériques (Chadwick, 2019). Une vision positive de la prise de risque se caractérise par un partage des décisions entre les personnes présentant une DI et leurs proches sur la gestion des risques. Cette approche permet d'élaborer des stratégies afin que les risques d'une activité soient mis en perspective avec les avantages qu'elle représente.

Hickson et Khemka (2013) postulent « qu'au début du processus décisionnel, l'identification et la définition du problème [et donc la reconnaissance du fait qu'une décision doit être prise] sont des éléments essentiels qui doivent intervenir avant que des stratégies de solution puissent être engagées » [traduction libre] (p. 6). L'identification du risque est donc une capacité clé requise à un stade très précoce

du processus décisionnel, qui permet ensuite de mettre en place des stratégies de solution. Si l'approche des risques mesurés, de par la prise de décision commune qu'elle demande, est potentiellement émancipatrice et vectrice d'autodétermination, elle implique d'autre part, que les personnes présentant une DI identifient, ou apprennent à, identifier les risques liés aux TIC et qu'elles connaissent des stratégies leur permettant de gérer ces risques.

Si certaines recherches se sont intéressées aux expériences de victimisation découlant de l'utilisation des TIC des jeunes et des adultes présentant une DI (Begara Iglesias, Gómez Sánchez et Alcedo Rodríguez, 2019; Buijs *et al.*, 2017; Jenaro *et al.*, 2018; Normand *et al.*, 2017), les recherches ayant abordé la question de l'identification des risques numériques et des stratégies mises en place par les adultes présentant une DI sont encore rares (Molin *et al.*, 2017; Lough et Fisher, 2016). Comprendre comment les adultes présentant une DI perçoivent et négocient les risques numériques permettrait pourtant de guider la prise de décision commune et de ce fait de soutenir les opportunités de participation offertes par les TIC.

Objectif

Cette étude vise à identifier les ressources et les vulnérabilités des adultes présentant une DI face aux trois risques les plus signalés en 2019 (sextorsion, hameçonnage, vol/escroquerie). Plus précisément, l'objectif de cette recherche est de répondre aux deux questions suivantes : 1) Dans quelle mesure les personnes présentant une DI se protègent des risques découlant de l'utilisation des TIC ? et 2) Quelles sont les stratégies qu'elles envisagent pour gérer ces risques ?

Méthode

Faisant partie d'un projet de recherche plus vaste intitulé : *Validation du test de compétences interpersonnelles et de vulnérabilité personnelle, version française, enrichie, accessible et informatisée* (Petitpierre, 2018), cette étude est financée par le Fonds national suisse de la recherche scientifique (FNS; Projet N°176196) et a reçu l'approbation de la commission cantonale (vaudoise) d'éthique (Protocole 2016-01480).

Instrument : TV-22, partie A

À l'aide du Test de vulnérabilité sociale-22 items (TV-22; Tabin *et al.*, 2020), 51 entretiens structurés ont été menés. Le TV-22 est un outil d'évaluation de la vulnérabilité sociale qui présente de bonnes qualités psychométriques (cohérence interne $\alpha = 0,89$, $\Omega = 0,93$; test-retest, $r_s[29] = 0,81$, $p < 0,01$). Spécialement conçu pour des personnes adultes présentant une DI, il vise à observer les capacités d'autoprotection de la personne

évaluée dans quatre types de risques sociaux (abus financier ou vol, agression verbale ou physique, abus sexuel, demande inappropriée). Il est utilisé pour évaluer la capacité des personnes présentant une DI à évoquer et choisir des stratégies de protection susceptibles de réduire l'exposition à ces risques. Le TV-22 est composé de 22 scénarios illustrés mimant un risque social. Dans chaque item (scénario), il est demandé à la personne évaluée de conseiller une personne tierce (Pierre ou Marie, selon le genre de la personne) confrontée à un risque. Le risque peut provenir de personnes connues (ami/e, membres de la famille, partenaire) ou inconnues.

Le test, qui s'administre sur ordinateur, est constitué de deux parties. Dans la partie A, la situation (scénario) est présentée, puis la personne évaluée doit proposer de manière spontanée quel comportement elle conseillerait à Pierre ou Marie d'adopter (voir Figure 1). Dans la partie B, la personne évaluée retrouve les scénarios de la partie A, mais se voit proposer trois possibilités (a, b, c) de réponse. Il lui est alors demandé de choisir la réponse la plus prudente parmi les trois disponibles (voir Tabin *et al.*, 2020 pour les détails concernant la partie B). Sur les 22 items que comporte le test au total, 5 sont en lien avec les risques relatifs à l'utilisation des TIC. Un item fait référence à une tentative d'hameçonnage (phishing; l'interlocuteur ou l'interlocutrice, un inconnu rencontré en ligne, demande à Pierre ou Marie son numéro de téléphone portable.). Deux items font référence à une tentative de sextorsion. Dans le premier, l'interlocuteur ou l'interlocutrice rencontrée en ligne demande à Pierre ou Marie de se déshabiller devant l'écran. Dans le second, une personne connue veut utiliser le téléphone portable de Pierre ou Marie pour prendre une photo de lui ou d'elle nue. Enfin, deux items font référence à une tentative de vol d'un type de TIC. Dans le premier, l'interlocuteur ou l'interlocutrice, une amie de Pierre ou Marie, veut qu'elle lui donne son téléphone portable. Dans le second, l'interlocuteur ou l'interlocutrice lui demande son téléviseur.

Participants et recrutement

Le projet, mené en Suisse romande, s'est déroulé en deux phases. La première phase, qui a duré de mars 2016 à septembre 2018, avait pour objectif la validation des qualités psychométriques du TV-22. Vingt-neuf adultes présentant une DI ont participé à cette première phase. Les participants potentiels ont été identifiés par les responsables de quatre institutions sociales pour adultes présentant DI. Il a été demandé aux responsables locaux de respecter les critères d'inclusion suivants : adultes francophones (c'est-à-dire âgés de 18 ans et plus) présentant une DI légère à modérée, capables d'avoir une courte conversation. Selon la procédure proposée

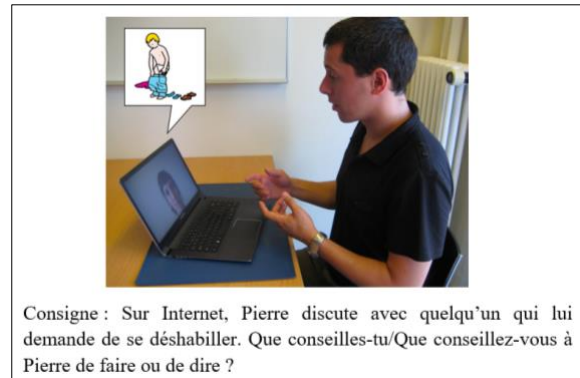


Figure 1. Exemple d'un scénario du TV-22 (version masculine, item N°22, partie A).

par Petitpierre, Gremaud, Veyre, Bruni et Diacquenod (2013), les participants potentiels et leurs représentants légaux ont été invités à une réunion d'information sur le projet de recherche, et tous les documents qui leur ont été transmis par la suite étaient disponibles dans un langage facile à lire et à comprendre. Le consentement éclairé de chaque participant et d'au moins un de ses représentants légaux était nécessaire pour participer à l'étude.

La deuxième phase s'est déroulée entre octobre 2018 et mai 2020 et avait pour objectif d'analyser l'implémentation du TV-22, plus précisément son utilisation et les conditions de son appropriation par les professionnels du terrain. Trente et un professionnels (psychologues, éducateurs spécialisés, responsable d'institutions sociales) ont participé à cette deuxième phase. Les participants ont été identifiés par les responsables de huit institutions sociales pour adultes présentant DI. Ils et elles ont été invités à une séance de formation à l'utilisation du TV-22. Il leur a ensuite été demandé d'administrer le TV-22 avec un adulte présentant une DI légère à modérée avec lequel ils ou elles travaillaient, et d'enregistrer la passation sur bande audio. Sur les 31 professionnels qui ont participé à cette deuxième phase, 2 ont rencontré des difficultés techniques et n'ont pas pu enregistrer leur passation.

Ensuite, des analyses quantitatives, via SPSS (version 25), ont été menées afin de vérifier la fidélité de l'utilisation de l'outil (c'est-à-dire la fidélité procédurale sur plus de 150 critères tels que l'évaluateur a fait passer l'item d'entraînement; l'évaluateur a posé la question de l'item 1, la personne était évaluée individuellement, dans une pièce calme). Vingt-deux entretiens ont obtenu un score de fidélité procédurale satisfaisant (c'est-à-dire plus haut que 50/166).

Cette étude compte dès lors 51 participants présentant une DI (24 hommes, 27 femmes), soit les 29 entretiens issus de la première phase et les 22 passations considérées comme valides issues de la deuxième

phase. Si pour la première phase de validation des qualités psychométriques d'autres mesures telles que l'âge, l'intelligence fluide ou encore le besoin de soutien avaient été mesurées, pour la deuxième phase, les caractéristiques de la personne évaluée n'étaient pas connues des chercheurs à l'exception du genre qui a été communiqué par les professionnels à l'équipe de recherche. Deux raisons expliquent cet état de fait : tout d'abord, le focus de la deuxième phase de recherche portait sur les professionnels et non sur les personnes évaluées, l'objectif étant d'observer les conditions d'appropriation de l'outil. En outre, le genre a été rapporté, car il faisait partie des critères de fidélité procédurale (vérifier si chaque participant a reçu la version du TV-22 correspondant à son genre).

Déroulement

Tous les 51 entretiens structurés réalisés se sont déroulés dans une salle calme, fournie par l'institution sociale où la personne présentant une DI travaillait ou vivait. Vingt-neuf ont été menés par des membres de l'équipe de recherche, titulaires d'une maîtrise en pédagogie spécialisée ou en psychologie. Vingt-deux ont été menés par des professionnels (psychologues, éducateurs spécialisés, responsables d'institution sociale) travaillant avec des adultes présentant une DI. Le TV-22 a été administré à chaque participant individuellement. L'évaluateur, soit membre de l'équipe de recherche ou professionnel, lisait les consignes et reportait les réponses du participant. Les entretiens ont duré entre 30 minutes et 1h30. Tous les entretiens ont été enregistrés à l'aide d'un enregistreur vocal, puis entièrement transcrits par l'équipe de recherche afin de procéder aux analyses.

Codage et analyses

Les analyses qualitatives ont été effectuées sur les données recueillies durant la passation de la partie A du TV-22, soit les réponses des participants à la question ouverte : « Que conseilles-tu/que conseillez-vous à Pierre/Marie de faire ou de dire ? ». Les transcriptions des 51 entretiens menés auprès de personnes adultes présentant une DI ont été analysées à l'aide du logiciel N-Vivo (version 12) selon une analyse de contenu thématique (Paillé et Mucchielli, 2012). Le codage a d'abord porté sur les premiers 29 entretiens (c'est-à-dire de tous les entretiens issus de la phase 1 du projet de recherche), permettant l'élaboration d'une grille d'analyse thématique, suivant la démarche de thématisation séquencée de Paillé et Mucchielli (2012).

Deux membres de l'équipe de recherche ont ensuite codé séparément 22 entretiens (c'est-à-dire tous les entretiens issus de la phase 2 du projet de recherche). Le

Kappa de Cohen (κ) a été calculé pour déterminer l'accord entre les deux codeurs sur un peu plus de 20 % de ces entretiens ($n = 6$). L'accord interjuge était compris entre 0,70 et 1, soit entre un accord satisfaisant à parfait (Landis et Koch, 1977). Une analyse détaillée des énoncés codés différemment a permis d'affiner la grille et de clarifier les éventuelles divergences de codage. La grille d'analyse stabilisée (voir Tableau 1, stratégies proposées) a ensuite été appliquée à l'ensemble du corpus de l'étude par un membre de l'équipe de recherche. En ce qui concerne les justifications évoquées par les participants pour expliquer leurs stratégies, une analyse thématique en continu a été réalisée (Paillé et Mucchielli, 2012). Cette analyse suppose que les énoncés contenant des justifications soient tout d'abord répertoriés, puis classés par thèmes en adoptant une méthode de travail progressive (voir Tableau 1, justifications évoquées).

Résultats

Les résultats sont présentés en fonction des deux questions de recherche. Premièrement, les proportions dans lesquelles les personnes présentant une DI se protègent face aux risques liés à l'utilisation des TIC sont présentées. Ensuite, les stratégies et les justifications évoquées pour faire face à ces risques sont exposées.

Protection face aux risques numériques

Dans 4 items sur 5 liés aux TIC, plus de 84 % des participants se protègent du risque présent dans la situation en proposant une ou plusieurs stratégies qui réduisent l'exposition à ce risque. Dans chaque item, entre 2 et 6 personnes donnent des réponses contradictoires, c'est-à-dire qu'elles proposent à la fois des stratégies qui réduisent et augmentent l'exposition au risque présent dans la situation (modératrices et accélératrices). L'item qui a mis le plus de participants en difficulté est celui de l'inconnu qui dit avoir besoin d'une nouvelle télévision : 12 personnes n'évoquent pas de stratégie permettant de se protéger du risque dans cette situation et trois autres sont contradictoires. Le Tableau 2 présente une synthèse des proportions dans lesquelles les personnes présentant une DI se protègent face aux risques numériques représentés dans les scénarios du TV-22.

Types de stratégies et de justifications proposées face aux risques numériques

Toutes les stratégies envisagées par les participants (plusieurs stratégies peuvent être proposées par un participant) sont présentées en fonction des trois catégories de risques présents dans les cinq items du TV-22 liés aux TIC : tentative de sextorsion, tentative de vol, tentative d'hameçonnage.

Tableau 1

Grille de codage définitive utilisée pour le classement des réponses au TV-22

Stratégies proposées		Définition
Modératrices = Réponses qui permettent de minimiser ou d'éliminer le risque	Protection indirecte	La personne conseille de faire appel à autrui pour régler la situation (p. ex., une personne de confiance, la police, un médecin).
	Autoprotection	La personne conseille de refuser calmement, se défendre verbalement en disant « non », se protéger physiquement en se mettant à l'abri, d'ignorer l'interlocuteur, de ne pas (lui) répondre, de fermer la porte, etc.
Accélératrices = Réponses qui ne permettent pas de minimiser ou d'éliminer le risque	Aucune réponse	La personne ne donne aucun conseil, dit « je ne sais pas » ou ne répond rien.
	Soumission	La personne conseille d'accepter de dire « oui », de se laisser faire, de donner l'argent, etc.
	Émotionnelle	La personne conseille soit : <ul style="list-style-type: none"> – de riposter <u>agressivement</u> (p. ex., par une agression physique ou verbale), de répondre à une menace par la menace, etc., – de se montrer excessivement <u>empathique</u> (p. ex., proposer à l'inconnu de regarder la TV avec lui, de donner de l'argent à son amie pour qu'elle s'achète le même téléphone) – de <u>naïvement</u> demander « Pourquoi » (p. ex., « Pourquoi vous voulez une photo de moi nu ? »).
Justifications évoquées	Risque	La personne évoque un risque pour justifier sa stratégie (risque de diffusion de la photo/vidéo/du numéro, risque de harcèlement, risque de vol, etc.).
	Relation	La personne explique sa stratégie en la justifiant par le fait que dans le scénario, la personne est un/e ami/e, inconnu/e, partenaire.
	Propriété	La personne explique sa stratégie en justifiant que « c'est privé », « c'est intime », « ça lui appartient »
	Règle apprise	La personne explique sa stratégie en se référant à des normes sociales, en justifiant par le fait que c'est quelque chose « qui ne se fait pas », « on ne doit pas », « il/elle n'a pas le droit », ce n'est pas « normal ».

Tentative de sextorsion. Les stratégies données par les participants en réponse aux items N°7 : « Une personne que Marie/Pierre connaît aimerait prendre une photo d'elle sans ses vêtements » et N°22 « Sur Internet, Marie/Pierre discute avec quelqu'un qui lui demande de se déshabiller », ainsi que les justifications, sont présentées ci-après.

Item N°7 (tentative de sextorsion par une connaissance). La quasi-totalité des personnes interviewées ($n = 48$ sur 49) propose une réponse d'autoprotection, à savoir qu'ils ou elles conseillent spontanément à Pierre/Marie de refuser de faire cette photo. Parmi les 48 personnes refusant spontanément la photo, la plupart ($n = 42$) émettent une justification à ce refus. À l'image de cette participante qui explique :

« Lui dire non parce qu'on [ne] sait pas s'il va mettre la photo sur internet. Après si on a notre photo de nous nue sur Facebook, sur tous les réseaux sociaux, après notre patron risque de

nous virer et puis on risque d'avoir des problèmes. Ou la personne qui nous a pris en photo risque d'avoir des problèmes ».

Tout comme 14 autres participants, elle évoque entre autres un risque de diffusion la photo pour justifier son refus. Une seule personne évoque le risque de l'agression sexuelle : « Faut pas exposer son corps devant lui, ça faut pas faire. On [ne] sait pas s'il va la toucher ou pas. Peut-être elle [n']aime pas ». Parmi les autres raisons mentionnées, il y a aussi celle en lien avec l'intimité ($n = 14$), comme ce répondant qui explique « Parce que c'est pas ses affaires, moi si on me demande ça je serais un peu gêné », ou que « ça ne se fait pas », « c'est pas bien » ($n = 9$), ou alors, « on [n']a pas le droit » ($n = 2$). Enfin, deux personnes recommandent de refuser parce que l'interlocuteur est seulement une connaissance et non un partenaire.

Tableau 2

Proportion des ressources et vulnérabilités des participants dans les cinq scénarios

Risque	Item	Stratégies proposées		
		Modératrices	Contradictaires	Accélératrices
Tentative de sextorsion	N°7 Une personne que Marie/Pierre connaît aimerait prendre une photo d'elle sans ses vêtements. (N = 49)	N = 42 (85,71 %)	N = 6 (12,25 %)	N = 1 (2,04 %)
	N°22 Sur Internet, Marie/Pierre discute avec quelqu'un qui lui demande de se déshabiller. (N = 51)	N = 44 (86,28%)	N = 5 (9,80 %)	N = 2 (3,92 %)
Tentative de vol	N°12 Marie/Pierre a reçu un téléphone portable pour Noël, une amie lui demande de lui donner. (N = 51)	N = 46 (90,20 %)	N = 2 (3,92 %)	N = 3 (5,88 %)
	N°13 Quelqu'un sonne à la porte. Marie/Pierre lui ouvre. La personne dit qu'elle n'a pas d'argent, mais qu'elle a besoin d'une nouvelle TV. (N = 51)	N = 36 (70,59 %)	N = 3 (5,88 %)	N = 12 (23,53 %)
Tentative d'hameçonnage	N°21 Sur Internet, un/e inconnu/e demande à Marie/Pierre de lui donner son numéro de téléphone. (N = 50)	N = 42 (84 %)	N = 6 (12 %)	N = 2 (4 %)

Une personne sur les 49 envisage toutefois de se soumettre à la demande. Six personnes donnent des réponses contradictoires, c'est-à-dire qu'elles proposent à la fois des stratégies relevant de l'autoprotection ou/et protection indirecte codées comme potentiellement « modératrices » et d'autres stratégies codées « accélératrices ». Comme ce participant qui propose tout d'abord « *il doit dire oui, mais qu'il fasse en privé* », parce que c'est plus prudent « *d'aller en privé que d'aller dans une salle* » où il y aurait d'autres personnes, mais propose aussi de « *dire non, parce que pour lui c'est un peu gênant* ». Parmi les autres stratégies de réaction proposées par ces 6 personnes, les réponses de 3 participants ont été catégorisées comme « émotionnelles » dans le sens où ces personnes proposent de « *lui demander d'abord pourquoi elle veut lui faire une photo nue et que ça servirait à quoi* » (n = 2) ou de « *faire mieux connaissance* » (n = 1). Une personne dit tout d'abord ne pas savoir quoi faire (codé « aucune réponse »), puis après avoir été questionnée à nouveau par l'évaluateur, répond qu'elle dirait non. Une participante répond tout d'abord que Marie ne « *doit pas se déshabiller* », puis change d'avis quand l'évaluatrice lui précise que Marie connaît la personne qui lui fait la demande : « *Elle se laisse faire puis voilà !* ».

Item N°22 (tentative de sextorsion par une personne inconnue). La quasi-totalité des personnes interviewées (n = 49, sur 51) propose une stratégie de réponse catégorisée « modératrices ». Une participante mentionne la possibilité de faire appel à un tiers, et une participante mentionne les deux options (autoprotection et protection indirecte) spontanément. Parmi les 49 personnes refusant spontanément de se déshabiller, la plupart (n = 39) émettent une, voire plusieurs justifications, à ce refus (n = 47 justifications), à la manière de cette participante qui explique :

« Si on [ne] connaît pas la personne, il faut lui dire non. Parce qu'il peut nous prendre en photo et mettre partout sur internet et puis c'est assez privé. Puis si on [n']a pas envie, et puis si l'inconnu insiste, il faut en parler à ses parents ».

Cette participante évoque ainsi plusieurs raisons à son refus et propose plusieurs stratégies (dire non, en parler à des personnes de confiance). Tout comme elle, d'autres participants relèvent principalement le fait que la personne est inconnue (n = 8), et/ou font référence au risque de diffusion de l'image (n = 13) pour expliquer leur refus, comme cette autre participante qui explique « *après on [ne] sait pas s'il va mettre sur Facebook ou les réseaux sociaux* ». Une autre partie des raisons évoquées (n = 13) est liée au fait que la demande touche à l'intimité, « *dire non, c'est privé montrer, c'est intime* ».

» ou encore que « *ça ne se fait pas* », « *c'est pas bien* » ($n = 11$). Deux personnes justifient leur refus plutôt par le fait de ne pas avoir le droit de se déshabiller, que « *c'est interdit* ».

Deux personnes, parmi les 51 ayant répondu à l'item N°22, accepteraient de se déshabiller. L'une des deux pose tout de même une condition : « *Il doit lui dire oui. Mais seulement, si c'est que elle qui regarde* ». Cinq personnes proposent des réponses contradictoires. Un participant dit tout d'abord ne pas savoir quoi faire, puis après avoir été questionné à nouveau par l'évaluateur, répond qu'il dirait non. Quatre personnes proposent d'abord de demander pourquoi « *Il doit dire : Pourquoi je dois mettre tout nu ?* », puis après évoquent la possibilité de « *dire non* ».

Tentative de vol. Les stratégies proposées dans les items N°12 « Pierre/Marie a reçu un téléphone portable pour Noël, une amie lui demande de lui donner » et N°13 « Quelqu'un sonne à la porte. Marie/Pierre lui ouvre. La personne dit qu'elle n'a pas d'argent, mais qu'elle a besoin d'une nouvelle TV » et justifications sont présentées ci-après.

Item N°12 (tentative de vol par une amie). La quasi-totalité des personnes interviewées ($n = 48$ sur 51) propose une stratégie de réponse catégorisée comme étant de l'autoprotection. Une personne mentionne deux stratégies (autoprotection et protection indirecte). Parmi les 48 personnes qui refuseraient de donner leur téléphone, la plupart ($n = 40$) émettent une ou plusieurs justifications à ce refus ($n = 44$ justifications). Plusieurs participants font référence au fait qu'il s'agit d'un cadeau de Noël ($n = 15$), comme ce participant qui explique : « *Dire non parce que c'est le téléphone qu'il a reçu pour Noël, donc c'est pas bien de donner* ». Ils sont aussi plusieurs à souligner le fait que le téléphone soit « le sien » ($n = 15$), à l'image de cette participante : « *Moi, je dirais non. Parce que d'abord, c'est son propre natel¹* » et/ou que si Pierre (ou Marie) le donne, « *après il a plus de natel* » ($n = 2$). Parmi les autres raisons évoquées pour refuser le fait de donner son téléphone, cinq participants trouvent qu'il y a des choses privées dessus et que par exemple, « *après il peut fouiller dans les numéros et regarder les numéros privés* ». Quatre personnes expliquent en avoir potentiellement besoin, comme ce participant qui propose de refuser, car « *en plus, c'est important les téléphones si on doit faire un appel urgent* ». Deux personnes mentionnent le fait qu'un téléphone, ça coûte cher : « *Bon là il est en cadeau ça va, mais, ça a coûté cher un téléphone donc faut pas qu'elle le donne*

après ». Enfin, une personne explique refuser « *parce qu'après elle peut aller téléphoner à quelqu'un d'autre et puis après elle fait des demandes et elle peut harceler quelqu'un au téléphone et la personne [ne] l'aime pas* ».

Trois personnes parmi les 51 interviewées ne proposent aucune stratégie réduisant l'exposition au risque. Deux acceptent de donner leur téléphone, sans donner plus d'explication « *elle lui donne* ». La troisième propose d'aller « *acheter un au magasin* » pour son amie, et explique que c'est parce qu'elles se connaissent que cette solution est la plus appropriée. Deux participants ont une réponse contradictoire. L'un d'eux propose tout d'abord de donner, tandis que l'autre propose de lui dire : « *Pourquoi tu veux ce téléphone, c'est mon cadeau ?* ». Tous deux changent d'avis par la suite et proposent de dire non.

Item N°13 (tentative de vol par un inconnu). Trente-neuf personnes interviewées sur 51 proposent une stratégie de réponse catégorisée comme étant de l'autoprotection. Vingt-huit d'entre elles proposent une justification pour expliquer leur refus. Douze relèvent que c'est son argent, comme l'explique ce participant « *parce que voilà, c'est son argent et il fait ce qu'il veut avec* » tandis qu'une autre explique « *c'est pas la banque* ». De la même manière, cinq participants relèvent le fait que la télévision appartient à Pierre ou Marie, « *c'est pas un magasin* » explique un participant, tandis qu'un autre dit « *parce que c'est sa télé à lui, il va pas lui donner* ». D'autres soulèvent le fait que la personne est une inconnue ($n = 4$) : « *Alors, elle [ne] devrait pas... La personne, elle [ne] la connaît pas...* » ou plus généralement, que cela n'est pas « normal », « *qu'elle ne doit pas donner son argent, ni sa télé à cet homme* » ($n = 6$) ou encore que ce n'est pas son problème : « *Parce que voilà, il [ne] veut pas lui donner sa télévision ni son argent, parce que c'est, voilà, c'est pas bien. Et puis, je pense, elle peut ... si elle [n]a pas d'argent, après, voilà, c'est son problème* ».

Douze personnes parmi les 51 interviewées acceptent la demande de l'inconnu. Trois personnes proposent des réponses contradictoires, c'est-à-dire qu'elles proposent à la fois des stratégies relevant de l'autoprotection ou/et protection indirecte (codées « modératrices ») et d'autres stratégies codées « accélératrices ». Parmi les stratégies proposées par ces 15 participants, une personne dit ne pas savoir quoi répondre, une autre propose que Pierre, : « *Prend la télé et met sur la porte là* ». Treize personnes proposent des réponses très empathiques, comme celle d'inviter l'inconnu/e pour regarder la télé avec lui ($n = 3$), ou alors de demander comment il s'appelle, pourquoi il

¹ Natel fait référence au téléphone portable en Suisse

vient frapper à la porte, pourquoi il veut de l'argent ($n = 3$) et évoquent certaines justifications, comme : « *parce qu'on dirait qu'elle a besoin de s'exprimer* » ($n = 1$), ou de « *donner de l'argent pour qu'il s'achète la même* » ($n = 7$), « *parce que s'il [n']a pas d'argent, il [ne] peut pas s'acheter une télé* » ($n = 6$) et/ou « *parce que comme ça il lui fiche la paix* » ($n = 2$).

Tentative d'hameçonnage. L'item 21 « Sur Internet, un/e inconnu/e demande à Marie/Pierre de lui donner son numéro de téléphone » fait référence à une tentative hameçonnage. Les stratégies proposées par les participants et les justifications sont présentées ci-après.

Item N°21. La quasi-totalité des personnes interviewées ($n = 48$, sur 50) propose une stratégie de réponse catégorisée comme étant de l'autoprotection ($n = 46$), parfois associée à une protection indirecte ($n = 2$), à l'image de cette participante, qui explique « *elle pourrait dire :*

« Écoute, vous êtes un inconnu, je [ne] donne pas mon numéro à des inconnus... Surtout qu'elle [ne] connaît pas cet inconnu. Parce que des fois on [ne] sait pas sur qui on tombe sur internet... Parce que une fois qu'il a son numéro, l'inconnu, il pourrait la harceler de messages, de appels puis c'est mieux pas de ça justement ».

Comme elle, d'autres participants évoquent des raisons à leur refus ($n = 40$ participants évoquent 48 justifications). La plupart refusent, car la demande provient d'une personne inconnue ($n = 22$) et/ou parce qu'il/elle risque d'harceler la personne ou de diffuser son numéro ($n = 18$). Huit participants expliquent que « *ça ne se fait pas* », « *qu'on ne doit pas* » donner son numéro sur internet.

Deux personnes parmi les 50 interviewées acceptent la demande de l'inconnu. Six personnes proposent des réponses contradictoires. Parmi les stratégies proposées par ces huit participants, deux participants disent « *je [ne] sais pas* » puis ils proposent « *il [ne] devrait pas donner* ». La troisième participante explique qu'il faut dire non, puis propose ensuite de « *lui dire d'aller en prison, parce que ça fait du mal* ». Deux autres participants proposent de « *demander pourquoi il/elle veut son numéro* », puis un des deux refuse. Enfin, un participant propose d'éteindre l'ordinateur et de ne plus aller sur internet : « *Dire non. Puis, éteindre l'ordinateur. Et [ne] plus aller sur Internet* ». Finalement, trois participants donnent leur numéro, dont deux changent d'avis ensuite et refusent, parce que « *il [ne] doit pas donner* » ou « *parce qu'il dit, connaît pas, parce qu'il [ne] faut pas donner* ».

Discussion

En interrogeant les personnes présentant une DI sur leurs réactions face à des scénarios spécifiques, cette étude donne un premier aperçu de leurs ressources et vulnérabilités face aux risques numériques. Les résultats permettent non seulement de saisir dans quelle mesure les personnes présentant une DI se protègent face à ces risques et les stratégies qu'elles proposent, mais ils contribuent également à éclairer quelles sont les difficultés qu'elles rencontrent face aux risques véhiculés par les TIC. Cela étant, ces résultats fournissent des indications importantes concernant le développement des interventions en matière de sécurité sur internet.

Tout d'abord, les résultats montrent que, dans les cinq scénarios présentés, une majorité de participants propose des stratégies autodéterminées permettant de se protéger face aux risques numériques. Ces résultats sont similaires aux résultats de la recherche de Molin *et al.* (2017). En effet, les résultats issus de l'analyse de contenu d'entretien mené avec 27 jeunes adultes présentant une DI, ont permis de mettre en évidence que ces jeunes étaient conscients des risques et des opportunités liés à l'utilisation d'internet et des réseaux sociaux, comme Mia, 17 ans, le rapporte dans leur recherche :

« I am very, very careful on the Internet, because you never know if you will get into trouble [...]. I would rather not meet people on the Internet because I'm afraid something bad will happen, e.g., me being abused by someone » (Molin *et al.*, 2017, p. 651).

La deuxième constatation de cette étude est qu'une proportion non négligeable de participants (environ 13 %, sauf pour l'item N°13, environ 29 %) ne propose pas de stratégie permettant de diminuer l'exposition aux risques présents dans les scénarios présentés, ou propose des stratégies ambivalentes. Inconscientes du risque existant, ces personnes sont potentiellement à risque de victimisation (Greenspan, Switzky et Woods, 2011). Cette proportion de 13 % correspond à celle rapportée par Begara Iglesias *et al.* (2019), dans leur recherche sur le cyber harcèlement auprès d'adolescents présentant une DI. En effet, dans cette recherche impliquant 181 participants (45 jeunes présentant une DI, 31 jeunes présentant un syndrome d'Asperger et 105 jeunes tout-venant), 13,3 % des jeunes présentant une DI répondaient par l'affirmative (contre 2,85 % des jeunes tout-venant) à l'item « *Without my consent, someone has taken photos or made video recordings of me with sexual content and has disseminated them via mobile phone or the Internet* ». Ce résultat semble également s'aligner avec la recherche de Jenaro *et al.* (2018) dans laquelle, sur

un échantillon de 269 adultes présentant une DI, 15 % rapportent avoir été victimes de cyber harcèlement.

Dans notre troisième observation, nous constatons que près de 30 % des participants rencontrent des difficultés à proposer des stratégies de protection face à l'item N°13 : « Quelqu'un sonne à la porte. Marie/Pierre lui ouvre. La personne dit qu'elle n'a pas d'argent, mais qu'elle a besoin d'une nouvelle TV ». Une hypothèse pour expliquer que cet item soit le moins réussi des cinq scénarios liés aux risques véhiculés par les TIC pourrait être liée à la nature du risque présent dans ce scénario. Contrairement aux autres items, l'item N°13 suppose ni de se déshabiller, ni de donner (des informations concernant) son téléphone. En ce sens, il peut être considéré comme sollicitant plus un côté social que les autres scénarios. Cela irait en tout cas dans la direction des résultats de la recherche de Lough et Fisher (2016) portant sur 28 adultes présentant un syndrome de Williams. En analysant les réponses des participants à des scénarios liés à la sécurité sur internet, Lough et Fisher (2016) ont rapporté que, comme c'est le cas dans cette étude, la plupart des participants donnent des réponses correctes qui minimisent le risque. Néanmoins, les participants étaient plus susceptibles de proposer des stratégies qui augmentaient le risque lorsque le risque était social (p. ex., envoyer des photos de soi à une personne inconnue en ligne) versus « non social » (p. ex., donner son numéro de compte en banque). Une autre hypothèse qui pourrait expliquer pourquoi cet item N°13 a mis près de 30 % des participants en difficulté serait liée au scénario lui-même. Ainsi, la majorité des participants semble comprendre les risques liés aux TIC et connaît des stratégies autodéterminées pour s'en protéger. Pourtant, il se pourrait qu'ils et elles se contentent de répéter des mesures de sécurité qui leur ont été enseignées. C'est en tout cas ce que laisse entrevoir le nombre élevé de justifications liées à une règle apprise (« on ne doit pas »; « ça ne se fait pas »). L'item le moins réussi serait donc celui auquel les participants n'ont pas été « préparés », et en ce sens il est vrai que le scénario de la télévision peut paraître invraisemblable. Ce lien avec les règles apprises est également évoqué par Löfgren-Mårtenson (2008) qui s'est intéressée à l'utilisation d'internet de jeunes adultes présentant une DI. L'analyse des 10 entretiens qu'elle a menés suggère que ces jeunes adultes comprennent et ont des stratégies qui leur permettent de gérer les risques liés à l'utilisation d'internet. Néanmoins, l'auteure émet l'hypothèse qu'à l'exception de certains contextes où ils s'en affranchissent, ils se contentent parfois de répéter les mesures de sécurité qu'on leur a enseignées ce qui rend difficile l'évaluation de leur niveau de maîtrise des conduites d'autoprotection.

Ces résultats soulignent d'un côté, l'importance de concevoir, de manière holistique, les mesures de prévention contre la victimisation des personnes présentant une DI. En effet, les résultats, et plus particulièrement le taux de difficulté rencontré à l'item N°13, semblent confirmer l'affirmation de Finkelhor (2014) selon laquelle les problèmes que posent les technologies de l'information et de la communication ne sont pas spécifiques, mais bien des extensions des problèmes d'interaction sociale. Pour les personnes présentant une DI, cela signifie que les facteurs qui alimentent leur vulnérabilité dans le monde réel sont susceptibles de servir également de facteurs de risque dans le monde en ligne (Lough et Fisher, 2016). Dans ce sens, il ne s'agit pas d'éviter les risques numériques, ni de concevoir des programmes spécifiques liés à leur prévention, mais plutôt d'insérer ce type de prévention dans les programmes qui visent à développer les habiletés prosociales, émotionnelles, de gestion des conflits et de la colère (Sallafranke-St-Louis, 2015; Wells et Mitchell, 2014).

De l'autre, les résultats confirment l'importance de l'approche des risques mesurés (Seale, 2014). Comprendre comment la personne perçoit et négocie les risques constitue ainsi une première étape, permettant de réfléchir et d'organiser ensemble les soutiens conduisant à une meilleure participation sociale, tant hors ligne qu'en ligne. Cette approche rappelle en outre que les technologies de l'information et de la communication sont vectrices de risques, mais qu'elles offrent des opportunités de participation qui peuvent être émancipatrices pour les personnes présentant une DI (Löfgren-Mårtenson, 2008; Molin *et al.*, 2017; Sorbring, Molin et Löfgren-Mårtenson, 2017).

Conclusion

Certaines limites dans cette étude doivent toutefois être mentionnées quant aux résultats obtenus. Tout d'abord, si le TV-22 permet d'observer quelles sont les connaissances des participants en théorie, cela ne signifie pas pour autant que leurs réactions dans la réalité reflèteront leurs connaissances. De la même manière, l'utilisation que les participants font des TIC n'a pas été rapportée (p. ex., la fréquence et le type d'utilisation qu'ils ou elles font de leur téléphone, de l'ordinateur, d'internet, des médias sociaux). En outre, nous n'avons pas exploré si les scénarios présentés dans le TV-22 étaient entièrement fictifs ou si les participants avaient déjà été confrontés à ce genre de situations. Enfin, les stratégies mentionnées par les participants sont peut-être issues d'un désir de plaire ou d'acquiescer : les entretiens menés avec le TV-22 ayant été enregistrés sur bande audio et non filmés, il n'a pas été possible d'analyser l'influence potentielle des

réactions non-verbales des évaluateurs sur les stratégies, notamment les stratégies contradictoires, évoquées par les participants.

Aussi, au-delà des critères d'inclusion (plus de 18 ans, présentant une DI) et mis à part le genre, le profil des participants (p. ex., âge, besoin de soutien, lieu de résidence) n'était pas connu de l'équipe de recherche, ce qui limite les hypothèses et analyses pouvant être effectuées. Enfin, la démarche d'analyse de contenu séquencée, bien que permettant une analyse efficace et uniforme du corpus, contribue également à la perte de certains détails qui peuvent être importants (Paillé et Mucchielli, 2012).

Malgré les limites énoncées, cette étude propose des pistes de compréhension sur la façon dont les adultes présentant une DI perçoivent et négocient les risques numériques. En outre, en plus d'amener de nouvelles connaissances sur les ressources et vulnérabilités de ces personnes, elle présente l'avantage d'analyser directement les propos des personnes concernées et non celle de leurs proches. Les résultats de cette recherche permettent ainsi de relever que, dans les 5 scénarios présentés, la majorité des participants semblent comprendre les risques associés aux TIC et connaissent des stratégies autodéterminées pour s'en protéger. Cependant, il se peut que certains d'entre eux répètent les mesures de sécurité qui leur ont été enseignées, avec une intégration très relative. C'est du moins ce que suggère le nombre élevé de justifications liées à une règle apprise (« on ne doit pas »; « ça ne se fait pas »). En outre, une minorité de participants (environ 13 %, sauf pour l'item N°13, environ 29 %) ne propose pas de stratégie pour réduire l'exposition aux risques présents dans les scénarios présentés, ou propose des stratégies ambivalentes, qui les exposeraient potentiellement à un plus grand risque de victimisation.

Il s'agit d'une première étape d'exploration des ressources et des vulnérabilités face aux risques véhiculés par les TIC. D'autres recherches sont nécessaires afin de mieux documenter les interactions entre la vulnérabilité en ligne et hors ligne, les risques et les opportunités offertes par les TIC. Analyser les réponses données au TV-22 dans les autres scénarios et les catégories de risques qui ne sont pas liées aux TIC permettra notamment d'observer si les personnes concernées présentent des proportions similaires de ressources et de vulnérabilités dans d'autres scénarios ou si ces résultats sont spécifiquement liés aux risques numériques. La validité comportementale du TV-22 reste à être explorée : des recherches futures pourraient s'intéresser par exemple aux comportements en ligne réels des personnes présentant une DI et mettre en regard les comportements réels et leurs réponses au TV-22 ; de l'autre, elles pourraient aussi s'intéresser aux situations de risques et/ou de victimisation vécues et explorer les stratégies mises en place à ce moment par les personnes concernées.

Face aux taux élevés de victimisation des adultes présentant une DI, tant hors ligne qu'en ligne, il semble primordial d'encourager le développement, l'implémentation et l'évaluation de programmes de prévention axés sur les habiletés sociales et les compétences d'identification des risques et de prise de décision. Si certains programmes prometteurs ont été développés outre-Atlantique (Khemka et Hickson, 2008; Ward, Smith et Windsor, 2013), leur efficacité doit encore être confirmée (Institut national de la santé et de la recherche médicale, 2016; Mikton, Maguire et Shakespeare, 2014) et ces derniers restent pour l'heure encore rares dans le paysage francophone (Petitpierre et Tabin, 2020).

RESOURCES AND VULNERABILITIES TO DIGITAL RISKS OF ADULTS WITH INTELLECTUAL DISABILITIES

Abstract: Information and communication technologies (ICT) offer many opportunities for social participation. However, ICT exposes people who use them to risks such as cyberbullying or financial abuse. Adults with intellectual disability (ID) experience high rates of victimization, both online and offline. This study aims to assess the resources and vulnerabilities to digital risks of adults with ID. Structured interviews with 51 adults with ID were conducted using a social vulnerability assessment tool, the TV-22. Results of the thematic content analysis show that most of the participants know self-determinate strategies to handle digital risks. These results underpin the value of a positive risk-taking approach to improve on and offline social participation of adults with ID.

Keywords: Intellectual disability; ICT; digital risks; social vulnerability; Internet; social networking.

Références

- Ågren, K. A., Kjellberg, A. et Hemmingsson, H. (2020). Internet opportunities and risks for adolescents with intellectual disabilities: A comparative study of parents' perceptions. *Scandinavian Journal of Occupational Therapy*, 27(8), 601-613. doi:10.1080/11038128.2020.1770330
- Begara Iglesias, O., Gómez Sánchez, L. E. et Alcedo Rodríguez, M. A. (2019). Do young people with Asperger syndrome or intellectual disability use social media and are they cyberbullied or cyberbullies in the same way as their peers? *Psicothema*, 31(1), 30-37. doi:10.7334/psicothema.2018.243
- Borgström, Å., Daneback, K. et Molin, M. (2019). Young people with intellectual disabilities and social media: A literature review and thematic analysis. *Scandinavian Journal of Disability Research*, 21(1), 129-140. doi:10.16993/sjdr.549
- Buijs, P. C. M., Boot, E., Shugar, A., Fung, W. L. A. et Bassett, A. S. (2017). Internet safety issues for adolescents and adults with intellectual disabilities. *Journal of Applied Research in Intellectual Disabilities*, 30(2), 416-418. doi:10.1111/jar.12250
- Caton, S. et Chapman, M. (2016). The use of social media and people with intellectual disability: A systematic review and thematic analysis. *Journal of Intellectual & Developmental Disability*, 41(2), 125-139. doi:10.3109/13668250.2016.1153052
- Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI. (2020). Sûreté de l'information. Situation en suisse et sur le plan international. Repéré à <https://www.melani.admin.ch/>
- Chadwick, D. D. (2019). Online risk for people with intellectual disabilities. *Tizard Learning Disability Review*, 24(4), 180-187.
- Chadwick, D. D., Chapman, M. et Caton, S. (2018). Digital inclusion for people with an intellectual disability. Dans A. Attrill-Smith, C. Fullwood, M. Keep et D. J. Kuss (dir.), *The oxford handbooks of cyberpsychology* (p. 261-284). Oxford, Royaume-Uni: Oxford Handbooks Online.
- Chadwick, D. D. et Fullwood, C. (2018). An online life like any other: Identity, self-determination, and social networking among adults with intellectual disabilities. *Cyberpsychology, Behavior, and Social Networking*, 21(1), 56-64. doi:10.1089/cyber.2016.0689
- Chadwick, D., Wesson, C., et Fullwood, C. (2013). Internet access by people with intellectual disabilities: Inequalities and opportunities. *Future Internet*, 5, 376-397.
- Chiner, E., Gómez-Puerta, M. et Cardona-Moltó, M. C. (2017). Internet use, risks and online behaviour: The view of internet users with intellectual disabilities and their caregivers. *British Journal of Learning Disabilities*, 45(3), 190-197. doi:10.1111/bld.12192
- Finkelhor, D. (2014). Commentary: Cause for alarm? Youth and internet risk research - a commentary on Livingstone and Smith. *Journal of Child Psychology and Psychiatry*, 55(6), 655-658. doi:10.1111/jcpp.12260
- Greenspan, S., Switzky, H. N. et Woods, G. W. (2011). Intelligence involves risk-awareness and intellectual disability involves risk-unawareness: Implications of a theory of common sense. *Journal of Intellectual & Developmental Disability*, 36(4), 246-257. doi:10.3109/13668250.2011.626759
- Hickson, L. et Khemka, I. (2013). Problem solving and decision making. Dans M. Wehmeyer (dir.), *The Oxford handbook of positive psychology and disability* (p. 198-225). New York, NY: Oxford University Press.
- Hughes, K., Bellis, M. A., Jones, L., Wood, S., Bates, G., Eckley, L., ... Officer, A. (2012). Prevalence and risk of violence against adults with disabilities: A systematic review and meta-analysis of observational studies. *The Lancet*, 379(9826), 1621-1629. doi:10.1016/S0140-6736(11)61851-5
- Institut national de la santé et de la recherche médicale. (2016). *Déficiences intellectuelles*. Repéré à http://www.ipubli.inserm.fr/bitstream/handle/10608/6817/expcol_2016_DI_synthese_fr.pdf?sequence=1&isAllowed=y
- Jenaro, C., Flores, N., Vega, V., Cruz, M., Pérez, Ma. C. et Torres, V. A. (2018). Cyberbullying among adults with intellectual disabilities: Some preliminary data. *Research in Developmental Disabilities*, 72, 265-274. doi:10.1016/j.ridd.2017.12.006
- Khemka, I. et Hickson, L. (2008). *ESCAPE-DD: An effective strategy-based curriculum for abuse prevention and empowerment for adults with developmental disabilities*. New York, NY: Center for Opportunities and Outcomes for People with Disabilities, Teachers College, Columbia University.
- Landis, J. R. et Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159-174. doi:10.2307/2529310
- Le Robert. (n.d.). Hameçonnage. Repéré le 10 novembre 2020 sur <https://dictionnaire.lerobert.com/definition/hameconnage>
- Löfgren-Mårtenson, L. (2004). "May I?" About sexuality and love in the new generation with intellectual disabilities. *Sexuality and Disability*, 22(3), 197-207. doi:10.1023/B:SEDI.0000039062.73691.cb
- Löfgren-Mårtenson, L. (2008). Love in cyberspace: Swedish young people with intellectual disabilities and the internet. *Scandinavian Journal of Disability Research*, 10(2), 125-138. doi:10.1080/15017410701758005

- Lough, E. et Fisher, M. H. (2016). Internet use and online safety in adults with williams syndrome: Online safety and WS. *Journal of Intellectual Disability Research*, 60(10), 1020-1030. doi:10. 1111/jir.12281
- Lussier-Desrochers, D., Normand, C. L., Romero-Torres, A., Lachapelle, Y., Godin-Tremblay, V., Dupont, M.-È., ... Bilodeau, P. (2017). Bridging the digital divide for people with intellectual disability. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 11(1), Article 1.
- Mikton, C., Maguire, H. et Shakespeare, T. (2014). A systematic review of the effectiveness of interventions to prevent and respond to violence against persons with disabilities. *Journal of Interpersonal Violence*, 29(17), 3207-3226. doi:10.1177/0886260514534530
- Molin, M., Sorbring, E. et Löfgren-Mårtenson, L. (2017). New emancipatory landscapes? Young people with intellectual disabilities, internet use, and identification processes. *Advances in Social Work*, 18(2), 645-662. doi:10.18060/21428
- Normand, C. L., Rodier, S., Lussier-Desrochers, D. et Giguère, L. (2017). Peut-on favoriser l'inclusion sociale des jeunes par l'utilisation des médias sociaux? *Revue francophone de la déficience intellectuelle*, 27, 101-115. doi:10.7202/1043127ar
- Office québécois de la langue française. (2018). Sextorsion. Repéré le 10 novembre 2020 à http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26529614
- Paillé, P. et Mucchielli, A. (2012). *L'analyse qualitative en sciences humaines et sociales* (2^e éd.). Paris, France: Armand Colin.
- Petitpierre, G. (2018). *Validation du test de compétences interpersonnelles et de vulnérabilité personnelle, version française, enrichie, accessibilisée et informatisée*. Repéré à <http://p3.snf.ch/Project-176196>
- Petitpierre, G., Gremaud, G., Veyre, A., Bruni, I. et Diacquenod, C. (2013). *Aller au-delà de l'alibi. Consentement à la recherche chez les personnes présentant une déficience intellectuelle*. Repéré à http://www.seg-sse.ch/pdf/2013-03-27_Petitpierre.pdf
- Petitpierre, G. et Tabin, M. (2020). From social vulnerability assessment to active prevention measures: A decision-making perspective [Manuscrit soumis pour publication].
- Ramsten, C., Martin, L., Dag, M. et Marmstål Hammar, L. (2019). A Balance of social inclusion and risks: Staff perceptions of information and communication technology in the daily life of young adults with mild to moderate intellectual disability in a social care context. *Journal of Policy and Practice in Intellectual Disabilities*, 16(3), 171-179. doi:10. 1111/jppi.12278
- Sallafranque-St-Louis, F. (2015). *L'utilisation d'Internet et la sollicitation sexuelle sur le Web auprès des personnes avec une déficience intellectuelle (DI) ou un trouble du spectre de l'autisme (TSA)* (Thèse de doctorat inédite). Université du Québec en Outaouais, QC.
- Salmerón, L., Fajardo, I. et Gómez-Puerta, M. (2019). Selection and evaluation of Internet information by adults with intellectual disabilities. *European Journal of Special Needs Education*, 34(3), 272-284. doi:10.1080/08856257.2018.1468634
- Seale, J. (2014). The role of supporters in facilitating the use of technologies by adolescents and adults with learning disabilities: A place for positive risk-taking? *European Journal of Special Needs Education*, 29(2), 220-236. doi:10.1080/08856257. 2014.906980
- Seale, J. et Chadwick, D. (2017). How does risk mediate the ability of adolescents and adults with intellectual and developmental disabilities to live a normal life by using the Internet? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 11(1), article 2. doi:10.5817/CP2017-1-2
- Sorbring, E., Molin, M. et Löfgren-Mårtenson, L. (2017). "I'm a mother, but I'm also a facilitator in her every-day life": Parents' voices about barriers and support for internet participation among young people with intellectual disabilities. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 11(1), article 3. doi:10. 5817/CP2017-1-3
- Tabin, M., Diacquenod, C., De Palma, N., Gerber, F., Straccia, C., Wilson, C., ... Petitpierre, G. (2020). Cross-Cultural Preliminary Validation of a Measure of Social Vulnerability in People with Intellectual Disabilities. *Journal of Intellectual & Developmental Disability*. doi: 10.3109/13668250.2020.1793450
- Ward, K. M., Smith, C. et Windsor, R. (2013). A friendship et dating program for adults with intellectual and developmental disability: A formative evaluation. *Research in Developmental Disabilities*, 51, 22-32. doi:10.1352/1934-9556-51.01.022.
- Wells, M. et Mitchell, K. J. (2014). Patterns of Internet use and risk of online victimization for youth with and without disabilities. *The Journal of Special Education*, 48(3), 204-213.
- Wong, A., Chan, C., Litsang, C. et Lam, C. (2009). Competence of people with intellectual disabilities on using human-computer interface. *Research in Developmental Disabilities*, 30(1), 107-123. doi:10. 1016/j.ridd.2008.01.002