CONSULTATION PUBLIQUE CONCERNANT LA CYBERSÉCURITÉ AU QUÉBEC

L'objectif de cet appel de mémoires est de recueillir plusieurs points de vue sur les enjeux et défis du Québec en matière de cybersécurité et sur les pistes de solutions concrètes pour un Québec cybersécuritaire et cyberrésilient.

Mémoire déposé par le Centre de documentation sur l'éducation des adultes et la condition féminine

CDEACF
Centre de documentation
sur l'éducation des adultes et la condition féminine

À l'attention du ministère de la Cybersécurité et du Numérique.

29 novembre 2023

TABLE DES MATIÈRES

RENSEIGNEMENTS SUR LA PERSONNE QUI DÉPOSE LE MÉMOIRE

Mme Lise Chovino, responsable Stratégie numérique au Centre de documentation sur l'éducation des adultes et la condition féminine. Le CDÉACF est un OBNL (voir la présentation du CDÉACF à la page suivante).

PRÉSENTATION DU CDÉACF

Mission :

Dans une perspective de démocratisation des connaissances, de transformation sociale, de reconnaissance du droit à l'information, de valorisation du patrimoine documentaire communautaire canadien et québécois et d'inclusion de toutes et tous dans la société de l'information, le Centre de documentation sur l'éducation des adultes et la condition féminine constitue un carrefour d'échanges et un espace d'expression qui a pour fonction de collecter, de diffuser, de promouvoir et de rendre accessibles, en français, les savoirs et les savoir-faire à tous les milieux de l'éducation, de la formation et de l'alphabétisation des adultes ainsi qu'à tous les milieux de la condition des femmes du Québec et des communautés francophones du Canada.
Nos principes sous-jacents sont :

- la démocratisation des connaissances;
- la démocratisation des technologies de l'information et des communications;
- le droit à l'information;
- le droit des adultes à l'éducation et à la formation;
- la valorisation du patrimoine documentaire communautaire;
- la valorisation des savoirs et savoir-faire des milieux de l'éducation des adultes, de l'alphabétisation, de la condition féminine et de l'action communautaire;
- l'importance et la reconnaissance des organismes de la société civile.

Le CDÉACF œuvre depuis 40 ans auprès des groupes d'alphabétisation, d'éducation aux adultes et des groupes de femmes de la francophonie canadienne. Il est leur centre de documentation et de formation sur l'utilisation des technologies du numérique depuis ses débuts. Reconnu comme un organisme de formation par le ministère de l'Éducation et de l'Enseignement supérieur, il fournit à ces groupes du matériel didactique et andragogique sur différents thèmes, du soutien technique et technopédagogique, ainsi que de la formation.

Le CDÉACF a été précurseur dans la formation des groupes de femmes sur les technologies de l'information et des communications. Sa vision du rôle que les TIC pouvaient jouer dans le développement des groupes de femmes et du mouvement féministe s'est rapidement traduite en action avec la mise en place d'*Internet au féminin* en 1997, puis du site *Netfemmes*.

Le CDÉACF a aussi développé une grande expérience d'intervention avec les groupes de femmes sur les questions de cybersécurité en contexte communautaire et est devenu une référence pour les maisons d'hébergement pour femmes victimes de violence conjugale sur les questions de sécurité en lien avec les appareils connectés depuis 2016.

RÉSUMÉ DU MÉMOIRE ET SOMMAIRE DES RECOMMANDATIONS

Résumé du mémoire

Nous pensons qu'il est essentiel de prendre en compte certains enjeux qui risquent d'affecter le déploiement, la réception auprès de la population et en bout de ligne l'efficacité du Plan national de cybersécurité du Québec (PNCQ). Particulièrement, le CDÉACF souhaite par ce mémoire attirer l'attention sur 3 enjeux, qui sont encore trop peu étudiés, ou, quand ils le sont, sont abordés en silos hermétiques. Or, à l'heure actuelle, nous devons adresser l'interdépendance de ces 3 enjeux, afin d'offrir des solutions véritablement structurantes en matière de développement numérique et de cybersécurité.

Les 3 enjeux présentés dans ce mémoire sont:

1. Les fractures numériques
2. Le capitalisme de surveillance
3. Les violences facilitées par la technologie.

Premièrement, parler des fractures numériques, c'est prendre en compte le fait qu'une grande partie de la population québécoise est confrontée à des difficultés d'accès et d'utilisation des outils numériques. Dans ce sens, les mesures mises en place dans le cadre du PNCQ afin d'améliorer la sécurité et la confidentialité en ligne doivent être facilement accessibles aux usagers et usagères des plateformes et outils numériques déployés. Les organismes œuvrant auprès des populations ayant besoin d'aide avec le numérique doivent aussi être soutenus dans ce travail, que ce soit leur mission directe ou non.

Deuxièmement, rappeler que nous sommes à l'ère de l'internet commercial et du capitalisme de surveillance est central dans la réflexion sur les pistes d'action à entreprendre afin de rendre le Québec cyberrésilient. Dans ce sens, penser au capitalisme de surveillance, c'est reporter l'attention sur les systèmes de capitalisation à l'œuvre dans le domaine numérique et comprendre que ces enjeux dépassent complètement le niveau individuel.

Il est en effet essentiel d'avoir une vision globale des besoins, enjeux et acteurs du domaine du numérique afin de ne pas se tromper de cible dans les mesures qui seront proposées dans le PNCQ.

Troisièmement, les violences facilitées par la technologie touchent un grand nombre de personnes, particulièrement les femmes et les personnes racisées et autochtones. Le fait d'avoir le contrôle sur son identité et sur la confidentialité de ses informations en ligne est important pour toute la population.

Cependant, en contexte de violence, les incidents de confidentialité peuvent avoir des conséquences désastreuses, tant en ligne que pour la sécurité physique de la personne ciblée, de son entourage et des travailleuses des ressources d'aide qui la soutiennent.

Prenant en compte les questions de fractures numériques et de capitalisme de surveillance, il s'avère que les solutions devant émaner du PNCQ ne devront pas uniquement reposer sur la responsabilisation des individus, mais aussi, et surtout, soutenir une action collective et compréhensive du contexte numérique global dans lequel nous vivons, afin d'améliorer la protection des victimes de violence facilitée par la technologie.

Sommaire des recommandations

- **RECOMMANDATION 1 :** Soutenir les groupes communautaires faisant office d'aidants numériques

- **RECOMMANDATION 2 :** Fournir de l'information accessible sur les mesures de cybersécurité décidées dans le PNCQ

- **RECOMMANDATION 3 :** Appliquer les recommandations du rapport *Protéger la vie privée pour prévenir l'homicide conjugal*

- **RECOMMANDATION 4 :** Faire le lien entre le MCN, les autres ministères et le SCF pour adresser le continuum des violences

- **RECOMMANDATION 5 :** Analyser les questions de protection de la vie privée en ligne de manière structurelle et systémique

- **RECOMMANDATION 6 :** Prendre des mesures fortes face aux GAFAM pour améliorer la protection des données de la population

- **RECOMMANDATION 7 :** Élaborer et évaluer le PNCQ en concertation plurisectorielle

- **RECOMMANDATION 8 :** Ne pas justifier en ligne des pratiques décriées, malgré le besoin de sécurité, ex. surveillance

ENJEUX ET DÉFIS POUR LE QUÉBEC

Les principaux enjeux et défis, actuels ou émergents, en matière de cybersécurité que le Québec devrait prendre en considération

1. Fractures numériques

La population du Québec n'est pas homogène en matière d'accès aux technologies et d'aisance à les utiliser. En effet, plusieurs études démontrent une disparité aux différents niveaux de fracture numérique: accès matériel aux technologies (ressources, accessibilité universelle, infrastructures), littératie numérique, accès aux services essentiels en ligne.

Par exemple, l'impact des fractures numériques sur l'accès de la population québécoise aux services de cyberadministration est déjà bien documenté. Le gouvernement du Québec, comme fournisseur de services numériques, a donc la responsabilité de s'assurer que la population soit accompagnée de manière adéquate pour comprendre et utiliser les outils mis à disposition. Il en est de même pour toute mesure de sécurité et de confidentialité numérique qui seront développées dans le cadre du PNCQ.

Défi 2 : le Québec manque d'aidants numériques. Les personnes vulnérables se tournent donc vers leurs ressources de confiance pour chercher des réponses et utiliser les services en ligne du gouvernement. Ces personnes cherchent surtout du support dans les organismes communautaires, qui les accompagnent sans pour autant être financés ou reconnus pour ce travail. Il s'agit de la réalité de nombreux centres de femmes, groupes d'alphabétisation pour adultes et groupes d'éducation populaire à travers le Québec.

Défi 3 : la cyberadministration, la plus sécurisée soit-elle, ne doit pas ignorer le besoin de maintien de services en présence dont fait état la population aux prises avec les fractures numériques.

2. Capitalisme de surveillance

Aborder le capitalisme de surveillance, c'est adresser les pratiques numériques qui contreviennent à la protection de nos renseignements personnels et peuvent augmenter la vulnérabilité de la population.

Plusieurs pratiques problématiques sont déjà documentées : chambres à écho renforçant la stigmatisation, propagation massive de la désinformation genrée amplifiée par les technologies d'hypertrucage, déploiement d'algorithmes de recommandation de contenus (bons ou mauvais, souhaités ou non), pratiques anti-consentement empêchant de refuser l'enregistrement de nos données, politiques de confidentialité difficiles à comprendre, renforcement des inégalités, revente de données personnelles sans consentement explicite, hébergement de nos données sur des serveurs appartenant à des compagnies non soumises à la régulation québécoise voire canadienne, etc.

Bien qu'éduquer la population pour une meilleure prise en main des technologies soit important, cibler les individus n'est pas suffisant - un système alimenté par nos renseignements personnels cherchera constamment des moyens de les obtenir, quelles que soient nos initiatives individuelles.

3. Violences facilitées par la technologie

Défi 1: les violences facilitées par la technologie prennent plusieurs formes, utilisent plusieurs appareils et plateformes, et sont exercées dans plusieurs contextes, notamment : contextes plus dépersonnalisés des réseaux sociaux, attaques généralisées de vol d'identité, intimidation ciblant une personne ou un groupe de personnes, mais aussi violences en contexte intime, comme dans le contexte de violence conjugale. Les contextes de violence étant différents, il n'existe donc pas une stratégie universelle de cybersécurité.

Défi 2 : les outils et services numériques ne sont pas égaux en matière de recours offerts aux victimes souhaitant faire cesser ou reporter une attaque. Par exemple, il existe peu de procédures adaptées à la violence conjugale chez les fournisseurs de services et d'outils numériques.

Défi 3: recouper les questions de fractures numériques et de capitalisme de surveillance est essentiel pour accompagner les victimes. Comment aider sans ajouter à leur fardeau? De même qu'on adresse les réflexes stigmatisant la victime en contexte d'attaque physique, il faut éviter de reporter cette approche en ligne et que « pourquoi n'avais-tu pas un mot de passe fort? » devienne l'équivalent numérique de « quelle tenue portais-tu ce jour-là? ».

Le défi est donc d'adopter une approche autonomisante et déculpabilisante, mais aussi impliquer les fournisseurs de services numériques dans le renforcement du tissu de sécurité des victimes de violence facilitée par la technologie.

Rappelons aussi que, bien qu'on observe une amplification de certains types de violence via les technologies connectées (doxing, campagnes de harcèlement, etc.), les usages négatifs du numérique sont à replacer dans le continuum des violences. Par exemple: en contexte de violence conjugale, des intrusions dans les comptes en ligne peuvent avoir des conséquences directes et physiques.

BESOINS PRIORITAIRES POUR LE QUÉBEC

Les besoins prioritaires pour renforcer la cybersécurité du Québec?

1. Fractures numériques

Nous avons besoin de mesures de cybersécurité adaptées à la réalité des usages numériques au Québec, particulièrement pour les procédures demandant une action directe des usagères et usagers. Il faut que ces mesures prennent en compte et contribuent à réduire les impacts des fractures numériques.

Aussi, le fait de transposer les services publics en ligne ne supprime pas le besoin d'assistance en personne pour une grande partie de la population. Il est donc nécessaire de s'assurer d'avoir des contacts en personne qui peuvent répondre aux questions et accompagner les personnes en ayant besoin.

En plus des points de service publics en personne, les organismes communautaires ont besoin de ressources et d'être appuyés afin de continuer d'accompagner leur clientèle ayant des questions technologiques, que ce soit leur mission directe ou non.

2. Capitalisme de surveillance

Dans un contexte où la collecte, l'usage et le réemploi de nos données personnelles sont une source de pouvoir, tant pour des géants du numérique aux capitalisations boursières astronomiques que pour des instances publiques qui utilisent ces données pour alimenter des prises de décision à grand impact; dans un contexte où nos gouvernements font aussi affaire avec ces géants du numérique, au-delà de nos choix individuels d'utiliser ou non les services d'un ou l'autre des GAFAM; dans un contexte où les outils technologiques évoluent vite et où les pratiques du capitalisme de surveillance augmentent la mise en danger des victimes de violence, il est essentiel que les fournisseurs de services numériques, tant privés que publics, prennent leur part de responsabilité dans la protection de la population.

Il ne s'agit pas d'adopter des approches qui augmenteraient la surveillance de la population et d'autres pratiques déjà remises en question, notamment dans d'autres territoires étudiant les mêmes questions de cybersécurité et de confidentialité, mais d'intervenir sur l'essence même du capitalisme de surveillance en mettant la confidentialité au cœur du développement des technologies et des mesures adoptées en matière de cybersécurité, d'outiller la population pour qu'elle puisse reprendre le contrôle de ses données.

Il s'agit aussi de garder une analyse critique et différenciée (notamment ADS+, accessibilité universelle et fractures numériques) des impacts potentiels des décisions prises en matière de cybersécurité sur les différents groupes de la population afin de ne laisser personne à la marge.

3. Violences facilitées par la technologie

Il est prioritaire de fournir des solutions de cybersécurité adaptées aux contextes de violence, particulièrement au contexte de violence entre des partenaires intimes.

En effet, la recherche démontre, d'une part, que les réponses applicables quand l'agresseur connait sa victime (ex. violence conjugale) doivent nécessairement être différentes de celles à apporter dans un contexte de violence plus dépersonnalisée (ex. hameçonnage en ligne), et d'autre part,

qu'apporter des réponses technologiques prévues pour d'autres contextes de menace est peu efficace, voire a le potentiel de mettre davantage en danger les victimes de violence en contexte intime (isolement, faux sentiment de sécurité, mise en danger, absence de recours, etc.).

Il faut aussi promouvoir des approches déculpabilisantes des victimes et ne pas rejeter tout le fardeau de la sécurité technologique sur elles. Bien que l'éducation et l'information de la population soient toujours importantes, un besoin d'action concertée entre les fournisseurs de services et d'outils numériques, les ressources d'aides aux victimes et les pouvoirs publics afin de produire des solutions au niveau même du déploiement des technologies est nommé et doit être répondu.

WEBOGRAPHIE

Références:

Protéger la vie privée pour prévenir l'homicide conjugal: État des lieux des besoins en maisons d'hébergement de 2e étape et recommandations aux fournisseurs de services et outils numériques / Lise Chovino (CDÉACF), Anne-Sophie Letellier (Lab 2038), Amélie Tremblay (Lab 2038), Fanny Tan Therrien (Lab 2038), Hayfa Ben Miloud (Alliance MH2) https://biblio.cdeacf.ca/cgi-bin/koha/opac-detail.pl?biblionumber=229749

Compétences numériques des adultes québécois / CEFRIO https://transformation-numerique.ulaval.ca/wp-content/uploads/2022/09/netendances-2016-competences-numeriques-des-adultes-quebecois.pdf

Les compétences en littératie, en numératie et en résolution de problèmes dans des environnements technologiques: des clefs pour relever les défis du XXIe siècle: rapport québécois du Programme pour l'évaluation internationale des compétences des adultes (PEICA) / Institut de la statistique du Québec (ISQ) https://statistique.quebec.ca/en/fichier/competences-en-litteratie-en-numeratie-et-en-resolution-problemes-dans-environnements-technologiques-clefs-pour-relever-defis-xxie-siecle.pdf

L'inclusion sociale par le numérique: Mémoire de Communautique déposé au Ministère de l'Emploi et de la Solidarité sociale dans le cadre de la consultation publique pour l'élaboration du quatrième plan d'action gouvernemental en matière de lutte contre la pauvreté et l'exclusion sociale https://www.communautique.quebec/memoire-plan-pauvrete-et-exclusion-sociale/

Inégalités d'accès et d'usage des technologies numériques: un déterminant préoccupant pour la santé de la population? / Institut national de santé publique du Québec https://www.inspq.qc.ca/publications/3148-inegalites-acces-usage-technologies-numeriques

La fracture numérique genrée / Printemps numérique https://www.printempsnumerique.ca/veille/etude/livre-blanc-la-fracture-numerique-genree/

Dématérialisation et inégalités d'accès aux services publics / Défenseur des Droits, République française https://www.vie-publique.fr/rapport/38324-dematerialisation-et-inegalites-dacces-aux-services-publics

Les angles morts des réponses technologiques à la pandémie de COVID-19 / Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) https://observatoire-ia.ulaval.ca/rapport-les-angles-morts-des-reponses-technologiques-a-la-pandemie-de-covid-19/

Le capitalisme de surveillance: menace à la démocratie et aux droits [Dossier] / Ligue des droits et libertés https://liguedesdroits.ca/revue-le-capitalisme-de-surveillance/

Le capitalisme de surveillance « like » la fracture numérique / Lise Chovino et Catherine St-Arnaud Babin https://liguedesdroits.ca/le-capitalisme-de-surveillance-like-la-fracture-numerique/

À l'ère du capitalisme de surveillance / Ligue des droits et libertés https://liguedesdroits.ca/a-lere-du-capitalisme-de-surveillance/

The State of Digital Literacy: A literature review / Brookfield Institute for Innovation + Entrepreneurship (BII+E) https://brookfieldinstitute.ca/the-state-of-digital-literacy-a-literature-review/

When Protection Becomes an Excuse for Criminalisation: Gender Considerations on Cybercrime Frameworks / Association for Progressive Communications (APC) https://www.apc.org/sites/default/files/gender_considerations_on_cybercrime_0.pdf

Privacy First: A Better Way to Address Online Harms / Electronic Frontier Foundation https://www.eff.org/wp/privacy-first-better-way-address-online-harms

Gender Approaches to Cybersecurity: Design, Defence and Response / UN Institute for Disarmament Research https://www.apc.org/sites/default/files/Gender_Approaches_to_Cybersecurity_Digital_Final.pdf

A Framework for Developing Gender-Responsive Cybersecurity Policy / Association for Progressive Communications (APC) https://www.apc.org/en/pubs/framework-gender-cybersec

Supporting Safer Digital Spaces : Highlights / Centre for International Governance Innovation (CIGI) https://www.cigionline.org/static/documents/OGBV_Highlights_web.pdf

Orbits: a Global Field Guide to Advance intersectional, Survivor-Centred, and Trauma-Informed Interventions to TGBV : Policy Chapters

https://file.notion.so/f/f/15feab91-487b-4b2d-85f3-c04b28a217ba/c88a813d-f661-4493-8b07-5ddb411d1fdf/Policy_chapters.pdf

Violence basée sur le genre facilitée par la technologie: rendre tous les espaces sûrs / Fonds des Nations Unies pour la population https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-FR.pdf

Étude: L'hostilité en ligne envers les femmes / Conseil du statut de la femme https://csf.gouv.qc.ca/wp-content/uploads/Etude-hostilite-en-ligne-envers-les-femmes.pdf

Business and Technology: Feminist Design / Fonds des Nations Unies pour la population https://www.unfpa.org/sites/default/files/resource-pdf/SummaryforBusiness%20and%20Tech-Feminist%20Design_2022.pdf

Gender and Technology: A rights-based and intersectional analysis of key trends / Oxfam https://oxfamilibrary.openrepository.com/bitstream/handle/10546/621189/rr-gender-and-technology-050521-en.pdf