ACPPU Actualité juridique

juin 2024

Rapport concernant une plainte sur la protection de la vie privée PI21-00001 Objet : Université McMaster 28 février 2024

Le Commissariat à l'information et à la protection de la vie privée (CIPVP) de l'Ontario a conclu que l'avis d'utilisation d'un logiciel de surveillance d'examens par l'Université McMaster contrevenait à certains aspects de la *Loi sur l'accès à l'information et la protection de la vie privée*[1] de la province. En 2021, le CIPVP a reçu une plainte concernant l'utilisation par l'Université McMaster de logiciels de surveillance d'examens, Respondus LockDown et Respondus Monitor. Un étudiant se plaignait que McMaster recueillait de manière inappropriée des renseignements personnels sans faire preuve de transparence quant à l'utilisation et à la disposition de ces renseignements. Puisque l'étudiant n'a pas consenti à révéler son identité, le CIPVP a abordé la question comme un examen des pratiques d'une institution. En effet, une plainte relative à la protection de la vie privée doit être liée à une personne en particulier pour que l'institution enquête et réponde.[2]

Le rapport du CIPVP souligne que les logiciels utilisés par McMaster comprenaient deux applications. La première, Respondus LockDown Browser, verrouille l'ordinateur de l'étudiant au sein d'un système de gestion de l'apprentissage, lui interdisant ainsi l'accès à d'autres sites Web pour l'empêcher de tricher lors d'un examen effectué à distance.[3]

[1] L.R.O. 1990, chap. F.31
[2] Paragr. 2.
[3] Paragr. 6.

La deuxième application, Respondus Monitor, permet à la webcam de l'appareil de l'étudiant de l'enregistrer pendant qu'il rédige l'examen. Les enregistrements recueillent des renseignements biométriques et le logiciel utilise l'intelligence artificielle (IA) pour passer en revue les séquences vidéo qui pourraient indiquer que l'étudiant triche. Les moniteurs de cours reçoivent du logiciel un rapport sur toute activité jugée suspecte. Le logiciel ne décide pas s'il y a eu tricherie ou non et le moniteur de cours n'a pas d'accès immédiat aux enregistrements. Le moniteur de cours peut demander au bureau de l'intégrité académique de McMaster la permission de voir les enregistrements, conformément à la politique sur l'intégrité académique.

Dans le cadre de son analyse juridique, le CIPVP a déterminé que les renseignements personnels, tels que définis dans la *LAIPVP*, étaient en cause. Le CIPVP a jugé que McMaster recueillait, conservait et utilisait les renseignements personnels des étudiants grâce aux deux logiciels de Respondus. Les renseignements personnels incluaient les noms des étudiants, des photos, des vidéos les montrant, de l'information sur les cours et d'autres données biométriques.[4]

Le CIPVP a jugé que la loi donnait le droit à McMaster de recueillir les renseignements personnels. Selon l'article 38(2) de la *LAIPVP*, un organisme public doit être « autorisé expressément par une loi » à recueillir des renseignements personnels; par ailleurs, la collecte peut être considérée légale si elle est nécessaire à l'exécution de la loi ou pour le « bon exercice d'une activité autorisée par la loi ».

La *McMaster University Act*, 1976 n'autorise pas expressément McMaster à recueillir les types de renseignements personnels mentionnés ci-dessus. Toutefois, la collecte de ces renseignements personnels était nécessaire pour permettre à McMaster de mener une activité autorisée par la loi – faire passer des examens en tant qu'université.[5] Autrement dit, les renseignements personnels recueillis grâce au logiciel Respondus étaient nécessaires pour remplacer la surveillance en personne, qui sert à assurer l'intégrité académique. Le rapport du CIPVP énonce toutefois clairement qu'une université ne devrait pas présumer que la surveillance d'examens en ligne répondra toujours à la définition de « nécessaire ».[6]

Bien que la collecte de renseignements personnels ait été jugée conforme à la *LAIPVP*, l'avis donné aux étudiants et l'utilisation faite par Respondus ne l'étaient pas. Respondus a soutenu avoir utilisé des vidéos anonymes d'étudiants pour former son logiciel et son intelligence artificielle. Le CIPVP a jugé que les données n'avaient pas vraiment été rendues anonymes puisqu'il existait une représentation visuelle des étudiants.

Le but de l'avis prévu dans la *LAIPVP* est que les institutions publiques informent le public et soient transparentes quant aux renseignements personnels recueillis et utilisés.[7] Le CIPVP a conclu que l'avis de McMaster n'était pas assez clair pour satisfaire aux critères de la *LAIPVP*. Le document n'était pas complet et contenait différents liens. L'avis n'informait pas les étudiants que Respondus utiliserait leurs renseignements personnels pour améliorer ses produits.

[4] Paragr. 34.
[5] Paragr. 60.
[6] Paragr. 65.
[7] Paragr. 67.

Mais le plus troublant, c'est qu'il n'existait aucun moyen clair de se soustraire à l'utilisation par Respondus de données visant à améliorer le logiciel. Le développement de produit de Respondus n'était pas nécessaire à l'exercice par McMaster de l'activité autorisée par la loi, c'est-à-dire l'administration d'examens.[8]

Le CIPVP a jugé que la supervision humaine de tout comportement suspect signalé par Respondus Monitor était inappropriée.[9] Le CIPVP a approuvé la pratique visant à permettre uniquement aux moniteurs de cours de voir les vidéos en fonction de rapports d'activités suspectes. Il était important pour la CIPVP que le logiciel ne soit pas l'élément décisionnel pour l'examen de la conduite d'un étudiant. Il devait plutôt être un outil pour le moniteur de cours.

Le CIPVP a fait plusieurs recommandations à l'intention de McMaster, dont les suivantes :[10]

- McMaster devrait assurer, par écrit, que Respondus n'utilisera pas les renseignements personnels des étudiants à ses fins propres (amélioration de logiciels) sans le consentement de ces derniers. Si Respondus ne peut pas accepter cette condition, McMaster devrait cesser de recourir à ses services.
- McMaster devrait confirmer que Respondus traitera tous les enregistrements audios et vidéos comme des renseignements personnels.
- Le contrat entre McMaster et Respondus devrait exiger un avis si Respondus est tenu de divulguer son information au gouvernement ou aux autorités policières.
- Le contrat entre McMaster et Respondus devrait exiger – au minimum – la suppression annuelle de toutes les données personnelles conservées sur ses serveurs.
- Le personnel de la TI de McMaster devrait confirmer que la désinstallation du logiciel effacera toute trace de sa présence dans l'ordinateur.
- McMaster devrait modifier ses pratiques et politiques futures de manière à tenir compte des expériences de diverses communautés, à permettre aux étudiants de se soustraire à la surveillance d'examens en ligne, à fournir une procédure d'appel moins formelle pour les étudiants signalés par le logiciel et à contrôler de plus près la façon dont Respondus élabore, améliore et utilise ses logiciels.
- McMaster devrait créer des protections additionnelles pour les examens surveillés par IA.

Les recommandations du CIPVP ne sont contraignantes pour aucune personne ni organisation. Par conséquent, les questions en cause devront être mises à l'épreuve dans des litiges futurs ou comparées à tout changement futur à la *LAIPVP* (p. ex. des modifications apportées en réponse au recours à l'IA). Les lois sur la protection de la vie privée varient au pays. Celle de l'Ontario est l'une des moins contraignantes mais sa définition des commissaires est l'une des plus actives et influentes. D'autres provinces pourraient s'inspirer de ce rapport pour élaborer leurs propres approches à l'utilisation de logiciels de surveillance d'examens en ligne.

[8] Paragr. 81-84.
[9] Paragr. 150.
[10] Paragr. 166.