Logiciels de surveillance d'examens en ligne en temps de pandémie

À la recherche d'une minimisation des risques d'atteinte à la vie privée des étudiants

Céline Castets-Renard
Professeur, Faculté de droit civil, Université d'Ottawa
Titulaire de la chaire de recherche
Intelligence artificielle responsable à l'échelle mondiale

Avec la contribution de
Simon Robichaud-Durand
Étudiant à la Maîtrise Droit et Technologie
Université d'Ottawa
Membre de la chaire de recherche
Intelligence artificielle responsable à l'échelle mondiale

Étude financée par le Commissariat à la protection de la vie privée du Canada

Remerciements

Les auteurs remercient sincèrement le Commissariat à la protection de la vie privée du Canada pour la confiance et les moyens accordés pour la réalisation de cette étude.

Ils remercient également la Faculté de droit civil de l'Université d'Ottawa, spécialement le bureau de la recherche pour son soutien dans l'élaboration du projet de recherche, ainsi que la vice-doyenne à la recherche, la professeure Jennifer Quaid, pour l'organisation en ligne d'une table ronde d'experts qui s'est tenue le 16 mars 2022. Outre les deux contributeurs du présent rapport, cette table ronde était composée de la professeure Teresa Scassa de la Faculté de Commun Law de l'Université d'Ottawa et du professeur Sébastien Gambs de l'UQAM. Qu'ils soient ici à nouveau remerciés pour leurs profondes contributions à cette discussion. La table ronde peut être retrouvée sur le site de la chaire de recherche *IA responsable à l'échelle mondiale*[1].

La professeure Céline Castets-Renard tient à remercier chaleureusement Simon Robichaud-Durand pour son excellent travail de recherche et ses pertinentes suggestions et contributions.

Elle remercie également Olga Abimana, étudiante en droit et Développement international et mondialisation (L.LL & B.Sc.Soc. & J.D.) à la Faculté de droit civil de l'Université d'Ottawa, assistante de recherche au sein de la chaire *Intelligence artificielle responsable à l'échelle mondiale*, qui a contribué efficacement aux recherches préliminaires.

Note des auteurs

Cette étude académique a été réalisée dans le cadre du « Programme des contributions » du Commissariat à la protection de la vie privée du Canada.

Elle a été rédigée en toute indépendance et ne reflète pas l'opinion du Commissariat à la protection de la vie privée du Canada.

Les auteurs ont utilisé exclusivement le masculin pluriel dans le rapport pour désigner à la fois les hommes et les femmes. L'utilisation du genre masculin a été adoptée afin de faciliter la lecture et n'a aucune intention discriminatoire.

[1] En ligne : <https://chaireia.openum.ca/2022/03/16/table-ronde-sur-quels-enjeux-juridiques-des-logiciels-de-surveillance-dexamen-etude-realisee-pour-le-commissariat-a-la-protection-de-la-vie-privee-du-canada/>.

SOMMAIRE

SOMMAIRE EXECUTIF

Résumé

En période de pandémie de covid-19, de nombreuses universités ont eu recours à des outils de surveillance d'examens pour compenser l'impossibilité d'organiser des examens en présentiel.

S'il existe plusieurs procédés de surveillance et entreprises opérant dans le secteur, la plupart des outils mettent en œuvre des techniques d'intelligence artificielle comme la fouille des données et la reconnaissance faciale pour détecter des comportements suspects, susceptibles de constituer de la tricherie.

Ces entreprises utilisent les renseignements personnels recueillis dans le cadre de la mission de surveillance des examens organisés par les universités. Elles les utilisent aussi pour des usages secondaires consistant à améliorer les outils d'intelligence artificielle. Pour ce faire, elles obtiennent le consentement des étudiants mais les conditions de recueil ne sont pas favorables à l'expression d'un consentement libre, éclairé et distinct. En outre, la séparation entre les lois de protection des renseignements personnels du secteur public et du secteur privé rend difficile la qualification de ces entreprises sous-traitantes. La mise en œuvre de leur responsabilité éventuelle à titre principal, sur le fondement de loi de protection des renseignements personnels et des documents électroniques (LPRPDE), se conçoit difficilement dans un contexte de mise en œuvre des lois provinciales du secteur public.

Par ailleurs, le contrôle exercé sur les conditions de collecte et conservation des données est rendu délicat par le fait que de nombreuses entreprises technologiques sont américaines et imposent l'application du droit américain, voire le transfert des données sur le territoire américain.

Recommandations

Pour tenter de remédier à ces difficultés, cinq recommandations sont faites :

Recommandation 1 : renforcer les conditions de consentement dans la LPRPDE

Recommandation 2 : revoir l'articulation des lois du secteur public / privé et la qualification des responsables

Recommandation 3 : encadrer les flux internationaux de renseignements personnels hors Canada

Recommandation 4 : créer un effet extraterritorial de la LPRPDE

Recommandation 5 : exiger une étude des facteurs sur la vie privée (PIA) pour évaluer les systèmes d'IA impliquant des renseignements personnels

1. INTRODUCTION

Le sujet de l'utilisation de logiciels de surveillance d'examens pose plus largement la question du recours à la technologie en éducation (1). Si la technologie répond à différents objectifs et n'est pas nouvelle en soi, force est de constater que la pandémie a fortement encouragé les universités à se doter de solutions de surveillance automatique, alors que les cours et examens devaient principalement se dérouler hors campus (2). Il est d'ailleurs peu probable qu'un retour à la normale, espéré par la plupart des universités pour septembre 2022, implique un abandon de ces dispositifs ayant montré leur utilité. Cependant, bien que ces outils puissent permettre de réaliser des économies en temps de déplacement et en argent, ils suscitent des enjeux sociaux et éthiques (3) mais aussi juridiques (4). Ces réserves invitent à faire preuve de prudence dans l'usage de technologies dans un contexte d'éducation, en particulier au stade de l'évaluation des connaissances.

1.1. Recours à la technologie en éducation

Les objectifs à atteindre par l'usage des technologies en éducation sont variés[2]. Il peut s'agir notamment : de trier et sélectionner les candidats à l'entrée dans les universités ou grandes écoles[3] ; de mettre à disposition des ressources en ligne sur un campus virtuel[4] ; de mesurer le rendement et la performance académique[5] ; de déterminer un score de résultat final[6] ; de surveiller les examens. Ce dernier usage nous intéresse particulièrement ici. Les outils de vidéoconférence comme Zoom ont aussi été fortement utilisés pendant les périodes de confinement strict[7], ce qui n'est pas allé sans atteinte à la vie privée et à la cybersécurité[8].

---

[2] Hannah Natanson, « Live vs. Tape-Delayed: How Two Approaches to Online Learning Change Life for teachers and Students » *Washington Post* (28 avril 2020) en ligne : <https://www.washingtonpost.com/local/education/live-vs-tape-delayed-how-two-approaches-to-online-learning-change-life-for-teachers-and-students/2020/04/25/250fb7d0-7bfe-11ea-9bee-c5bf9d2e3288_story.html>.

[3] Exemple en France de l'algorithme de tri ParcourSup pour accéder aux établissements d'enseignement supérieur, en ligne : <https://www.parcoursup.fr/>.

[4] Comme BrightSpace par exemple qui collecte des renseignements personnels et des informations sur l'activité des utilisateurs.

[5] Des systèmes d'IA prédictif ont été déployés afin de prédire le rendement académique des évaluations annulés voir Simon Coghlan, Tim Miller et Jeannie Paterson, Good Proctor or "Big Brother"? AI Ethics and Online Exam Supervision Technologies, (2020) à la p 3, en ligne : <http://arxiv.org/abs/2011.07647v1>.

[6] Voir au Royaume-Uni, le scandale généré par l'utilisation pendant la pandémie de l'outil A-levels de prédiction des scores, en ligne : <https://www.djib-xinwen.com/2020/08/le-royaume-uni-recule-dans-la-debacle-des-tests-de-niveau-a-liee-au-coronavirus/>.

[7] Elly A. Hogan & Viji Sathy, « 8 Ways to Be More Inclusive in Your Zoom Teaching » (8 avril 2020), en ligne: *Chronicle* <https://www.chronicle.com/article/8-Ways-to-Be-More-Inclusive-in/248460>.

[8] Anny Hakim & Natasha Singer, New York Attorney General Looks Into Zoom's Privacy Practices, *The New York Times* (30 mars 2020), en ligne : <https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html>; Lauren Feiner, « Zoom Strikes a Deal with NY AG Office, Closing the Inquiry Into Its Security Problems » *CNBC* (May 7, 2020), en ligne : <https://www.cnbc.com/2020/05/07/zoom-strikes-a-deal-with-ny-ag-office-closing-security-inquiry.html>; Valerie Strauss, « School Districts, Including New York City's, Start Banning Zoom Because of Online Security Issues » *Washington Post* (4 avril 2020) en ligne :<https://www.washingtonpost.com/education/2020/04/04/school-districts-including-new-york-citys-start-banning-zoom-because-online-security-issues>.

Les logiciels de surveillance d'examen à distance ne sont pas nouveaux. Ils sont en effet mobilisés au Canada dans le secteur de l'éducation à distance[9] depuis les vingt dernières années[10]. Queen's University a par exemple indiqué au début de la pandémie en 2020 utiliser ces procédés depuis plusieurs années[11]. La surveillance en éducation est devenue un nouveau terrain de la "surveillance capitalistique"[12]. En effet, avant la pandémie, le secteur des technologies pour l'éducation (« *Ed-Tech* ») était déjà en plein essor. À la fin de l'année 2019, la part estimée du marché de ces services était évaluée à 19 milliards USD[13]. Mais plus encore, en 2020, le secteur plus large d'apprentissage en ligne surpassait une valeur de 100 milliards USD[14]. Il est en outre estimé qu'entre 2020 et 2027, le marché des logiciels de surveillance va croître de 16,4% annuellement[15]. Ailleurs, il est estimé que d'ici 2027, seul le marché des logiciels de surveillance représentera une valeur de 10 milliards[16]. Certains auteurs notent un accroissement d'utilisation de 720% depuis la pandémie[17]. À n'en pas douter, un marché rentable de la surveillance se déploie désormais.

Historiquement, les logiciels de surveillance n'ont pas toujours mobilisé l'intelligence artificielle (IA). Durant les années 2010, les logiciels de surveillance d'examen étaient ancrés dans une méthode qui comportait une intervention humaine, notamment des superviseurs d'examen, qui assuraient l'identité de l'étudiant et surveillaient le déroulement de l'examen en temps réel. Cependant, cette tendance a changé vers la fin des années 2010, lorsque ces logiciels ont adopté des systèmes d'IA utilisant des marqueurs biométriques pour réaliser une surveillance d'examens à distance, tels que des dispositifs de reconnaissance faciale en combinaison avec les photos d'identification des étudiants[18]. Peu après, des techniques automatisées ont été adoptés par les logiciels de surveillance, telle que la biométrie de frappe (« biometirc keystroke analysis »), le suivi des mouvements

---

[9] Barbara Fedders, The Constant and Expanding Classroom: Surveillance in K-12 Public Schools, 97 N.C. L. Rev. 1673 (2019).

[10] Neil Selwyn, Chris O'Neill, Gavin Smith, Mark Andrejevic et Xin Gu, « A necessary evil? The rise of online exam proctoring in Australian universities » 2021, 1-16, à la pp 1-2 en ligne : <https://journals.sagepub.com/doi/pdf/10.1177/1329878X211005862>.

[11] Queen's University, « Exams Services: Remote Proctoring » (s.d.) en ligne : *Queen's University* <https://www.queensu.ca/registrar/students/examinations/exams-office-services/remote-proctoring>.

[12] Shoshana Zuboff, The age of surveillance capitalisme: the fight for a human future at the new frontier of power, Profile Book Ltd (2019).

[13] Neil Selwyn et al, *supra* note 9 à la p 2.

[14] Ludwig Slusky, Cybersecurity of Online Proctoring Systems, Journal of International Technology and Information Management, 2020, 29-1, 56-86, à la p 57, en ligne : <https://www.semanticscholar.org/paper/Cybersecurity-of-Online-Proctoring-Systems-Slusky/80a084a512745c8b05c85a0870733d5cc435971c>.

[15] Neil Selwyn et al, *supra* note 9, à la p 4.

[16] Daniel Woldeab & Thomas Brothen, Video Surveillance of Online Exam Proctoring: Exam Anxiety and Student Performance, 2021, International Journal of E-Learning & Distance Education, 36-1, 1–26 à la p 2, en ligne: <https://www.proquest.com/docview/2572618998?parentSessionId=zl%2BfEpWBBJvqZTbySIdGxUyimOQu0URzQYQ9uoPGi%2FY%3D&pq-origsite=primo&accountid=14701>.

[17] David G Balash, Dongkun Kim, Darika Shaibekova, Rahel A Fainchtein, Micah Sherr, and Adam J Aviv, 2020 à la p 1, en ligne : <https://arxiv.org/ftp/arxiv/papers/2106/2106.05917.pdf>.

[18] Neil Selwyn et al, *supra* note 9 à la p 2.

des yeux (« eye tracking »), la surveillance auditive (« audio monitoring ») et la détection faciale cherchant des indices de tricheries ou d'utilisation de matériel non autorisée[19].

Ces usages sont plus ou moins discutables et causent plus ou moins de problèmes éthiques voire juridiques, spécialement d'atteinte à la vie privée[20]. Il faut, quoi qu'il en soit, noter que la plupart des outils sont proposés par des acteurs privés, en dehors de toute mission de service public d'éducation. Les entreprises dominantes sont en particulier les entreprises technologiques américaines connues comme Microsoft et Google. Leur mise en œuvre conduit aussi à la collecte de nombreuses informations sur les étudiants voire sur les écoliers lorsque ces outils sont utilisés dès l'école élémentaire comme Google ClassRoom par exemple. Les informations collectées sont non seulement des renseignements personnels permettant d'identifier les élèves mais sont aussi des indicateurs de nature à connaître leurs résultats et inférer des performances pouvant donner lieu à des profilages discriminants.

1.2. Contexte de la pandémie et surveillance technologique

Alors que la pandémie de la COVID-19 sévit depuis mars 2020 et a contraint une bonne partie de la population mondiale à télé-travailler, le milieu académique n'a pas non plus été épargné. Du jour au lendemain, les universités, notamment au Canada, ont cherché à compenser la présence physique par des solutions technologiques[21]. Une grande partie des cours et examens se sont passés en ligne, spécialement pendant les périodes de confinement strict, et le demeurent encore aujourd'hui, au moins en partie, pour certaines Universités ou Facultés.

Les examens ont dû rapidement s'organiser en ligne. Malgré la pandémie, les universités souhaitent maintenir un niveau de qualité et d'intégrité des diplômes. Mais dans un contexte distancié, la tâche est rendue particulièrement difficile. Selon certaines études, les étudiants sont plus portés à tricher lors d'un examen en ligne que s'ils assistent à un examen en personne[22]. La tricherie universitaire serait donc plus répandue lors des évaluations à distance comparativement aux évaluations en présentiel[23], ce qui a été constaté dans le monde entier[24]. Les principales fautes académiques relevées sont : le plagiat, la falsification d'informations, la soumission de travaux réalisés par quelqu'un d'autre ou encore la collaboration et le partage non autorisés de questions ou de réponses aux tests. Certes, la

[19] Neil Selwyn et al, *supra* note 9 aux pp 2-3.
[20] Jane Bailey, Jacquelyn Burkell, Priscilla Regan, Valerie Steeves, « Children's privacy is at risk with rapid shifts to online schooling under coronavirus » (21 avril 2020) en ligne : *The Conversation* <https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787>.
[21] Kelly McCarthy, The Global Impact of Coronavirus on Education, *ABC News* (Mar. 6, 2020), en ligne : <https://abcnews.go.com/International/global-impact-coronavirus-education/story?id=69411738>.
[22] Simon Coghlan, Tim Miller & Jeannie Paterson, 2020, *supra* note 4 à la p 5.
[23] Ludwig Slusky, *supra* note 13 à la p 57.
[24] Sheena Rossiter, « Cheating becoming an unexpected COVID-19 side effect for universities » *CBC News Edmonton* (21 juin 2020), en ligne : <https://www.cbc.ca/news/canada/edmonton/cheating-becoming-an-unexpected-covid-19-side-effect-for-universities-1.5620442>.

tricherie n'est pas propre à l'environnement virtuel mais y est rendu plus facile et plus tentante, dans un contexte particulièrement stressant pour les étudiants[25].

Pour faire face à ces enjeux, la majorité des universités canadiennes a opté pour l'utilisation de logiciels de surveillance d'examen à distance. Il n'est pas surprenant que de nombreuses universités dans le monde aient choisi de recourir à ces logiciels, dès lors que certains écrits affirment que ces outils sont capables d'atténuer complètement les opportunités de tricherie lors des évaluations à distance[26].

Ces logiciels, aussi connus sous la terminologie anglophone de « *proctoring software* », tels par exemple Respondus Monitor, ProctorU, Proctorio, Examity, proposent différentes solutions pour maintenir une certaine unité dans le temps et dans l'espace face à l'impossibilité d'une surveillance présentielle. Ils tentent aussi d'identifier des comportements pouvant être indicatifs d'incidents de tricherie potentielle. C'est ainsi par exemple que le blocage de l'ordinateur empêche les étudiants d'utiliser le logiciel de navigation pendant l'examen. Il peut aussi leur être demandé d'activer la caméra pour qu'une surveillance « en temps réel » puisse se faire. La vidéo est même parfois associée à un système de reconnaissance faciale ou de surveillance automatique permettant de repérer des comportements anormaux. Les systèmes peuvent ainsi signaler la « disparition » du visage d'un étudiant ou la présence de deux personnes, au lieu d'une seule. Aujourd'hui, les dispositifs de surveillance d'examen à distance requièrent de moins en moins d'intervention humaine, notamment en raison de leur dépendance algorithmique servant tant à l'identification des étudiants qu'à la détection de tricherie académique[27]. Certains outils technologiques pour la surveillance d'examen en ligne mettent en œuvre des systèmes d'intelligence artificielle dans l'espoir d'augmenter l'efficacité et la précision[28].

La pandémie a été un accélérateur dans l'utilisation de ces solutions et probablement aussi un facteur de banalisation des systèmes automatiques de surveillance. Cependant, la décision de mobiliser des logiciels de surveillance d'examen à distance a fait beaucoup de mécontentements parmi les étudiants à l'échelle mondiale. On a ainsi vu en Australie, des manifestations d'étudiants pour s'opposer à l'usage de ces outils[29]. Les étudiants ont ainsi exprimé leurs craintes aux États-Unis[30] et au Canada où une pétition a par exemple circulé

---

[25] Giacomo Panico, « University cheating might be up — but don't just blame students » *CBC News Ottawa* (19 juillet 2020), en ligne : <https://www.cbc.ca/news/canada/ottawa/university-cheating-might-be-up-but-don-t-just-blame-students-1.5618272>.
[26] Timothy H Reisenwitz, Examining the Necessity of Proctoring Online Exams, 2020, Journal of Higher Education Theory & Practice, 20-1, 118, à la p 123, en ligne : <https://doi.org/10.33423/jhetp.v20i1.2782>.
[27] Neil Selwyn, et al, *supra* note 9 à la p.1-2.
[28] Simon Coghlan, Tim Miller et Jeannie Paterson, *supra* note 4 à la p 1.
[29] *Ibid*; Neil Selwyn et al., *supra* note 9 au p 1-2; Jake Evans, ANU to Use Facial Detection Software on Student Computers in Response to Coronavirus Remote Exams, *ABC* (Apr. 20, 2020), en ligne :<https://www.abc.net.au/news/2020-04-20/coronavirus-anu-to-use-ai-spying-software-on-student-computers/12164324>.
[30] Shawn Hubler, Keeping Online Testing Honest? Or an Orwellian Overreach?, New York Times (10 mai 2020), en ligne :<https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html>.

en juillet 2020 à l'université d'Ottawa[31]. Des inquiétudes se sont aussi exprimées au Manitoba[32]. À l'université de Colombie-Britannique, certaines initiatives ont été prisse pour s'opposer à l'utilisation des logiciels de surveillance par les universités, notamment des manifestations étudiantes et des lettres ouvertes par les corps étudiants. Un site web conçu pour signaler les universités américaines qui mobilisent des logiciels de surveillance a même été créé[33]. Les tensions se sont amplement apaisées depuis, eu égard aux efforts réalisés par la plupart des universités pour renforcer la protection des informations de leurs étudiants et tenir compte des craintes exprimés. Au fur et à mesure que la pandémie dure, l'urgence d'une solution, exprimée en mars 2020 alors que la fin du semestre d'hiver et de la période d'examen approchait, s'estompe avec le temps. Le recours aux logiciels de surveillance a ainsi pu être allégé et devenir parfois aujourd'hui un simple accommodement proposé aux étudiants qui ne pourraient se rendre sur le campus comme à Polytechnique Montréal. Thompson Rivers University[34] constate d'ailleurs que la majorité des étudiants ont apprécié le confort de passer l'examen à la maison. L'examen en ligne est devenu ainsi une option proposée aux étudiants qui seraient éloignés des centres d'examen pour passer un examen en personne. Ainsi, l'université de Toronto[35] prévoit que l'université offre les services de surveillance en ligne de Examity aux apprenants inscrits à des cours en ligne qui ne vivent pas à moins de 30 km d'un centre d'examen canadien établi. Cela inclut tous les apprenants internationaux. La surveillance en ligne permet d'effectuer l'évaluation de votre cours à partir d'un lieu hors campus. On voit ainsi que certaines solutions ponctuellement mises en place pendant la pandémie ont vocation à rester en place. Il est donc particulièrement nécessaire de les analyser et de rester vigilant sur le choix laissé ou non aux étudiants d'utiliser ces procédés.

La vigilance est d'autant plus nécessaire que d'aucuns soutiennent que l'intégration de ces logiciels durant la pandémie pourrait servir de *preuve de concept* pour les logiciels de surveillance[36]. Une chose est sûre, une technologie utilisée dans le contexte de la surveillance d'examen, telle la reconnaissance faciale, peut naturellement être utilisée dans d'autres domaines et pour des usages variés comme le contrôle aux frontières ou le maintien de l'ordre.

Si on comprend la bonne intention des universités et des enseignants, il n'en demeure pas moins que de nombreux risques sociaux, éthiques et juridiques sont susceptibles d'apparaître et justifient une analyse approfondie. Loin de vouloir jeter l'opprobre sur les universités, l'objectif de cette étude est d'analyser quelques outils mis en œuvre et de

---

[31] Giamoco Panico, U of O students wary of 'extreme' anti-cheating software, (2 juillet 2020) *CBC New Ottawa*, en ligne : <https://www.cbc.ca/news/canada/ottawa/exam-surveillance-software-university-ottawa-1.5633134>.

[32] Radio-Canada, L'utilisation d'un logiciel de télésurveillance pour les examens inquiète des étudiants, *Radio-Canada* (18 août 2020), en ligne: <https://ici.radio-canada.ca/nouvelle/1727368/universites-examens-surveillance-covid-19-winnipeg-vie-privee>.

[33] Voir https://www.baneproctoring.com

[34] Thompson Rivers University, « Final Exams » (s.d.) en ligne : *Thompson Rivers University* <https://www.tru.ca/distance/services/exams.html>.

[35] University of Toronto, « How does online proctorig work » (s.d.), en ligne : *University of Toronto* <https://help.learn.utoronto.ca/hc/en-us/articles/115004994514-How-does-online-proctoring-work->.

[36] Neil Selwyn et al, *supra* note 9 à la p 12.

mesurer leur impact sur la vie privée et la protection des données personnelles des étudiants, dans le but d'alerter et de faire des recommandations aux décideurs (universités et législateurs).

1.3. Quelques exemples d'outils

Plusieurs entreprises proposent leurs outils de surveillance d'examen, tel Respondus Monitor, Proctorio, ProctorU, ProctorExam, Examity, ProctorTrack, basés sur de l'intelligence artificielle, suivant des méthodes plus ou moins intrusives. Ces systèmes de surveillance sont le plus souvent intégrés au système de gestion de l'apprentissage (Online Learning Platform ou D2L), mis en œuvre par d'autres entreprises.

Ainsi par exemple, Respondus Monitor est utilisé par l'Université d'Ottawa[37], l'Université du Manitoba[38] ou encore l'Université de Ryerson[39]. Respondus Monitor prétend être la principale solution de surveillance à distance pour l'enseignement supérieur[40]. Le système de Ryerson est intégré au système de gestion de l'apprentissage (Online Learning Platform ou D2L), comme par exemple, le Campus Virtuel de Brightspace à l'Université d'Ottawa[41].

Proctorio a été mis en œuvre par l'Université Laval[42] et l'Université Concordia[43]. L'université Laval indique ainsi sur son site internet que « Proctorio a fait l'objet d'une première expérimentation à l'Université Laval à l'automne 2020. Ce logiciel de télésurveillance s'avère être un outil dissuasif. À la suite des constats effectués, nous poursuivons l'utilisation de cette solution à la session d'automne 2021 ».

ProctorU[44] a été mis en œuvre par plusieurs universités pour la surveillance d'examen, tel que l'Université de Toronto[45], l'Université de Waterloo[46], l'Université Athabasca

---

[37] Université d'Ottawa, « Respondus LockDown Browser for student » (s.d.), en ligne: *Université d'Ottawa* <https://www.uottawa.saea-tlss.ca/en/transition-to-remote-teaching/respondus-lockdown-browser-for-student >.

[38] University of Manitoba, « Respondus » (s.d.), en ligne : *University of Manitoba* <https://umanitoba.ca/centre-advancement-teaching-learning/technologies/respondus#respondus-lockdown-browser-and-respondus-monitor>.

[39] Ryerson University, « Respondus LockDown Browser and Monitor virtual proctoring (integration with Brightspace) » (s.d.), en ligne : *Ryerson University* <https://www.ryerson.ca/courses/instructors/tutorials/integrations/virtual-proctoring-with-respondus-monitor/ >.

[40] Respondus, Respondus Monitor, (s.d.), en ligne : <https://web.respondus.com/he/monitor/>.

[41] Université d'Ottawa, « Bienvenue au Campus Virtuel propulsé par Brightspace (D2L) » (s.d.), en ligne : *Université d'Ottawa* <https://uottawa.saea-tlss.ca/fr/campus-virtuel >.

[42] Université Laval, « Surveillance d'examen en télésurveillance avec Proctorio » (s.d.), en ligne : *Université Laval* <https://www.enseigner.ulaval.ca/ressources-pedagogiques/proctorio>.

[43] Université Concordia, « Proctorio » (s.d.) en ligne : *Université Concordia* <https://www.concordia.ca/ctl/digital-teaching/proctorio.html>.

[44] Meazure Learning, « Privacy Policy » (17 février 2022), en ligne : *Meazure Learning* <https://www.meazurelearning.com/privacy-policy>.

[45] University of Toronto, « ProctorU: Privacy and Security Information Notice for Students » (s.d.) en ligne : *University of Toronto* <https://teaching.utoronto.ca/ed-tech/online-learning/online-proctoring/proctoru-privacy/>.

[46] University of Waterloo « Online proctoring FAQs » (s.d.) en ligne : *University of Waterloo* <https://uwaterloo.ca/extended-learning/learn-online/write-exams/online-proctoring-faqs>.

(Alberta)[47], l'Université Thompson Rivers (Colombie-Britannique)[48] et l'Université Memorial (Terre-Neuve-et-Labrador) [49].

ProctorExam[50] est utilisé par Polytechnique Montréal pour accommoder les étudiants qui demanderaient à passer leurs examens en ligne[51]. ProctorExam est une société néerlandaise régie par le Règlement général sur la protection des données (« RGPD »). Polytechnique a conclu une entente en vertu de laquelle ProctorExam s'engage à respecter les règles du RGPD et à prendre les mesures raisonnables équivalentes à la *Loi du Québec sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels pour protéger vos renseignements personnels contre les accès et divulgations non autorisés*. Ces dispositions sont *a priori* plus protectrices que celles mises en œuvre par des entreprises américaines, ce qui ressort clairement de l'information donnée aux utilisateurs sur le site internet de cette entreprise et des limites imposées.

Examity[52], utilisé par l'université de Toronto[53], fournit un service de surveillance en direct par des surveillants *humains* hautement qualifiés. Un surveillant à distance observe la façon de passer l'examen à l'aide d'un logiciel spécialisé et des enregistrements sont effectués et conservés pendant une période limitée afin de garantir le maintien de l'intégrité académique. L'Université de Toronto a conclu un accord avec Examity® qui affirme protéger la confidentialité des enregistrements et d'autres informations personnelles.

ProctorTrack[54] est le logiciel choisi dans le programme e-campus Ontario financé par la province[55]. Des licences ont ainsi été mises à la disposition des établissements d'enseignement. Queen's University[56], Western University[57] ont par exemple utilisé cette solution. Ailleurs, en Saskatchewan, l'Université de Regina a également mis en œuvre

---

[47] Athabasca University, « Using ProctorU for online exams » (s.d.), en ligne : *Athabasca University* <https://www.athabascau.ca/support-services/exam-services-support/using-proctoru-for-online-exams.html>.
[48] Thompson Rivers University, « ProctorU » (s.d.), en ligne : *Thompson Rivers University* <https://www.tru.ca/distance/faq/faq-proctoru.html>.
[49] Memorial University, « Online Proctoring » (s.d.), en ligne : *Memorial University* <https://citl.mun.ca/TeachingSupport/TeachOnline/OnlineProctoring.php>.
[50] Proctor Exam, Legal & Privacy, (s.d.), en ligne :<https://proctorexam.com/privacy-and-data-security/>.
[51] Polytechnique Montréal, « Mention légale relative à la protection des renseignements personnels », (s.d.), en ligne : *Polytechnique Montréal* <https://share.polymtl.ca/alfresco/service/api/path/content;cm:content/workspace/SpacesStore/Company%20Home/Sites/etudes-web/documentLibrary/examens-finaux/Mention_legale_Proctor_Exam_Accommodement_Finaux.pdf?a=true&guest=true>.
[52] Examity, « Privacy & Security » (s.d.), en ligne : *Examity* < https://www.examity.com/features/privacy-and-security/>.
[53] University of Toronto, (s.d.), *supra* note 34.
[54] Proctortrack, « Politique de confidentialité » (15 juillet 2021).
En ligne : *Proctortrack* <https://www.proctortrack.com/privacy-policy/>.
[55] E-Campus Ontario, en ligne : <https://www.ecampusontario.ca/fr/proctortrack/>.
[56] Queens'University, en ligne : <http://www.queensu.ca/registrar/students/examinations/exams-office-services/remote-proctoring>.
[57] Western University, en ligne : <https://www.cbc.ca/news/canada/london/western-students-alerted-about-security-breach-at-exam-monitor-proctortrack-1.5764354>.

ProctorTrack[58]. Il faut cependant noter que ProctorTrack a dû interrompre ses services à la suite d'une faille de sécurité[59]. Dans ce contexte, il n'est pas clair de savoir si des renseignements personnels des étudiants ont pu fuiter mais ces derniers manifestent des inquiétudes fortes face à un tel risque[60].

Il ne s'agit là que de quelques exemples d'outils mais on voit que de nombreuses universités à travers toutes les provinces du Canada se sont tournées dans l'urgence vers ces solutions. Face à l'impossibilité et l'inutilité de faire une étude exhaustive de ces outils et de leur utilisation dans tous les établissements d'enseignement supérieur, nous proposons d'étudier trois outils (Respondus, Proctorio et ProctorU) en se basant sur quelques universités les utilisant.

1.4. Enjeux sociaux et éthiques

Les outils de surveillance d'examen ne sont pas neutres. Le site de l'Université du Manitoba indique ainsi que « l'utilisation de Respondus n'est pas obligatoire et s'accompagne de contraintes possibles telles que la limitation de la bande passante Internet des étudiants, l'incapacité à répondre aux exigences informatiques et le risque d'une anxiété accrue »[61]. Ces outils interrogent d'abord en effet sur leur impact concernant la santé mentale des étudiants. De nombreux témoignages de candidats font part de l'augmentation de l'anxiété liée aux examens[62] quand il s'agit de surcroît d'installer un outil de surveillance et devoir utiliser une (voire deux) caméra constamment allumée pendant toute la durée de l'examen[63]. Les étudiants ressentent ainsi un sentiment d'être sous surveillance constante[64]. Ils craignent en outre que certains de leurs mouvements ne soient indûment signalés comme suspects et ne conduisent ensuite à de fausses accusations de malhonnêteté académique[65]. Même parmi les auteurs qui recommandent l'adoption des logiciels de surveillance comme

---

[58] Regina University, en ligne : <https://www.cbc.ca/news/canada/saskatchewan/university-regina-proctortrack-security-breach-1.5765850>.

[59] Regina University, en ligne : <https://www.620ckrm.com/2020/10/19/u-of-r-test-monitoring-software-the-victim-of-a-security-breach/>. Western University, en ligne : <https://ici.radio-canada.ca/nouvelle/1741804/informatique-pirate-fuite-vie-privee?fromApp=appInfoIos&partageApp=appInfoiOS&accesVia=partage>. E-campus Ontario, en ligne : <https://www.ecampusontario.ca/fr/13855/>.

[60] Regina University, en ligne : <https://www.cbc.ca/news/canada/saskatchewan/university-regina-proctortrack-security-breach-1.5765850>.

[61] University of Manitoba, *supra* note 37.

[62] Monica Chin, « Exam Anxiety: How Remote Test-Proctoring Is Creeping Students Out » (29 avril 2020), en ligne : *Verge* <https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education>.

[63] Jessica Wong, « Post-secondary students call for changes to online exam rules as cheating concerns rise » *CBC News* (25 octobre 2020), en ligne :<https://www.cbc.ca/news/canada/post-secondary-assessment-integrity-proctoring-1.5767953>.

[64] À cet égard, selon certains auteurs, les étudiants éprouvent un sentiment de « big brother is watching » lors des examens à distance qui mobilisent des logiciels de surveillance. Voir Simon Coghlan, Tim Miller et Jeannie Paterson, 2020, supra note 4 à la p 2.

[65] Jessica Wong, *supra* note 51.

solution à la tricherie académique lors des évaluations à distance, la problématique d'intensification de l'angoisse chez les étudiants est considérée[66].

Également, ces outils créent une rupture d'égalité et sont sources de discrimination. Peuvent ainsi apparaître différentes causes de discriminations liées à la race ou à l'ethnie, au handicap, aux facteurs socio-économiques, au territoire (conditions d'accès à internet). La rupture d'égalité entre les étudiants peut d'abord provenir de la couleur de peau. Il a été prouvé par plusieurs recherches que les outils de reconnaissance faciale reconnaissent mal les peaux sombres[67], ce qui est confirmé ici aussi s'agissant des logiciels de surveillance d'examen[68]. Les algorithmes utilisés sont souvent les mêmes d'une application à une autre et il n'est pas surprenant de constater des difficultés similaires dans différents cas d'usage.

Il faut ajouter que la situation de handicap de certains étudiants crée aussi des difficultés supplémentaires[69]. Des étudiants handicapés rapportent ainsi que le logiciel de lecture d'écran spécifique qu'ils utilisent habituellement peut s'avérer incompatible avec un logiciel de surveillance à distance[70]. Certains programmes d'accessibilité de lecteur d'écran, tels que JAWS, Windows-Eyes ou VoiceOver par exemple, sont rendus compatibles avec un outil comme Respondus mais pas nécessairement avec d'autres outils d'accessibilité. Si les étudiants rencontrent des difficultés à télécharger le logiciel ou s'ils ne peuvent pas accéder à un examen après avoir lancé le navigateur, ils sont la plupart du temps invités à obtenir de l'aide directement auprès des entreprises technologiques. La plupart ont un service de dialogue en direct 24 heures sur 24 et 7 jours sur 7 mais un tel scénario est certainement anxiogène pour les étudiants qui doivent faire face à ces difficultés au moment même de passer leur examen. Plus largement, se pose la question de la prise en compte des accommodements dont bénéficient les étudiants.

Par ailleurs, il est aussi souvent requis que les étudiants fassent leurs examens seuls dans une pièce isolée, alors qu'il n'est pas toujours aisé de réunir toutes ces conditions matérielles dans le lieu où se trouvent les étudiants pendant la pandémie, alors que beaucoup d'entre eux ont dû retourner chez leurs parents. L'inégalité résulte de facteurs

---

[66] Timothy Reisenwitz, supra note 25 à la p 123.

[67] Voir les travaux de Joy Buolamwini, chercheuse au MIT et fondatrice de l'Algorithmic Justice League : http://gendershades.org/overview.html. Joy Buolamwini, "Artificial Intelligence Has a Problem With Gender and Racial Bias: Here's How to Solve It", *Time* (7 Février 2019), en ligne: <https://time.com/5520558/artificial-intelligence-racial-gender-bias>; Drew Harwell, Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use, *The Washington Post* (19 Décembre 2019), en ligne :<https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use.>; R Benjamin, Race after Technology: Abolilitionist Tools for the New Jim Code, Polity, 2019.

[68] Anushka Patil et Jonah Engel Bromwich « How It Feels When Software Watches You Take Tests », *New York Times* (29 septembre 2020), en ligne :<https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html>.

[69] Johnathan Custodio, « Disabled Students Already Faced Learning Barriers. Then Coronavirus Forced an Abrupt Shift to Online Classes » (7 avril 2020), en ligne : *Chronicle* <https://www.chronicle.com/article/Disabled-Students-Already/248444>.

[70] Jessica Wong, *supra* note 51.

économiques et sociales mais aussi de disparités territoriales[71]. Les étudiants doivent avoir un accès[72] performant au réseau internet[73], s'équiper d'une webcaméra et d'un microphone fonctionnels qu'ils doivent activer sur l'ordinateur à tout moment pendant l'évaluation. Ce matériel doit être suffisamment récent pour être compatible avec les logiciels de surveillance. S'il est parfois précisé qu'il n'y a pas d'exigence spécifique de bande passante en matière de kb/s pour l'utilisation d'une webcam, la qualité d'enregistrement pouvant s'ajuster automatiquement lorsqu'une connexion plus lente est détectée, l'étudiant qui utilise une connexion Internet partagée est toutefois invité à s'assurer que les autres personnes sur la même connexion n'utilisent pas de services exigeants en bande passante pendant l'examen (tels que les films en ligne, les jeux, le partage de fichiers, etc.). Beaucoup d'étudiants vivent en collocation en temps normal ou encore sont retournés chez leurs parents parfois loin des centres urbains en période de pandémie et il convient de prendre en compte le fait que la qualité de la connexion peut être un enjeu de taille, de nature à renforcer les disparités économiques et sociales. En outre, faire peser la responsabilité de la performance d'un équipement sur l'étudiant pour le bon fonctionnement de l'outil de surveillance d'examen pose la question de l'asymétrie de pouvoir et de l'injustice à exiger de l'étudiant qu'il réunisse lui-même les conditions pour passer correctement l'examen.

Bien que l'internet au Canada soit très accessible à travers les provinces, le gouvernement canadien relève que 6% des ménages canadiens sont toujours sans accès à l'internet pour diverses raisons, tel que le coût de l'abonnement internet ou encore le coût de l'équipement nécessaire[74]. En outre, concernant la rapidité de la connexion internet, seuls 45,6% des collectivités rurales ont accès à une connexion rapide d'au moins 50 Mbps de téléchargement et 10 Mbps de téléversement[75]. Conséquemment, il serait possible qu'un étudiant appartienne à la minorité d'inaccessibilité à internet ou à la minorité rurale de connexion internet inférieure. D'ailleurs, une publication gouvernementale récente a souligné que les personnes situées dans un milieu urbain sont plus portées à participer à des activités de formation ou d'apprentissage en ligne que ceux situés en milieu rural[76].

---

[71] Dana Goldstein, Adam Popescu et Nikole Hannah-Jones, « As School Moves Online, Many Students Stay Logged Out » *New York Time* (6 avril 2020), en ligne :<https://www.nytimes.com/2020/04/06/us/coronavirus-schools-attendance-absent.html>.

[72] Associated Press, « Million of Kids Are Struggling in School Because They Don't Have Internet Access at Home » (10 juin 2019), en ligne : *Market Watch* <https://www.marketwatch.com/story/nearly-3-million-students-in-the-us-struggle-to-keep-up-in-school-due-to-lack-of-home-internet-2019-06-10>.

[73] Deborah Brown, « Closing the 'Digital Divide' Critical in COVID-19 Response » (25 mars 2020), en ligne : *Human Rights Watch* <https://www.hrw.org/news/2020/03/25/closing-digital-divide-critical-covid-19-response>.

[74] Statistiques Canada, Gouvernement du Canada, Le Quotidien, le lundi 31 mai 2021, en ligne :<https://www150.statcan.gc.ca/n1/daily-quotidien/210531/dq210531d-fra.pdf>; Statistique Canada, Graphique 1 Proportion de Canadiens ayant accès à Internet à la maison, Canada et provinces, 2020, 5 mai 2021, en ligne :< https://www150.statcan.gc.ca/n1/daily-quotidien/210531/cg-d001-fra.htm>.

[75] Conseil de la radiodiffusion et des télécommunications canadiennes, Gouvernement du Canada, Fonds pour la large bande Combler le fossé numérique au Canada, 2021, en ligne : <https://crtc.gc.ca/fra/internet/internet.htm>.

[76] Statistique Canada, Gouvernement du Canada, accès à Internet au Canada, 2020, 5 mai 2021, en ligne: <https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00027-fra.htm>.

De plus, l'utilisation de logiciels de surveillance a pour effet d'interdire indirectement certains comportements étudiants qui seraient autrement permis tel que de marmonner à soi-même, de regarder dans tous les sens ou même d'aller à la salle de bain, puisque lors d'un examen avec un logiciel de surveillance, ces comportements peuvent être indicatifs d'un incident de tricherie[77].

Il faut enfin noter l'utilisation de solutions technologiques présentées comme universelles et utilisées partout dans le monde. Plusieurs des logiciels de surveillance ont ainsi été présentés comme une solution passe-partout (« *one size fits all* ») basée sur une formule algorithmique. Ce discours pose la question de l'adéquation de ces solutions aux contextes locaux. Les firmes de logiciels de surveillance d'examen offrent des recommandations quant à la configuration des logiciels, et conséquemment, les configurations recommandées ont souvent été suivies. Mais les logiciels n'ont pas été calibrés pour refléter les routines et les valeurs locales[78]. Cette solution généralisée omet de considérer certains facteurs, tels que les caractéristiques et les comportements culturels différents[79].

Ces sources de discrimination économique, sociale, raciale et de handicap sont particulièrement préoccupants et s'ajoutent aux difficultés générées dans le contexte de la pandémie. De nombreux étudiants n'ont pas réussi à s'adapter à un apprentissage en ligne, rendu bien plus difficile et solitaire[80]. Il est important de ne pas oublier que certains d'entre eux n'accèdent plus à l'éducation[81] et il sera certainement difficile, voire impossible, pour beaucoup d'entre eux de retourner étudier lors du retour en présentiel sur les campus.

1.5. Enjeux juridiques (vue générale)

L'utilisation des dispositifs de surveillance crée de nombreux défis pour les universités, en charge de préserver la santé physique et mentale des étudiants mais aussi de garantir la confidentialité de leurs renseignements personnels, tout en maintenant leur mission d'éducation et diplomation. Les risques sociaux et éthiques précités sont d'autant plus alarmant que l'on peut aussi s'interroger sur les enjeux juridiques, liés en particulier à l'invasion de la vie privée générée par ces outils[82].

Les craintes portent inévitablement sur la potentielle atteinte à la vie privée et à la protection des renseignements personnels. Outre le nombre considérable de données susceptibles d'être collectées par ces procédés, certains de ces outils impliquent la collecte

---

[77] Simon Coghlan, Tim Miller et Jeannie Paterson, *supra* note 4, à la p 8.
[78] Neil Selwyn et al, *supra* note 9 à la p13.
[79] À cet égard Daniel Woldeab and Thomas Brothen (2021) soutiennent que « [f]aculty should also be aware that when they are passing judgment on potential academic misconduct, this would typically be based on a one-size-fits-all algorithm-based proctoring software, which might not take into account culturally specific characteristics or behaviours » Daniel Woldeab & Thomas Brothen, *supra* note 15 aux pp 21-22.
[80] Shoshana Wodinsky, « Not Everyone Can Go to School Online » (7 avril 2020), en ligne : *Gizmodo* <https://gizmodo.com/not-everyone-can-go-to-school-online-1842726588>.
[81] Nicole Gaudiano, « Coronavirus Quarantines Could Rob Poor, Rural Students of Access to Education » (10 mars 2020), en ligne : *Politico* <https://www.politico.com/news/2020/03/10/coronavirus-quarantines-rural-students-125048>; Javier Tovar, Poor U.S. Students Miss Out As Virtual Learning Sharpens Divide, *Yahoo! News* (17 avril 2020), en ligne : <https://news.yahoo.com/poor-us-students-miss-virtual-learning-sharpens-divide-013742154.html>.
[82] Anushka Patil et Jonah Engel Bromwich, *supra* note 56.

de données biométriques sensibles, associées à un système d'intelligence artificielle pour vérifier la bonne correspondance des images des étudiants des bases de données avec les candidats postés devant la caméra. Des systèmes de reconnaissance faciale peuvent ainsi être mis en œuvre en vue de vérifier l'identité des étudiants. Le risque d'hyper-surveillance technologique des étudiants est réel.

En outre, alors que les prestataires sont pour la plupart situés aux États-Unis et que les données collectées lors des activités de surveillance y sont transférées, on peut se demander si les lois fédérales et provinciales de protection des renseignements personnels au Canada continuer de s'appliquer et si elles assurent une protection effective. Il existe un risque non négligeable d'une protection insuffisante des renseignements personnels auquel s'ajoute un risque de cybersécurité des réseaux et de conservation des données.

Enfin, si des obligations légales s'imposent aux universités pour protéger la vie privée et les renseignements personnels de leurs étudiants, il convient d'analyser aussi les obligations contractuelles imposées par les entreprises technologiques, tant dans leurs relations avec les universités qu'avec les étudiants. Le lien contractuel direct avec ses entreprises fait envisager la mise en œuvre des lois de protection des renseignements personnels du secteur privé.

1.6. Problématiques et méthodologie

Les risques ainsi soulevés fondent les principales questions de recherche posées par ce rapport, à savoir : quels sont le fonctionnement et les caractéristiques de ces systèmes ? Dans quelle mesure ces outils utilisent-ils des renseignements personnels et reposent-ils sur des techniques d'intelligence artificielle ? Comment bien identifier les risques et vérifier si des mesures protectrices sont prises par les entreprises qui créent et déploient ces solutions ? Les entreprises américaines fournissant la plupart des solutions sont-elles effectivement responsables du respect des législations canadiennes sur les données personnelles ? En cas d'insuffisance de protection des renseignements personnels, quels conseils peut-on donner aux universités et aux législateurs pour la renforcer y compris au-delà du territoire canadien ?

Pour répondre à ces questions, la méthodologie suivie a été à la fois empirique et théorique.

La *recherche empirique* a consisté à identifier les principaux outils de surveillance utilisés par les universités canadiennes, en se fondant sur la recherche documentaire en ligne à partir des sites des médias et des universités. Les documents contractuels analysés regroupent les "terms of use" et "Privacy Policy", tels que publiés sur les sites commerciaux des entreprises, ainsi que les informations diffusées sur les sites des universités (sources ouvertes). Par exemple, les termes et conditions contractuelles[83], ainsi que les politiques de vie privée[84] du système Respondus, sont disponibles en ligne sur le site internet. Des contrats plus spécifiques de fourniture de services peuvent cependant être

[83] Respondus, « Terms of Use – Respondus Monitor (Student) » en ligne : *Respondus* <https://web.respondus.com/tou-monitor-student/>.
[84] Respondus, « Respondus Privacy Policy » (25 mai 2021), en ligne : *Respondus* <https://web.respondus.com/privacy-policy/>.

conclus entre les universités et les entreprises mais restent confidentiels. Il est donc impossible de savoir dans quelle mesure les risques pour la protection de la vie privée et la sécurité des renseignements personnels ont effectivement pu être pris en compte. L'objectif est alors précisément de les identifier et d'inciter les universités à renforcer la protection au cours de négociations, ce en quoi nos analyses peuvent les aider.

Afin de compléter l'étude de ces outils en particulier, il a ensuite été procédé à *l'analyse théorique* des documents contractuels, incluant les conditions générales d'utilisation et les politiques de confidentialité, mises à l'épreuve du droit canadien et spécialement des lois de protection des renseignements personnels. Bien que ces outils soient largement déployés depuis longtemps aux États-Unis, le choix a été fait de se concentrer sur le Canada. Le champ de l'étude s'intéresse aux différentes provinces et il est ainsi constaté que des universités situées dans toutes les provinces à travers le Canada sont concernées, bien que les universités québécoises se soient montrées au début plus frileuses[85]. Les lois provinciales de protection des renseignements personnels vont avoir vocation à être mises en œuvre mais une place sera aussi réservée aux lois fédérales, plus spécialement à la loi sur la protection des renseignements personnels et les documents électroniques dite LPRPDE (ou PIPEDA).

1.7. Annonce du plan

La partie II présente les outils de surveillance d'examens utilisés par les universités canadiennes. Sur le fondement d'une analyse empirique des sources disponibles en libre accès, ont été retenus trois outils de surveillance d'examens utilisés par les universités canadiennes. Il s'agit d'identifier les caractéristiques techniques de chacun d'entre eux. L'objectif est de comprendre leur fonctionnement et de rechercher les risques effectifs pour la protection de la vie privée et des renseignements personnels.

Dans la partie III, cette approche empirique est ensuite complétée par une analyse des risques juridiques que les outils de surveillance d'examens font courir du point de vue de la protection des renseignements personnels et de la vie privée. Cette analyse théorique repose sur l'étude des lois fédérales et provinciales concernant la protection des renseignements personnels, ainsi que sur l'analyse des contrats et politiques de confidentialité, rendus publics par les entreprises technologiques. Outre les risques pour la vie privée, l'objectif est également de vérifier le recours ou non à des systèmes d'intelligence artificielle. Est recherché leur impact du point de vue de la vie privée mais aussi du point de vue de la redevabilité des entreprises impliquées. Cette étude juridique théorique s'appuie sur les points faibles révélés par l'étude empirique dans la partie II et se concentre sur les relations contractuelles entre les universités et les entreprises fournisseuses. Est aussi considérée la compatibilité entre l'utilisation de ces outils de surveillance et les politiques de confidentialité des universités envers les étudiants, de façon à appréhender largement les engagements en matière de protection des données dans cette relation tripartite (étudiants, universités et entreprises).

[85] Marco Fortier, « Des examens universitaires sous télésurveillance », *Le Devoir* (13 octobre 2020), en ligne : <https://www.ledevoir.com/societe/education/587717/education-examens-sous-surveillance>.

La partie IV permet de déduire les problèmes majeurs qui ne sont pas encore suffisamment considérés par la loi, en particulier la loi fédérale sur le secteur privé (LPRPDE). Si les universités tentent du mieux possible de protéger les intérêts des étudiants en respectant leur règlement de confidentialité et les législations de protection des renseignements personnels, il est possible que le niveau de protection exigé par ces dernières soit insuffisant pour protéger les personnes concernées, en particulier dans le cas d'un flux transfrontalier des données en dehors du Canada. Alors que les compagnies technologiques américaines proposent activement leurs solutions aux acteurs canadiens, tant publics que privés, la question de la protection des renseignements personnels dans un tel contexte transnational est particulièrement cruciale. Si on veut apporter des garanties réelles et effectives aux personnes qui confient leurs données personnelles aux entités publiques et privés canadiennes, il convient de se préoccuper du sort de ses données et de poser la question d'une responsabilité des entreprises proposant de telles solutions technologiques.

En partie V, nous ferons des recommandations à l'adresse des universités et du législateur pour tenter de prendre en considération les problèmes majeurs restés encore sans réponse à ce jour.

2. ANALYSE EMPIRIQUE : QUELQUES OUTILS DE SURVEILLANCE D'EXAMENS UTILISÉS PAR LES UNIVERSITÉS AU CANADA

Les fonctions des logiciels de surveillance d'examen varient grandement : certains d'entre eux ont seulement pour effet de verrouiller le navigateur internet des étudiants, alors que d'autres dispositifs enregistrent les étudiants par vidéo et analysent les enregistrements par le biais de dispositifs d'intelligence artificielle. De manière générale, il existe trois types de logiciels de surveillance d'examens.

Premièrement, les logiciels en temps réel (« *live proctoring* ») sont dotés d'une surveillance humaine. Une personne est chargée de faire la surveillance d'examen en temps réel, afin d'assurer l'authentification des étudiants et d'identifier d'éventuels indices de tricherie[86]. Ainsi, par exemple, Respondus Instructor Live Proctoring a été créé pour permettre aux formateurs de surveiller à distance l'exécution synchrone d'un examen sécurisé via des systèmes de visioconférence, tels que ZOOM ou Microsoft Teams. Respondus Instructor Live Proctoring permet aux étudiants de faire leur examen à l'aide de Respondus LockDown Browser qui bloque le navigateur, tout en étant surveillés en temps réel par leur enseignant via des outils de visioconférence. Ces dispositifs ne causent pas de problème particulier, dès lors que la surveillance a proprement parlé est humaine et réalisée par les enseignants. En particulier, le système n'alerte pas l'instructeur en cas d'événements suspects et les vidéos des étudiants ne sont pas enregistrées. Ces dispositifs ne retiendront donc pas davantage notre attention.

Deuxièmement, les logiciels d'enregistrement (« *recorded proctoring* ») sont des logiciels qui enregistrent les étudiants en captant des vidéos ou des enregistrements audios, afin d'être vérifiés entièrement par une personne chargée de déterminer s'il y a réellement un incident de tricherie[87]. Ces logiciels d'enregistrement requièrent donc une intervention humaine pour l'entièreté de la durée de l'enregistrement et, conséquemment, entrainent des coûts et du temps additionnel suivant la teneur de l'examen. Cependant, l'enregistrement en tant que tel n'est pas utile, s'il ne s'accompagne pas de moyens automatisés d'aider l'enseignant en lui signalant des vidéos présentant des comportements suspects. La trop grande quantité d'enregistrements produits par étudiant exclut que l'enseignant puisse les consulter et mettre effectivement en œuvre ce procédé. Ces moyens ne seront donc pas non plus considérés ici.

Troisièmement, les logiciels automatisés (« *automated proctoring* ») sont des logiciels qui peuvent aller jusqu'à réduire au minimum l'intervention humaine, tant pour la surveillance que pour la révision des examens. Ainsi, les logiciels automatisés vont notifier aux responsables de l'enseignement, lorsque le logiciel a identifié des incidents potentiels de tricherie ou des comportements jugés anormaux, afin qu'un contrôle humain soit effectué

[86] Hussein, Mohammed Juned et al., An Evaluation of Online Proctoring Tools, Open Praxis, vol. 12-4, International Council for Open and Distance Education (ICDE), 2020, pp. 509–25, à la p 510, en ligne : <https://files.eric.ed.gov/fulltext/EJ1285031.pdf>.
[87] *Ibid*.

pour déterminer s'il y a eu réellement de la tricherie[88]. Ces logiciels de surveillance ont pour principaux objectifs d'authentifier l'étudiant, de limiter les capacités de l'ordinateur, d'analyser les comportements des étudiants et de générer un rapport[89]. Seuls ces outils seront analysés dans cette étude. Parmi les logiciels automatisés, on note que certains d'entre eux sont totalement automatisés, alors que d'autres sont hybrides et combinent une surveillance humaine et des fonctionnalités automatisées intégrant de l'intelligence artificielle[90].

Les logiciels automatisés mobilisant l'intelligence artificielle suscitent un questionnement plus profond quant à la protection de la vie privée et des renseignements personnels des étudiants. Parmi eux, nous étudierons plus spécifiquement : (1) Respondus utilisé à l'université d'Ottawa, (2) Proctor U à l'Université de Toronto et (3) Proctorio à l'Université Laval et l'Université de Colombie-Britannique (UBC).

2.1. Respondus : Université d'Ottawa

Le premier outil externe que nous exposerons est Respondus. Respondus, Inc. est une entreprise américaine établie à Redmond dans l'état de Washington. La société fournit des webinaires d'apprentissages[91], des vidéos sur l'utilisation du logiciel[92] et un guide de démarrage rapide[93] à la destination des étudiants. Cet outil est utilisé par exemple par l'université du Manitoba[94] et l'Université d'Ottawa[95], laquelle a communiqué sur son site internet les conditions d'utilisation de l'outil. Deux types de paramétrages sont disponibles : LockDown Browser et Respondus Monitor.

LockDown Browser est un navigateur personnalisé qui verrouille l'environnement d'examen dans Brightspace (Campus Virtuel) sur lequel l'examen se déroule. Lorsque le navigateur est activé pendant un examen, les étudiants ne peuvent pas imprimer, copier, aller sur une autre adresse URL, accéder à d'autres applications ou fermer un examen avant qu'il ne soit soumis à la notation. Les examens créés pour être utilisés avec LockDown Browser ne sont pas non plus accessibles avec les navigateurs standards. Si les professeurs le souhaitent, ils peuvent permettre aux étudiants d'accéder à des sites web spécifiques pendant un examen. Il est affirmé qu'aucune donnée n'est accessible par Respondus qui

---

[88] *Ibid*.
[89] *Ibid*.
[90] *« Online proctoring systems can be grouped into three classes: discretional live- proctor systems, automated (AI-enabled) systems, and hybrid (automated with a live proctor) systems.* » Ludwig, *supra* note 13 à la p 71.
[91] Respondus, « Webinars » (s.d.) en ligne : *Respondus* <https://web.respondus.com/webinars/>.
[92] Respondus, « Preparing an Exam for Use with Respondus Monitor and LockDown Browser » (10 avril 2019), en ligne : *Youtube* <https://www.youtube.com/watch?v=7J1K8-R20ao>.
[93] Respondus, « LockDown Browser: Prevent cheating during online exams » (s.d.) en ligne : *Respondus* <https://web.respondus.com/he/lockdownbrowser/resources/>.
[94] University of Manitoba, Respondus, Respondus provides assessment tools to create, manage and monitor online exams in UM Learn, (s.d.) en ligne : *University of Manitoba* <https://umanitoba.ca/centre-advancement-teaching-learning/technologies/respondus>.
[95] Université d'Ottawa, « Logiciel de surveillance d'examens » (s.d.) en ligne : *Université d'Ottawa* <https://uottawa.saea-tlss.ca/fr/transition-vers-l-enseignement-a-distance/logiciel-de-surveillance-d-examens>.

n'a aucun accès ou contrôle sur la collecte de données sur les couches réseaux des appareils externes**.** Il empêche simplement l'étudiant de quitter l'environnement du navigateur Respondus LockDown et l'oblige à fermer les applications liées à la capture d'écran, à la messagerie, au partage d'écran, etc., jusqu'à ce que l'examen soit soumis. Seuls les logiciels d'accessibilité, tels que JAWS et VoiceOver, sont autorisés à fonctionner en parallèle avec le Respondus LockDown Browser. Respondus LockDown Browser ne nécessite cependant pas d'autorisation d'accès au noyau/racine pour fonctionner et n'effectue aucune action sur l'appareil de l'utilisateur sans son consentement. Au démarrage, LockDown Browser extrait les processus ouverts du "Task Manager" de l'appareil et demande à l'utilisateur de fermer ceux qui concernent les plateformes de communication telles que : SkypeBackgroundHost.exe, SkypeApp.exe, Recorder.exe, TeamViewer_Service.exe, SSInvitationAgent.exe. L'utilisateur peut choisir soit de fermer le processus et de procéder au lancement du navigateur LockDown Browser, soit de quitter simplement la plate-forme. Respondus n'a aucun contrôle ni pouvoir pour forcer cette étape et n'a donc pas d'accès au noyau sur l'appareil.

Respondus Monitor est une solution de surveillance entièrement automatisée. Les étudiants utilisent une webcam pour s'enregistrer pendant un examen en ligne. Par la suite, les événements marqués et les résultats de la surveillance sont accessibles à l'instructeur pour un examen plus approfondi[96]. Lorsque cette fonction est activée, les étudiants sont tenus d'utiliser une webcam et un microphone avec le navigateur LockDown Browser. Des paramètres supplémentaires apparaissent dans le tableau de bord du navigateur LockDown Browser. Une fois l'examen terminé, un instructeur peut revoir les détails de l'évaluation, y compris les vidéos enregistrées. Dans ce cas, l'outil permet aux enseignants d'exiger que les étudiants utilisent une webcam pendant l'examen, en sélectionnant la fonctionnalité. Si les étudiants utilisent la fonction webcam de Respondus Monitor, en principe seuls les enseignants peuvent accéder aux informations sur les sessions d'examen et visionner les vidéos enregistrées. À titre d'exemple, l'université d'Ottawa[97] possède une licence et propose une présentation résumée de l'outil pour les enseignants et étudiants.

Le dispositif Respondus LockDown Browser est le moins intrusif des deux systèmes puisque l'objectif n'est pas de surveiller l'activité des étudiants mais d'empêcher certaines actions pendant l'examen sur l'ordinateur. Ce type de dispositif est évidemment limité par le fait qu'il est toujours possible aux étudiants de recourir dans le même temps à un autre matériel comme un téléphone intelligent par exemple. Nous laisserons de côté cette hypothèse de contournement des logiciels de surveillance bien qu'elle favorise les étudiants les mieux équipés, soit majoritairement les plus aisés d'entre eux, ce qui peut constituer un facteur de discrimination.

2.2. Proctor U : Université de Toronto

ProctorU est une compagnie fondée en 2008, qui offre des services de surveillance académiques et professionnels. La firme est actuellement basée à Birmingham dans l'État

[96] Respondus, *supra* note 39.
[97] Université d'Ottawa, « FAQ Respondus pour les professeurs et les étudiants » (s.d.), en ligne : *Université d'Ottawa* <https://uottawa.saea-tlss.ca/fr/transition-vers-l-enseignement-a-distance/faq-respondus>.

américain d'Alabama. En janvier 2020, ProctorU et la firme canadienne Yardstick Assessment Strategies ont fusionné sous le nom de Meazure Learning tout en continuant d'opérer sous leurs noms distincts[98]. Jusqu'au mois de mai 2021, ProctorU offrait trois différents services : ProctorU Auto, ProctorU Live+ et ProctorU Pro[99]. ProctorU Auto était l'option automatisée qui déploie un dispositif d'IA pour signaler des comportements jugés suspects tout en enregistrant le déroulement de l'examen, afin d'être visionnée au besoin[100]. Un examen sous la surveillance de ProctorU Auto requiert que l'étudiant détienne une pièce d'identification gouvernementale et soit situé dans un environnement silencieux, bien éclairé et privé[101]. De plus, avant la tenue de l'examen sous la supervision de ProctorU Auto, l'étudiant doit lire et accepter les conditions d'utilisation. Par la suite, il devra prendre une photo de son visage et de sa pièce d'identité à partir du logiciel[102]. Lors de l'examen, il est demandé à l'étudiant de demeurer assis en direction de sa webcam et de travailler en silence[103]. En ce qui concerne l'exigence de silence durant l'examen, il est soutenu que le dispositif de ProctorU peut faussement accuser de tricherie les étudiants ayant une charge parentale qui parle à leur jeune enfant durant l'examen, ainsi que les étudiants ayant un chien qui aboie durant l'examen[104].

ProctorU Live+ est une option combinant un surveillant humain, ainsi qu'un dispositif d'IA pour assurer la surveillance d'examen[105]. ProctorU Pro était une version plus performante de ProctorU Live+ comportant davantage de paramètres pouvant être modifiés, ainsi que les surveillants humains « les mieux entrainés » offerts par ProctorU[106]. Les options de ProctorU sont intégrées aux plateformes d'apprentissage à distance.

En ce qui concerne, la surveillance et l'authentification d'examen, il est difficile de concevoir que ProctorU n'utilise pas les renseignements biométriques des étudiants[107]. D'ailleurs, quant à l'utilisation de l'IA, ProctorU a affirmé en 2020 que la combinaison de processus automatisé et d'intervention humaine serait capable d'atteindre un niveau élevé de précision et de fiabilité, afin d'améliorer sa capacité de détection de tricherie sur le plan

---

[98] Meazure Learning, « ProctorU Merges With Yardstick to Form New 'End-to-End' Testing Company » (14 janvier 2020), en ligne : *Edsurge* <https://www.edsurge.com/news/2020-01-14-proctoru-merges-with-yardstick-to-form-new-end-to-end-testing-company-meazure-learning>.
[99] ProctorU Platform Support, « Do you know all about our three tiers of proctoring… » (7 décembre 2018), en ligne : *Twitter* <https://twitter.com/ProctorUSupport/status/1071157226621059072>.
[100] Ava Abbott, « What is ProctorU, how it works and makes money? » (s.d.) en ligne : *Business Strategy Hub* <https://bstrategyhub.com/what-is-proctoru-how-it-works-and-makes-money/>.
[101] ProctorU, ProctorU Auto Demo for Test Takers, 30 mars 2018, en ligne : *YouTube* <https://www.youtube.com/watch?v=eTFDrRVQzO8>.
[102] *Ibid*.
[103] *Ibid*.
[104] Scott Jaschik, « ProctorU Abandons Business Based Solely on AI », (24 mai 2021) *Inside Higher Ed*, en ligne : <https://www.insidehighered.com/news/2021/05/24/proctoru-abandons-business-based-solely-ai>; Rhea Kelly, « ProctorU Gets Rid of AI-Only Proctoring », (24 mai 2021) *Campus Technology*, en ligne : <https://campustechnology.com/articles/2021/05/24/proctoru-gets-rid-of-ai-only-proctoring.aspx>.
[105] Ava Abbott (s.d.) supra note 88.
[106] *Ibid*.
[107] Ludwig, *supra* note 13 à la p 64

temporel[108], ce qui semble confirmer la présence d'un processus d'apprentissage automatique.

Cependant, le 24 mai 2021, Meazure Learning a annoncé que ProctorU cessera d'offrir des options qui mobilisent uniquement l'IA pour générer les rapports d'incidents et qu'elle s'assurera la vérification du rapport généré par l'IA par une personne[109]. En effet, selon ProctorU, l'utilisation exclusive de l'IA pour générer les rapports d'incidents était parfois injuste pour les étudiants[110]. Quoique ce changement de position pour la firme soit bienvenu, certaines critiques se questionnent quant à la formation offerte aux surveillants humains de ProctorU et contestent le changement de position à l'égard de l'utilisation d'IA. Il s'agirait là d'une simple tactique de relation publique étant donné la multiplication des articles médiatiques à l'égard des logiciels de surveillance[111]. Depuis mai 2021, ProctorU offre encore son option de ProctorU Live+, mais la firme a cessé de mentionner qu'elle utilise un dispositif d'IA, pour employer le terme « technologie avancée » qui serait déployé en combinaison avec une intervention humaine[112]. Ainsi, l'authentification et la surveillance, tant durant l'examen qu'après l'examen, sont maintenant faites par un surveillant humain et cette « technologie avancée » pour l'option ProctorU Live+[113]. Cette option est donc recommandée pour les examens à enjeux élevés.

Par ailleurs, ProctorU offre maintenant Review+ par lequel le processus d'authentification et les vérifications d'examen postérieures sont faites par des surveillants humains, alors que la surveillance est automatisée[114]. Toutefois, les détails quant à l'automatisation de la surveillance d'examen ne sont pas fournis. De plus, Review+ génère un rapport d'incidents

---

[108] « The exciting thing about innovating with machine learning technology is that our system is continuously learning, adapting and getting smarter with every exam. ProctorU's goal in introducing AI into proctoring is not to replace humans but, rather, to strengthen the accuracy of proctoring by assisting humans in identifying details such as shadows, whispers or low sound levels, reflections, etc., that may otherwise go unnoticed ProctorU [2020a] » [nos soulignements] Simon Coghlan, Tim Miller et Jeannie Paterson, *supra* note 4 à la p. 4.

[109] Meazure Learning, « Proctoru To Discontinue Exam Integrity Services That Rely Exclusively On Ai » (24 mai 2021) en ligne : *Meazure Learning* <https://www.meazurelearning.com/resources/proctoru-to-discontinue-exam-integrity-services-that-rely-exclusively-on-ai>; Lindsay McKenzie, « Time to Rethink AI Proctoring ? » 28 may 2021, en ligne : *Inside Higher Ed* <https://www.insidehighered.com/news/2021/05/28/are-colleges-checking-ais-work-remote-exam-proctoring>; Scott Jaschik, 2021, *supra* note 92; Rhea Kelly, 24 mai 2021, *supra* note 92.

[110] Rhea Kelly, 2021, *supra* note 92.

[111] Lindsay McKenzie, 2021, *supra* note 97.

[112]« Advanced Technology Paired with Human Review and Validation [...]During a Live+ session, the live proctor will be alerted if the platform detects a pattern of suspicious activity, but an incident report is not created unless a human proctor or intervention specialist confirms that the activity is not allowed in your exam rules.» [nos soulignements], *Meazure Learning*, « Live+ » (s.d.) en ligne : *Meazure Learning* <https://www.meazurelearning.com/products/proctoru-online-proctoring/live-plus>.

[113] *Ibid.*

[114] « Automated Monitoring Paired with Human Review and Validation […] During a Review+ session, the platform detects and flags patterns of suspicious activity, but an incident report is not created unless a certified proctor reviews the situation and confirms that the activity is not allowed in your exam rules. » Meazure Learning, « Review+ » en ligne : *Meazure Learning* <https://www.meazurelearning.com/products/proctoru-online-proctoring/review-plus>.

à l'attention des professeurs ou superviseurs[115]. Review+ est donc l'option qui est suggérée pour des examens à enjeux moyens et faibles[116]. Finalement, ProctorU offre maintenant l'option Record+ qui est une option assurant l'authentification d'examen de manière automatisée, ainsi qu'une surveillance d'examen automatisée cherchant à identifier des comportements suspects, vérifiés ensuite par un surveillant certifié avant l'émission d'un rapport d'incident[117].

Au Canada, plusieurs universités ont mis en œuvre ProctorU pour la surveillance d'examen tel que l'Université de Toronto[118], l'Université de Waterloo[119], l'Université Athabasca (Alberta)[120], l'Université Thompson Rivers (Colombie-Britannique)[121] et l'Université Memorial[122] (Terre-Neuve-et-Labrador).

Depuis mai 2021, ProctorU a cessé de générer des rapports d'incidents entièrement généré par l'IA. Pour les fins de cette recherche, nous considérons que ProctorU est un logiciel de surveillance hybride, combinant des dispositifs d'IA et une intervention humaine[123].

2.3. Proctorio : Université de Laval et Université de Colombie-Britannique (UBC)

Proctorio est un logiciel de surveillance automatisé proposé par une entreprise américaine située dans l'Arizona. Il mobilise des formules algorithmiques, tel que l'apprentissage automatique et la reconnaissance faciale, afin de détecter des comportements pouvant être indicatifs de tricherie[124]. Selon des communications universitaires, Proctorio est doté de fonctions, telle que l'authentification automatisée, la surveillance automatisée, l'enregistrement vidéo et audio, l'enregistrement de la salle physique et l'examen des comportements étudiant[125]. Ces options permettent la surveillance en temps réel et la

---

[115] *Ibid*.
[116] *Ibid*.
[117] « During a Record+ session, the platform detects and flags patterns of suspicious activity, but an incident report is not created unless a certified proctor reviews the situation and confirms that the activity is not allowed in your exam rules. » Meazure Learning, (s.d.) en ligne : *Meazure Learning* <https://www.meazure learning.com/products/proctoru-online-proctoring/record-plus>.
[118] University of Toronto, « ProctorU: Privacy and Security Information Notice for Students » (s.d.) en ligne : *University of Toronto* <https://teaching.utoronto.ca/ed-tech/online-learning/online-proctoring/proctoru-privacy/>.
[119] University of Waterloo « Online proctoring FAQs » (s.d.) en ligne : *University of Waterloo* <https://uwaterloo.ca/extended-learning/learn-online/write-exams/online-proctoring-faqs>.
[120] Athabasca University, « Using ProctorU for online exams » (s.d.), en ligne : *Athabasca University* <https://www.athabascau.ca/support-services/exam-services-support/using-proctoru-for-online-exams.html>.
[121] Thompson Rivers University, « ProctorU » (s.d.), en ligne : *Thompson Rivers University* <https://www.tru.ca/distance/faq/faq-proctoru.html>.
[122] Memorial University, « Online Proctoring » (s.d.), en ligne : *Memorial University* <https://citl.mun.ca/TeachingSupport/TeachOnline/OnlineProctoring.php>.
[123] Ludwig, *supra* note 13 à la p. 71
[124] Monica Chin, « An ed-tech specialist spoke out about remote testing software — and now he's being sued », (22 octobre 2020), en ligne : *The Verge* <https://www.theverge.com/2020/10/22/21526792/proctorio-online-test-proctoring-lawsuit-universities-students-coronavirus>.
[125] The University of British Columbia, « Software for Securing & Proctoring Exams » (s.d.), en ligne : *The University of British* Columbia <https://isit.arts.ubc.ca/software-for-securing-proctoring-exams/>.

surveillance par enregistrement (voir tableau 4 à l'annexe 1)[126]. Bien que situé dans un état américain, le site internet de Proctorio prétend s'adresser à des institutions situées aux États-Unis, au Canada ou en Europe, ce qui supposerait de respecter le règlement (UE) 2016/679 de protection des données personnelles (RGPD). Proctorio indique d'ailleurs sur son site internet pouvoir avoir la qualité de sous-traitant (data processor) ou de responsable de traitement (data controller).

Proctorio affirme que ses techniques algorithmiques sont supérieures et plus efficaces à la surveillance humaine pour combler les biais et les erreurs humaines et parvenant à de meilleurs résultats que l'humain lors de la détection de la tricherie académique[127] Toutefois, à maintes reprises, Proctorio a été accusée de mobiliser des algorithmes qui sont discriminatoires envers les étudiants de minorité visible[128]. Il est en effet constaté que Proctorio met en œuvre un algorithme de source ouverte qui est reconnu comme étant discriminatoire envers les individus appartenant à une minorité visible. Selon certains essais, 57% des tentatives d'authentification par les individus à la peau noire sont infructueuses[129]. De plus, il est aussi affirmé que les meilleurs taux d'authentification dans tous les groupes d'ethnicité sont inférieurs à 75%[130], ce qui implique que le taux d'erreur est élevé.

Par ailleurs, certains logiciels de surveillance, tel que Proctorio et Proctor U, ont fait l'objet de critiques par le sénateur américain Richard Blumenthal quant à l'opacité des logiciels et appelant à des explications sur leur fonctionnement[131]. Du côté de Protorio, l'entreprise défend ardemment ses intérêts. Le cas d'un étudiant en science informatique est exemplaire. Celui-ci aurait critiqué Proctorio ouvertement sur Twitter en invoquant une analyse de code informatique du logiciel. Par la suite, cet étudiant s'est fait demander par le PDG de Proctorio de supprimer ses tweets. Après son refus, l'adresse IP de l'étudiant a été supprimée des services de Proctorio, interdisant dorénavant l'étudiant de se brancher à Proctorio pour compléter des évaluations académiques utilisant le logiciel[132].

Au Canada, Proctorio a été mis en œuvre par l'université Concordia[133] et l'Université de la Colombie-Britannique (UBC). Toutefois en mars 2021, suivant un vote des deux Sénats

---

[126] Ibid.
[127] Simon Coghlan, Tim Miller et Jeannie Paterson, *supra* note 4 à la p 4.
[128] Ibid; Todd Feathers, « Proctorio Is Using Racist Algorithms to Detect Faces » 4 aout 2021 en ligne : *Vice* <https://www.vice.com/en/article/g5gxg3/proctorio-is-using-racist-algorithms-to-detect-faces>; Michelle Clark, « Students of color are getting flagged to their teachers because testing software can't see them » (8 avril 2021), en ligne : *The Verge* < https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning>.
[129] Todd Feathers, 2021, *supra* note 116.
[130] Monica Clark, *supra* note 116.
[131] Zack Whittaker, « Senator: 'More transparency is needed' by exam proctoring tech firms » (19 janver 2021), en ligne : *Techcrunch* <https://techcrunch.com/2021/01/19/senator-more-transparency-is-needed-by-exam-proctoring-tech-firms/>.
[132] Todd Feathers, Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools, (24 septembre 2020), en ligne : *Vice* <https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools>.
[133] Université Concordia, « Proctorio » (s.d.), en ligne : *Université Concordia* <https://www.concordia.ca/ctl/digital-teaching/proctorio.html>.

de l'UBC Vancouver et de l'UBC Okanagan, l'université a annoncé qu'elle interdisait l'utilisation de logiciels de surveillance automatisée, tel que Proctorio, dans tous les programmes à l'exception des programmes d'accréditation qui requièrent une telle utilisation[134]. Les professeurs qui prévoyaient d'utiliser de tels outils pour surveiller des examens dans le cadre de cours qui ne sont pas visés par l'exemption susmentionnée sont invités à chercher d'autres outils et/ou méthodes d'évaluation.

L'outil a fait l'objet d'une analyse d'impact sur la vie privée (PIA) et son abandon pourrait être justifié par des résultats insatisfaisants[135].

[134] The University of British Colombia, « UBC Senate motions on use of remote proctoring software », 18 mars 2021, en ligne : *The University of British Colombia* <https://lthub.ubc.ca/2021/03/18/ubcv-senate-motion-proctoring/>.

[135] The University of British Colombia, en ligne : *The University of British Colombia* <https://privacymatters.ubc.ca/sites/privacymatters.ubc.ca/files/PIA>.

3. ANALYSE JURIDIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

3.1. Détermination des lois de protection des renseignements personnels applicables

L'utilisation des logiciels de surveillance d'examens suppose la collecte de renseignements personnels dans le cadre de l'éducation. Les lois provinciales de protection des renseignements personnels du secteur public sont en principe applicables, dès lors que l'éducation relève de la compétence des provinces[136]. Les lois provinciales du secteur public reprennent le critère du *contrôle* posé par la *loi fédérale sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21 (LPRP). Ces lois s'appliquent aux renseignements personnels et aux documents qui *relèvent* d'un organisme ou d'une institution publique, ce qui est le cas de la plupart des universités. Le contrôle n'a toutefois pas besoin d'être absolu, direct ou permanent. La Cour d'appel fédérale a ainsi jugé dans l'arrêt *Société canadienne des postes c. Canada (Ministre des travaux publics)*, 1995 CAF 241, que l'expression « relevant de » doit faire l'objet d'une interprétation souple et libérale. Par exemple, si les renseignements sont détenus par un mandataire d'un organisme public, ils relèvent de l'organisme public lui-même et la loi du secteur public continue de s'appliquer.

Cette question est centrale s'agissant du recours aux outils de surveillance d'examens puisque les universités font appel à des entreprises privées pour les mettre en œuvre. Cependant, cette jurisprudence n'est pas applicable à ce cas. En effet, les universités ne se contentent pas ici de confier la gestion ou la conservation des données à des entreprises tierces. Elles mettent en relation les entreprises privées avec les étudiants dans des circonstances de collecte directe de renseignements personnels auxquels les universités elles-mêmes n'ont pas nécessairement accès. Les renseignements ainsi collectés échappent au contrôle des universités. Dès lors, doit-on considérer que les universités sont encore en contrôle ? Si ces dernières tentent d'imposer des conditions de protection des renseignements personnels en s'appuyant sur les lois provinciales du secteur privé et sur leurs propres politiques de confidentialité, elles se trouvent, de fait, confrontées à la puissance des outils technologiques et à la perte de maîtrise des outils. Ce constat vaut pour la collecte des données, les traitements, le stockage voire la durée effective de conservation.

Dans ce contexte, les lois du secteur public ont-elles encore vocation à s'appliquer ?

S'agissant des universités, l'application des lois du secteur public ne fait aucun doute puisque les lois du secteur privé s'appliquent dans l'hypothèse où l'organisation exerce une activité commerciale en dehors de son activité essentielle. Or, tel n'est pas le cas dans la mise en œuvre d'un système automatique de surveillance d'examen.

[136] Commissariat à la protection de la vie privée du Canada, « Application de la LPRPDE aux municipalités, universités, écoles et hôpitaux » (décembre 2015), en ligne : *Commissariat à la protection de la vie privée du Canada* <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/02_05_d_25/>.

En revanche, s'agissant des entreprises privées technologiques, faut-il considérer que les lois de protection des renseignements personnels du secteur privé s'appliquent ? Si tel est le cas, comment les régimes de protection du secteur public et du secteur privé devraient-ils s'articuler ? Ces entreprises interviennent pour le compte des organismes publics. Mais, plus encore, elles collectent directement et pour leur propre compte des données personnelles des étudiants par des moyens technologiques qu'elles sont les seules à contrôler.

Plusieurs facteurs peuvent faire pencher en faveur de la mise en œuvre des lois du secteur privé directement envers ces entreprises.

D'abord, les conditions générales d'utilisation ou les politiques de confidentialité de ces entreprises précisent que les renseignements personnels pourront être utilisés pour des activités d'apprentissage automatique afin d'améliorer leurs services. Une telle finalité dépasse celle prévue par les universités s'agissant des activités de surveillance d'examen.

Ensuite, la collecte de ces données fait l'objet d'un recueil du consentement des étudiants en même temps qu'ils consentent à utiliser les logiciels. En effet, la collecte de données personnelles dans le cadre initial de l'activité de surveillance d'examen relève d'une mission des universités et est autorisée par les lois provinciales du secteur public, sans qu'aucun consentement ne soit exigé, sur le modèle de la *loi fédérale sur la protection des renseignements personnels*. Mais la recherche du consentement est ici justifiée par le fait que la collecte des données fonde un tout autre usage, purement commercial, des données. Les entreprises technologiques ont ici l'occasion d'améliorer la performance de leurs outils sur un marché technologique intéressant différents secteurs d'activités privés ou publics. Ce changement de finalité dépasse l'autorisation de la collecte donnée par la loi et justifie la recherche du consentement.

Ce changement de finalité est d'autant plus aisé que des algorithmes similaires peuvent être utilisés pour différents cas d'usages. Le même dispositif de reconnaissance faciale peut tout autant servir à identifier les étudiants pendant les examens qu'à des fins policières ou de surveillance de certaines populations. Les finalités sont publiques du point de vue des missions des organismes publics mais aussi commerciales s'agissant des entreprises technologiques. Conséquemment, la distinction entre les activités du secteur public et du secteur privé trouve ici une limite fondamentale. Or, le régime juridique actuel du droit canadien, tant fédéral que provincial, repose sur cette distinction de la protection des renseignements personnels dans le secteur public et dans le secteur privé. Les partenariats publics-privés, particulièrement nombreux dans le domaine des outils et services technologiques, sont ainsi mal captés par la loi.

3.2. Identification des renseignements personnels collectés

Les logiciels de surveillance d'examen collectent des renseignements personnels, d'autant plus que ces derniers s'interprètent largement dans les lois sur le secteur public. Les énumérations législatives des renseignements ne sont ainsi pas exhaustives. À l'université d'Ottawa, par exemple, les professeurs et le personnel autorisé ont accès aux enregistrements vidéo et audio des examens, ainsi qu'aux informations personnelles, telles que le nom. L'autorisation est accordée cours par cours et est limitée aux professeurs et

assistants d'enseignement, aux surveillants autorisés par la faculté et aux administrateurs du Campus Virtuel de l'université d'Ottawa.

La politique de confidentialité de Respondus Monitor indique ainsi que des informations sont recueillies, afin de pouvoir offrir la meilleure expérience possible dans l'utilisation des services. Outre les renseignements directement collectés auprès des étudiants lors de l'accès au service (via notamment le compte, le formulaire de contact, le bulletin d'information, des concours ou enquêtes), sont aussi recueillies des informations supplémentaires, lorsque des services sont fournis pour assurer les performances nécessaires et optimales. Il peut s'agir d'informations liées au compte et collectées dans le cadre de l'utilisation des services. Dès lors que des informations personnelles sont collectées pour optimiser les performances, la finalité du traitement est large et la nature des données collectée n'est pas clairement indiquée. Ces procédés de collecte massive et d'exploration des données vont permettre de nourrir les systèmes d'intelligence artificielle.

Plus spécifiquement, la politique de vie privée de Respondus[137] précise que diverses données sont traitées automatiquement pendant une session d'examen qui utilise Respondus Monitor. L'enregistrement de la webcam passe lui-même par une étape de "post-traitement" automatisée qui utilise la technologie de détection et de reconnaissance du visage pour déterminer : si l'étudiant est resté dans le cadre vidéo, si plusieurs personnes apparaissent dans le cadre vidéo, si la personne dans le cadre vidéo diffère de la personne qui a commencé l'examen, et la position du visage de l'utilisateur par rapport au dispositif d'enregistrement de la webcam. Les conditions générales de Respondus[138] indiquent également que l'utilisation de Respondus Monitor nécessite l'enregistrement de l'activité individuelle des étudiants, à la fois auditive et visuelle, pendant certaines sessions d'évaluation. Lorsque Respondus Monitor est activé, le logiciel collecte les enregistrements vidéo et audio capturés par la webcam et le microphone, une image de la carte d'étudiant (ou autre document permettant d'identifier l'étudiant) et des données concernant l'activité, y compris les mouvements des yeux et le temps pris pour répondre à des questions spécifiques sur une évaluation.

En outre, Respondus Monitor[139] traite d'autres données provenant de la session d'examen, telles que : la date et l'heure auxquelles l'utilisateur commence et termine une session d'examen ; l'heure à laquelle il répond à chaque question d'examen ; le temps passé sur chaque question d'examen ; si/quand une réponse à une question d'examen est modifiée ; la qualité de la connexion Internet de l'utilisateur pendant la session d'examen (y compris l'heure et la durée de toute déconnexion Internet) ; l'activité de la souris, du clavier et de l'écran ; la qualité de l'enregistrement vidéo (en termes d'éclairage, de contraste, de mouvement) ; et la qualité de l'enregistrement audio, entre autres données. Ces données dites comportementales peuvent aussi être qualifiées de renseignements personnels.

---

[137] Respondus, *supra* note 125.
[138] Respondus, « Terms of Use – Respondus Monitor (Student) » (s.d.) en ligne : *Respondus* <https://web.respondus.com/tou-monitor-student/>.
[139] Respondus, *supra* note 125.

Plus inquiétant encore, d'autres données sont inférées en enregistrant la manière dont l'étudiant interagit avec LockDown Browser et Respondus Monitor, par exemple en recevant des rapports d'erreur ou des données d'utilisation provenant d'un logiciel fonctionnant sur l'appareil. En outre, il est précisé que Respondus Monitor peut analyser les enregistrements par le biais de processus automatisés, afin de générer des données supplémentaires dérivées des enregistrements, les données supplémentaires étant associées à des étudiants individuels pour être utilisées par l'établissement dans l'évaluation des enregistrements. Le logiciel utilise également des processus automatisés pour aider les professeurs à évaluer les enregistrements. Respondus Monitor suit en permanence les applications et les processus qui sont exécutés sur le dispositif informatique pendant une session d'examen. Les données individuelles de l'utilisateur peuvent être comparées aux données agrégées de l'ensemble des utilisateurs pour rechercher des modèles ou des anomalies, par exemple si un utilisateur a passé un temps anormalement long à répondre à une question par rapport aux autres utilisateurs.

Ces informations supplémentaires comprennent la création d'un modèle temporaire d'identifiants faciaux pendant le traitement automatisé et ce modèle est utilisé dans la mémoire temporaire du serveur exécutant le logiciel Respondus Monitor pour déterminer si l'étudiant qui a commencé l'examen diffère de la personne actuellement dans l'image vidéo traitée par le service Respondus Monitor. Le modèle n'est pas enregistré dans la base de données ou le stockage du serveur en nuage et est effacé de la mémoire du serveur par Respondus Monitor une fois le traitement terminé, ce qui se produit au plus tard deux (2) jours après la fin de l'examen. Les données supplémentaires, ainsi que les enregistrements originaux, peuvent être évalués par les agents de l'établissement, y compris les professeurs, afin d'examiner, d'évaluer et d'analyser les performances et la conduite des étudiants, et d'enquêter sur les violations présumées de la conduite des étudiants.

Par ailleurs, les conditions contractuelles[140] indiquent que les données collectées dépendent des fonctionnalités utilisées dans les Services d'aide, et comprennent notamment la vérification du système qui rassemble certaines informations provenant de l'appareil informatique, de l'environnement réseau, du système de gestion de l'apprentissage de l'établissement et du serveur Respondus Monitor lui-même.

Finalement, la liste de données personnelles collectées concerne les informations basiques collectées auprès des étudiants pour garantir le bon fonctionnement du service. Mais de nombreuses autres informations peuvent être inférées pour l'optimisation des services. En outre, le fait que des vidéos des étudiants soient collectées par Respondus Monitor et conservées pendant une durée qui n'est pas clairement indiquée par Respondus est particulièrement problématique. De telles données relèvent du droit à la vie privée, du droit à la protection des renseignements personnels et du droit à l'image. À la lecture des conditions contractuelles générales, les principes de minimisation, nécessité et proportionnalité ne semblent pas respectés. En particulier, les imprécisions contractuelles font douter de la conformité aux lois de protection des renseignements personnels, en particulier eu égard aux finalités trop larges et à la durée de conservation trop floue. Au

[140] Respondus, *supra* note 128.

demeurant, la liste des renseignements personnels effectivement collectés n'est pas clairement énumérés, ce qui porte atteinte au droit à l'information des personnes dont les renseignements sont collectés.

3.3. Consentement lié à la collecte des renseignements personnels et consentement lié à l'utilisation du système de surveillance

Une question importante est de savoir si les étudiants ont consenti à la collecte des renseignements personnels, en plus de consentir à l'utilisation d'un système de surveillance d'examen, ce qui supposerait l'expression de deux consentements distincts.

S'agissant d'abord du consentement à la collecte des renseignements personnels, les lois provinciales du secteur public, tout comme la loi fédérale, ne prévoient pas de principe de consentement à la collecte mais un simple droit à l'information et un droit d'accès. Le consentement ne sera donc pas requis par la loi et la collecte sera licite si elle réalisée dans un des buts suivants : (1) la collecte est explicitement autorisée par la loi : (2) la collecte est directement liée et est nécessaire pour mener un programme ou une activité d'un organisme public ; (3) la collecte est réalisée à des fins de mise en application des lois. Certaines juridictions (Canada, Saskatchewan, Québec) n'envisagent que la deuxième hypothèse. En conséquence, les universités sont autorisées par la loi à collecter les renseignements personnels des étudiants ce qui entre clairement dans leur mission.

Les universités peuvent en effet se prévaloir des deux premiers cas. Par exemple, à l'université d'Ottawa, les renseignements personnels transmis à l'Université par un étudiant, un employé, un diplômé, un donateur ou un autre particulier sont recueillis en vertu de la Loi de l'Université d'Ottawa de 1965[141] et sont censés être utilisés aux fins de l'administration des programmes et activités de l'Université et de manière conforme à ceux-ci, ainsi que pour l'exécution d'autres services et fonctions de l'Université, dont le recrutement, l'admission et l'inscription, les programmes d'études et les évaluations, et la remise des diplômes[142]. Dès lors, la collecte des renseignements personnels des étudiants dans le cadre des examens est régie par cette *Loi* dans ses rapports avec l'Université. Au demeurant, la plupart des universités prévoient un système de consentement, comme l'Université d'Ottawa[143], de l'étudiant qui acceptent les politiques de confidentialité sans y être légalement tenus puisque la loi de l'Ontario sur l'accès à l'information et la protection de la vie privée autorise la collecte[144].

En cas de questions sur la collecte, l'utilisation et la divulgation des renseignements personnels, les étudiants sont invités à contacter le responsable de la protection de la vie

---

[141] Loi de l'Université d'Ottawa 1965, S.O. 1965, C.137.

[142] Université d'Ottawa, « Règlement 90 - Accès à l'information et la protection des renseignements personnels », en ligne : *Université d'Ottawa* <https://www2.uottawa.ca/notre-universite/administration-gouvernance>.

[143] Université d'Ottawa, *supra* note 85.

[144] L'article 38(2) de la loi de l'Ontario sur l'accès à l'information et la protection de la vie privée, L.R.O. 1990, chap. F.31 dispose que « Nul ne doit recueillir des renseignements personnels pour le compte d'une institution à moins d'y être autorisé expressément par une loi, ou à moins que ces renseignements servent à l'exécution de la loi ou soient nécessaires au bon exercice d'une activité autorisée par la loi."
Loi sur l'accès à l'information et la protection de la vie privée, L.R.O. 1990, chap. F.31

privée par courrier électronique dont l'adresse courriel est indiquée. Il est préconisé par ailleurs d'enlever ou dissimuler les biens personnels portant des images ou des noms (par exemple, des photographies ou des signes de famille) pour préserver au maximum la vie privée. Ces précautions sont utiles mais ne peuvent compenser le fait que par définition les étudiants sont filmés et enregistrés pendant la session ce qui porte nécessairement atteinte au droit à l'image et constitue une collecte de renseignements personnels auxquels les étudiants consentent plus ou moins librement.

Il faut ajouter que les organismes publics peuvent vouloir utiliser les renseignements personnels pour un usage secondaire suivant des finalités déterminées : (1) pour la finalité pour laquelle l'information a été collectée ou pour un usage cohérent avec cette finalité ; (2) pour une finalité pour laquelle l'information peut être divulguée au public ; (3) dans l'hypothèse où la personne concernée a consenti, suivant la façon prescrite, à l'utilisation. Ces usages sont liés au premier usage et ne requièrent pas le consentement, ce qui sera différent pour d'autres usages secondaires non liés. Il faut en particulier relever que ces dispositions autorisent l'utilisation des renseignements personnels par les organismes publics mais n'emportent pas l'autorisation de divulgation et d'utilisation pour des entreprises privées qui fournissent des services à ces organismes publics. En conséquence, les entreprises privées doivent bénéficier d'une autorisation particulière pour utiliser les données qui suppose le consentement des personnes concernées.

S'agissant des logiciels de surveillance d'examen, les entreprises technologiques qui souhaitent utiliser les données pour entraîner les algorithmes, en particulier pour faire de la reconnaissance faciale, font alors un usage secondaire pour une finalité différente et doivent obtenir le consentement des personnes dont les données sont utilisées selon toutes les lois (fédérale et provinciales) du secteur public. Dès lors, les conditions générales d'utilisation des entreprises technologiques font logiquement reposer l'utilisation et la collecte des renseignements personnels sur le consentement donné par les étudiants. Proctorio requiert par exemple la communication de conditions d'utilisation claires et l'obtention du consentement des étudiants avant toute utilisation[145].

Mais un consentement unique est alors requis, englobant l'accord pour l'utilisation du service et la collecte de tous les renseignements personnels, sans que les étudiants puissent avoir clairement conscience que de la nature et de la quantité des renseignements personnels collectés et l'utilisation qui en sera faite par la suite. Ils en ont d'autant moins conscience que la nature des informations ainsi recueillies n'est pas listée avec certitude et exhaustivité dans les politiques de confidentialité. On peut donc douter du caractère libre et éclairé du consentement à l'utilisation des renseignements personnels qui serait donné aux entreprises, alors même que les étudiants ont une marge de manœuvre limitée pour accepter ou refuser l'outil dans le contexte de passation d'un examen.

Quant au consentement à la mise en œuvre du système de surveillance d'examen, il est nécessaire au moment même de l'installation des outils. Ainsi par exemple, la société

[145] Selon les informations fournies par l'université Laval par exemple :
voir Université Laval «Surveillance d'examen en télésurveillance avec Proctorio » (s.d.) en ligne : *Université Laval* <https://www.enseigner.ulaval.ca/ressources-pedagogiques/proctorio>.

Respondus prévoit que l'étudiant accepte ses conditions d'utilisation au moment de l'installation du système et qu'il doit en outre vérifier ces dernières avant chaque examen et les accepter. Si un étudiant refuse les conditions d'utilisation lors de la séquence de démarrage de Respondus ou lors de la phase d'installation, il ne pourra pas démarrer l'examen. Le consentement est donc directement lié à l'utilisation. À titre d'exemple, Polytechnique Montréal utilise ProctorExam et indique dans sa politique de confidentialité[146] que « les étudiantes et étudiants qui demandent un accommodement pour effectuer leurs examens en ligne doivent avoir conscience que certains examens pourraient être surveillés par le logiciel ProctorExam. Advenant que ce logiciel soit utilisé pour certains de vos examens, le refus d'effectuer votre examen en ligne par ProctorExam entraînera un abandon du ou des cours visé(s) par la surveillance d'examen et tous les droits de scolarité relatifs à ce ou ces cours seront exigés ». On le voit, les étudiants ne sont pas réellement placés dans la position de consentir librement, dès lors qu'ils auraient fait le choix en l'occurrence de passer leurs examens en ligne. Cependant, il convient de nuancer en précisant que le recours aux examens en ligne n'est pas le principe mais un accommodement accordé aux étudiants. La conséquence est alors que ces derniers doivent accepter l'utilisation d'un tel outil de surveillance.

À l'université d'Ottawa par exemple[147], en cas de refus, le professeur doit prévoir des options alternatives à la gestion des examens et des évaluations académiques. L'Université Laval prévoit pour sa part que l'étudiant est libre de choisir ce type d'examen en télésurveillance ou en présentiel[148]. Mais on comprend par ailleurs que l'examen de l'étudiant qui refuserait le système ne pourra être identique à celui des autres étudiants, ce qui pose la question d'une rupture d'égalité entre ces derniers. Ainsi, à la suite du mécontentent exprimé par les étudiants, la stratégie de l'Université de Colombie-Britannique a changé. L'Université encourage les professeurs à choisir d'autres alternatives aux examens en personne et à permettre aux élèves de démontrer leur apprentissage sans le stress supplémentaire et les problèmes de confidentialité qui peuvent découler du fait d'être surveillé par une caméra et de passer un examen à la maison[149].

Si le consentement paraît nécessaire, on peut s'interroger sur les conditions de sa collecte dans un tel contexte : est-il véritablement libre et éclairé ? Les étudiants ne sont-ils pas en situation de dépendance envers les enseignants et l'institution universitaire, dès lors qu'ils sont en attente de l'obtention de leurs notes et diplômes ? N'y a-t-il pas une asymétrie de pouvoir ? Les étudiants ont-ils un réel choix même si les enseignants doivent garantir des alternatives ?

Plus encore, il est difficile de savoir précisément quelles sont les conditions contractuelles applicables au service, dès lors que le site de Respondus indique que les conditions de

[146] Polytechnique Montréal, *supra* note 45.
[147] Université d'Ottawa *supra* note 85.
[148] Université Laval, *supra* note 45.
[149] The University of British Columbia, « Assignments & Assessments » (s.d.), en ligne : *The University of British Columbia* <https://keepteaching.ubc.ca/assignments-assessments/#exam-alternatives>.

Respondus Monitor peuvent varier selon les régions et les institutions[150]. En outre, les entreprises se réservent un droit de modification unilatérale et à tout moment des politiques de confidentialité. Dans sa politique de confidentialité[151], Respondus indique se réserver le droit de modifier ladite politique à tout moment. Dans ce cas, le changement fait l'objet d'une publication sur leur site Web et à tout autre endroit que Respondus jugera approprié, pour informer des données collectées, des utilisations et des circonstances dans lesquelles elles sont divulguées : « Si nous apportons des modifications importantes à cette politique de confidentialité, nous vous en informerons ici, par courrier électronique ou par le biais d'un avis sur notre page d'accueil, au moins trente (30) jours avant la mise en œuvre des modifications ».

Les étudiants sont invités à revoir les termes et conditions à chaque début d'examen, ce qui n'apparaît pas très réaliste pour la plupart des étudiants davantage concentrés sur leurs examens que préoccupés par les aspects matériels de la surveillance et les conditions de collecte de leurs renseignements personnels. Il est particulièrement discutable de mettre à leur charge l'obligation de se renseigner, ce qui aurait en contrepartie pour effet de libérer l'entreprise Respondus de toute obligation d'information spécifique en cas de changement de ces conditions. Dans la mesure où les étudiants sont placés dans une situation d'asymétrie d'informations par rapport à l'utilisation d'une technologie complexe qui collecte des données personnelles et les surveillent, l'obligation de s'informer ne devrait pas reposer sur eux.

3.4. Droits d'accès, de mise à jour et de suppression des données (durée de conservation)

Les lois provinciales de protection des renseignements personnels dans le secteur public accordent des droits d'accès, de mise à jour et de suppression des données. Par exemple, la politique de confidentialité de Respondus[152] donne ainsi la possibilité aux étudiants de mettre à jour et supprimer les informations personnelles. Il est en outre précisé que les données personnelles ne sont conservées que pendant la durée nécessaire à la fourniture des services et, par la suite, pour une variété d'objectifs légaux ou commerciaux légitimes. Il peut s'agir de périodes de conservation : prescrites par la loi, un contrat ou des obligations similaires applicables aux activités commerciales ; pour préserver, résoudre, défendre ou faire valoir des droits légaux/contractuels ; ou si nécessaire pour maintenir des dossiers commerciaux et financiers adéquats et précis.

On voit qu'il y a une certaine imprécision de la durée de conservation des données, en particulier eu égard à des *objectifs commerciaux légitimes*. Ce flou semble être en contradiction avec les politiques de confidentialité des universités. L'Université

[150] Respondus, « Terms of Use – Respondus Monitor (Student) » (s.d.) en ligne : *Respondus* <https://web.respondus.com/tou-monitor-student/>."A copy of the Respondus Monitor Terms of Use for Students is shown below for reference. Please note, terms may vary by region. Certain institutions may also use customized versions of these terms. Students should review the terms that appear each time they start an exam as those are the exact terms they must agree to at their institution in order to use Respondus Monitor".
[151] Respondus, *supra* note 32.
[152] *Ibid*.

d'Ottawa[153] indique par exemple sur son site internet que « Les vidéos des sessions d'examen sont stockées dans les serveurs Respondus pendant 1 an » à compter de la fin du semestre, en lien avec le délai de contestation possible des notes en cas de litige. En outre, il est possible de prolonger cette durée à la demande de l'institution.

Cependant, les conditions contractuelles de la société Respondus ne sont pas claires. En particulier, le renvoi aux finalités commerciales « légitimes » rend finalement incertaine la durée de conservation.

À l'inverse, Polytechnique Montréal utilise ProctorExam[154] et indique que les données recueillies seront stockées sur les serveurs de la société ProctorExam au Canada pendant 30 jours, puis détruites à l'issue de ce délai. En cas de soupçon de plagiat, cette durée de conservation sera prolongée à six mois et les données liées à la surveillance de l'examen en ligne seront également conservées par Polytechnique.

On le voit, les conditions d'accès, de mise à jour et de suppression des données varient d'un système et d'une université à une autre et peuvent s'avérer ambiguës ou contradictoires.

3.5. Partage des renseignements personnels

La politique de confidentialité de Respondus[155] indique par ailleurs que « les informations sur les étudiants, notamment le nom, les notes, le nom du cours et les photos prises sur les cartes d'identité, ne sont accessibles que dans le Campus Virtuel et Respondus ne peut pas consulter ou accéder aux informations des étudiant. Les cartes d'identité sont les cartes d'étudiant ou d'autres formes d'identification. L'étudiant doit simplement montrer une pièce d'identité universitaire ou gouvernementale valide à la caméra ». En outre, ces données ne peuvent être consultées que par le personnel autorisé. Seul le corps professoral du cours peut visionner les sessions vidéo en conjonction avec les informations d'identification des étudiants.

Respondus indique en outre ne pas vendre, louer ou divulguer les informations personnelles des étudiants à des tiers pour leurs besoins de marketing et de publicité. En revanche, la divulgation est possible à des entreprises partenaires en cas d'acceptation des personnes concernées. Cette divulgation peut être aussi nécessaire pour permettre aux étudiants d'accéder aux services, pour permettre à Respondus de respecter ses obligations légales, pour faire respecter ses conditions d'utilisation, pour faciliter ses activités de marketing, ou encore pour prévenir, détecter, atténuer et enquêter sur des activités frauduleuses ou illégales liées aux services. Respondus affirme réduire au minimum la quantité d'informations personnelles divulguées à ce qui est directement pertinent et nécessaire pour atteindre le but spécifié. Cette société prétend donc se conformer aux principes de nécessité et minimisation des données. Cependant, les finalités envisagées sont larges et sont en contradiction avec cette affirmation. En outre, on remarque d'autres contradictions dans le fait de prétendre ne pas avoir accès aux données d'identification des étudiants tout en

[153] Université d'Ottawa, *supra* note 85.
[154] Polytechnique Montréal, *supra* note 45.
[155] Respondus, *supra* note 72.

prévoyant la possibilité de divulguer ces informations à des entreprises tierces pour des motifs de marketing. Une fois encore, la liste des renseignements personnels auxquels Respondus a accès n'est pas clairement énoncée. On peut aussi douter des conditions de recueil du consentement des étudiants s'agissant du partage des renseignements personnels avec des entreprises tierces. Il est probable que le consentement au partage soit demandé en même temps que le consentement à l'utilisation du système et non pas de façon séparée. Ce consentement est en outre donné avant la rédaction d'un examen, alors que l'étudiant se trouve dans un état de stress notable, ce qui fait douter de son caractère libre et éclairé.

Par ailleurs, Respondus coopère avec le gouvernement et les responsables de l'application de la loi, ainsi qu'avec les parties privées pour faire respecter la loi et s'y conformer. Sera ainsi divulguée toute information concernant les personnes concernées à des fonctionnaires du gouvernement ou des forces de l'ordre ou encore à des parties privées si Respondus le juge nécessaire ou approprié, à sa seule discrétion, pour répondre à des réclamations et à des procédures judiciaires (telles que des demandes de citation à comparaître), pour protéger sa propriété et ses droits ou sa propriété et ses droits d'un tiers, pour protéger la sécurité du public ou de toute personne, ou pour prévenir ou arrêter une activité que Respondus considère comme illégale ou contraire à l'éthique. Dans la mesure où Respondus est légalement autorisé à le faire, des mesures raisonnables seront prises pour informer les personnes concernées au cas où des informations personnelles seront fournies à des tiers dans le cadre d'une procédure légale. Respondus reste responsable du soin des données qui sont transférées à des tiers, à moins que la personne concernée demande de les transmettre à la tierce partie.

À l'Université d'Ottawa[156], le système Respondus Monitor est mis en œuvre via le Campus Virtuel, géré par la compagnie D2L ce qui suppose que les données connectées via Respondus Monitor soient, de fait, partagées avec cette entreprise tierce, qu'il s'agisse tant des données d'identité que des enregistrements de sessions d'examens. Au demeurant, les professeurs consultent les rapports de Respondus Monitor à partir de l'outil Questionnaire du Campus Virtuel (Brightspace). Par ailleurs, il est indiqué que les vidéos des sessions d'examen sont stockées sur Brightspace pendant un an et dans les serveurs Respondus pendant la même durée. Or, le partage d'information entre ces deux entreprises n'est pas clair ni même les conditions de protection des renseignements personnels. Le même constat doit être fait pour la plupart des logiciels de surveillance qui sont mis en œuvre via les plateformes d'apprentissage en ligne (D2L). Les relations entre les entreprises et l'éventualité d'un partage des données ne sont pas clairement précisées, ni pour l'admettre, ni pour l'exclure.

Selon une étude de 2020 analysant 25 logiciels de surveillance, il en découle que 18 des 25 logiciels prévoyaient le partage d'information avec de tierces parties dans leurs politiques d'utilisateurs[157] (voir tableau 1 de l'annexe à la page 32).

[156] Université d'Ottawa, *supra* note 85.
[157] David G. Balash et al, *supra* note 16 à la p 2.

3.6. Larges finalités et entraînement des systèmes d'intelligence artificielle (apprentissage automatique, reconnaissance faciale)

En principe, les organismes du secteur public ne peuvent utiliser les renseignements personnels que pour des usages limités : (1) suivant la finalité pour laquelle l'information a été collectée ou pour un usage cohérent avec cette finalité ; (2) pour une finalité pour laquelle l'information peut être divulguée à cet organisme public ; (3) quand la personne concernée a consenti à l'utilisation. Notons que la loi du secteur public au Québec ne se réfère pas à la finalité pour l'utilisation des renseignements personnels par un organisme public.

Dans sa politique de confidentialité[158], Respondus affirme utiliser les renseignements personnels pour les finalités suivantes : améliorer et optimiser le fonctionnement et les performances des services (y compris les sites Web et les applications mobiles) ; diagnostiquer les problèmes et identifier les risques de sécurité, les erreurs ou les améliorations nécessaires aux services ; détecter et prévenir la fraude et les abus des services et systèmes ; collecter des statistiques globales sur l'utilisation des services ; comprendre et analyser la manière dont vous utilisez nos services et les produits et services qui vous sont les plus pertinents. Une collecte massive de données est ainsi organisée, ainsi que les procédés et motifs d'exploration. En particulier, les vidéos collectés peuvent servir à entraîner des systèmes de reconnaissance faciale.

Plusieurs dispositifs d'intelligence artificielle peuvent être mis en œuvre, en particulier le traitement automatique des données et la reconnaissance faciale[159]. Si la reconnaissance faciale n'est pas systématiquement mise en œuvre, il en va autrement des procédés de traitement automatique des données (*machine learning*). La politique de confidentialité de Respondus[160] indique qu'il n'y a pas d'algorithme qui analyse les cartes d'identité des étudiants depuis la base de données avec les entrées de l'étudiant, ce qui signifie qu'il n'y a pas de dispositif de reconnaissance faciale. La comparaison entre la photo sur la pièce d'identité et la personne qui passe l'examen est faite manuellement par l'enseignant pendant sa révision des enregistrements.

Respondus Monitor utilise un logiciel d'intelligence artificielle (IA), afin de signaler aux professeurs les vidéos présentant des comportements douteux pendant les examens. Les enseignants examinent les signaux enregistrés pour détecter d'éventuelles tricheries ou d'autres problèmes liés aux tests. Les enregistrements sont scannés pour détecter les comportements suspects. Le site de l'Université d'Ottawa informe par exemple sur le fonctionnement de l'intelligence artificielle mise en œuvre par Respondus[161]. Les algorithmes détectent plus d'un visage qui apparaît dans la caméra, l'étudiant détournant le

[158] Respondus, *supra* note 72.
[159] Ella Lee, « DePaul sued over facial recognition tech used for online test proctoring » (8 mars 2021), en ligne : The DePaulia <https://depauliaonline.com/52893/news/depaul-sued-over-facial-recognition-tech-used-for-online-test-proctoring/>.
[160] Respondus, *supra* note 72.
[161] Université d'Ottawa, *supra* note 85.

regard de l'axe de la caméra, l'étudiant qui éteint la webcam, ainsi que d'autres activités suspectes décrites en détail ci-dessous :

- **Absence d'image** - l'étudiant ou l'étudiante n'a pas pu être détecté temporairement par la caméra pendant l'examen ;
- **Personne différente dans l'image** - une personne différente de celle qui a commencé l'examen peut avoir été détectée temporairement par la caméra Web ;
- **Plusieurs personnes dans l'image** - plusieurs visages sont détectés temporairement par la caméra ;
- **Interruption de l'internet** - une interruption de la caméra s'est produite à la suite d'une panne de l'Internet ;
- **Réduction de la fréquence d'images vidéo en raison de la qualité de la connexion Internet** - si une mauvaise bande passante est détectée avec la connexion Internet, la fréquence d'images de la caméra est automatiquement réduite
- **L'étudiant ou l'étudiante a quitté le navigateur LockDown de manière anticipée** - l'étudiant ou l'étudiante a manuellement mis fin à la session d'examen de manière anticipée; la raison fournie par l'étudiant est alors indiquée ;
- **Détection faciale faible** - la détection faciale n'a pas pu être réalisée pendant de longues minutes pendant l'examen ;
- **La caméra Web a été déconnectée** - la caméra Web a été déconnectée de l'ordinateur pendant l'examen ;
- **La caméra Web a été connectée** - la caméra web a été connectée à l'ordinateur pendant l'examen ;
- **Une tentative de passage à un autre écran ou à une autre application** - indique qu'une combinaison de touches ou un balayage de commutation d'application a été tenté ;
- **Session vidéo terminée prématurément** - indique que la session vidéo s'est terminée de manière inattendue et qu'elle ne s'est pas automatiquement reconnectée avant que l'étudiant ait terminé l'examen ;
- **Échec de la vérification de la détection faciale** - la détection faciale n'a pas pu être réalisée pendant la partie de vérification de la détection faciale de la séquence de démarrage ;
- **L'étudiant a désactivé les alertes de détection faciale** - l'étudiant a sélectionné « Ne plus montrer cette alerte » lorsque l'alerte de détection faciale est apparue pendant l'évaluation. L'étudiant n'a plus reçu d'alertes après cela.

L'Université d'Ottawa[162] indique ainsi que Respondus Monitor ne met pas en œuvre un procédé de reconnaissance faciale mais utilise un outil d'intelligence artificielle. Le recours à la reconnaissance faciale est non seulement inquiétant pour la vie privée mais génère aussi de nombreuses questions sur la fiabilité des systèmes, sur les risques d'erreurs et de ne pas reconnaître les peaux sombres, conduisant alors à des risques de discrimination. En outre, l'efficacité du dispositif peut être interrogée. Il est ainsi précisé aux enseignants que Respondus Monitor utilise de nombreux facteurs pour déterminer quelles vidéos d'étudiants doivent être signalées. Mais cet outil est incapable de déterminer quelles vidéos

[162] Université d'Ottawa, *supra* note 85.

signalées sont réellement dignes d'intérêt de la manière dont un professeur pourrait le faire. Ces indicateurs sont destinés à être utilisés à titre indicatif, mais l'enseignant doit s'attendre à un nombre important de faux indicateurs (faux positifs). Il doit alors vérifier tous les points douteux présentés par cet outil. Cependant, il faut souligner que la surveillance des examens en personne n'est elle-même pas non plus parfaite. Elle peut aussi mener à des instances de tricherie manquée ainsi qu'à des instances de fausses accusations[163]

Surtout, les finalités ici énumérées doivent nous interroger. Les entreprises technologiques envisagent des finalités larges et bien différentes des finalités pour lesquelles les données ont été collectées par les universités, en lien avec leurs missions. Les procédés de traitements algorithmiques et l'apprentissage automatique sont mis en œuvre pour détecter les comportements de tricherie pour assurer l'intégrité des examens mais les données ainsi collectées pourront ensuite être réutilisées comme données d'apprentissage de ces systèmes pour d'autres usages dans des contextes différents, allant bien au-delà des missions des organismes publics d'enseignement. Il y a là un usage secondaire pour une finalité différente. En outre, seules les entreprises technologiques contrôlent le traitement de ces données. Elles déterminent les finalités des traitements et mettent les moyens, ce qui tend à faire d'elles les véritables responsables de leur mise en œuvre, et non plus les universités.

Il faut noter par ailleurs que le fait d'autoriser la réutilisation des données constitue à l'évidence un avantage concurrentiel important dans l'amélioration des services d'exploration des données et de reconnaissance faciale proposés par les entreprises technologiques. Les données sont nécessaires au fonctionnement de l'intelligence artificielle et à l'amélioration des algorithmes au-delà des finalités initiales de surveillance d'examen. Les traitements des données peuvent ainsi être réalisés à des fins purement commerciales. On le voit, les données sont collectées dans un contexte spécifique suivant une finalité déterminée mais il est contractuellement permis de les utiliser pour d'autres finalités qui sortent amplement des missions universitaires. Ce faisant, alors que les données ont été collectées pour un usage autorisé par les lois du secteur public, elles sont ensuite utilisées pour un usage commercial. Cette réutilisation des données à des fins d'entraînement et d'amélioration des outils dépasse le contexte de l'éducation et doivent relever des lois du secteur privé.

3.7. Risques de cybersécurité

Notons par ailleurs que le stockage des données sensibles, tant sur les serveurs des firmes que ceux des universités, peuvent être problématiques lorsqu'on envisage les risques de cyberattaques[164], d'autant quune hausse des cyberattaques a été constatée depuis le début de la pandémie. Si on prend l'exemple de Respondus, la sécurisation des données est assurée par le cryptage standard de l'industrie SSL (Secure Socket Layer) ou TLS (Transport Layer Security) pour transférer les informations. Selon les conditions d'utilisation de Respondus[165], les informations permettant d'identifier les étudiants, notamment le nom, la note, le nom du cours et les photos montrant les cartes

[163] Simon Coghlan, Tim Miller et Jeannie Paterson, *supra* note 4 à la p 10.
[164] *Ibid* à la p 8.
[165] Respondus, *supra* note 71.

d'identification, ne sont accessibles que par l'intermédiaire de l'architecture d'extension du système de gestion de l'apprentissage (LMS) (par exemple, Blackboard Building Block). Seuls les utilisateurs possédant une accréditation d'instructeur pour le cours du LMS (par exemple, les instructeurs, les assistants d'enseignement, les administrateurs du LMS) sont en mesure de visionner les sessions vidéo en conjonction avec les informations d'identification de l'étudiant. Les URL des vidéos sont "à usage unique" et ne fonctionneront pas si elles sont copiées. En outre, Respondus fait appel à des sociétés de sécurité tierces et indépendantes pour effectuer des « tests de pénétration » du système Respondus Monitor. Ces tests comprennent un examen de l'architecture de Respondus Monitor et des tests de vulnérabilité et d'exploitation.

Cependant, aucune transmission de données sur Internet n'est sécurisée à 100 % et Respondus ne garantit pas la sécurité des informations recueillies en utilisant ses services. En outre, Respondus indique que, en acceptant ces conditions, l'usager accepte d'utiliser Respondus Monitor à ses propres risques. Il accepte aussi que Respondus ne soit pas responsable si une faille de sécurité se produit, si le site fonctionne mal, ou si les informations sont mal utilisées ou mal gérées de quelque manière que ce soit au détriment des universités ou au détriment d'un étudiant ou d'un tiers, que ce soit par Respondus, l'établissement ou un tiers non autorisé.

Le risque de cybersécurité ne devrait pas peser sur les personnes concernées mais sur les organismes utilisateurs des données. Les lois de protection des renseignements personnels du secteur public requièrent que les organismes publics établissent et maintiennent des garanties de protection des données personnelles contre les risques de perte accidentelle des données ou d'altération, d'accès non autorisé, collecte, utilisation, divulgation ou destruction. Cette décharge de responsabilité est donc contraire aux obligations de sécurité des renseignements personnels posés par les lois. Rappelons en outre que le principe 7 de l'annexe 1 de la loi fédérale LPRPDE pour le secteur privé pose aussi des obligations de sécurité suivant la sensibilité de l'information.

3.8. Qualification des responsables

Pour aller plus loin dans l'analyse des différentes utilisations des données personnelles et des responsables de traitement, il convient de préciser les rôles joués par les universités et les entreprises technologiques. Par exemple, suivant la politique de confidentialité de ProctorU[166] : « Dans la plupart des contextes de traitement, ProctorU agit en tant que sous-traitant ou prestataire de services pour un établissement d'enseignement ou une entité de certification responsable du traitement ». Cependant, tel n'est pas le cas en toutes circonstances et en particulier quand il s'agit d'utiliser les données pour améliorer les outils d'exploration des données et de reconnaissance faciale. Dans ce cas, les universités ne contrôlent plus ces utilisations et n'en sont plus responsables. Les entreprises technologiques devraient l'être sur le fondement des lois du secteur privé, en particulier de la loi fédérale LPRPDE, dès lors que seules trois provinces (Québec, Colombie-Britannique et Alberta) disposent de leurs propres législations.

[166] ProctorU «Privacy Policy » (s.d.) en ligne : *ProctorU* <https://www.proctoru.com/privacy-policy>.

Cette interprétation est confirmée par les entreprises technologiques européennes qui sont soumises au RGPD. Ces dernières font une différence selon leurs activités et admettent être sous-traitantes ou responsables de traitement suivant les traitements. Par exemple, ProctorExamen[167], entreprise européenne basée aux Pays-Bas indique agir au titre de « responsable de traitement », dès lors que les données sont traitées en dehors de l'activité de test elle-même. Il en est de même de Proctorio[168] qui distingue deux activités sur son site internet selon les traitements : « Proctorio est un sous-traitant lorsque Proctorio surveille un examen, vérifie les identités, protège le contenu ou vérifie l'originalité d'un devoir ». Dans ces cas, c'est l'université qui contrôle les informations et non Proctorio. Mais parallèlement, Proctorio est un responsable de traitement lorsque les étudiants ont directement saisi des informations personnelles dans un formulaire sur le site Web de Proctorio ou lorsqu'ils fournissent directement des informations personnelles par le biais des services clients et/ou produits de Proctorio. Rien n'est indiqué dans l'hypothèse d'utilisation des données à des fins d'entraînements algorithmiques mais on peut considérer que ce type de traitement échappe au contrôle des universités et tombe sous la responsabilité des entreprises technologiques en tant que responsable de traitement, dès lors que ces entreprises définissent les finalités et les moyens des traitements.

On voit pourtant des entreprises qui cherchent à rejeter toute responsabilité. Respondus indique sur son site[169] que : « en termes de GDPR, le service Respondus Monitor est un " sous-traitant " de vos informations personnelles ; l'établissement de licence (par exemple, l'université) est le " contrôleur " des informations personnelles recueillies et traitées. Cela signifie que nous fournissons la technologie permettant de stocker et d'analyser les données, mais que l'institution qui délivre les licences (par exemple, les instructeurs et les administrateurs) contrôle l'utilisation réelle des données ». Si cette analyse est correcte pour une partie des activités menées par ces entreprises, elle ne l'est pas pour toutes et en particulier en cas d'utilisation secondaire des données.

3.9. Transferts internationaux de renseignements personnels vers les États-Unis

Dans sa politique de confidentialité[170], Respondus indique que si les étudiants se connectent aux services à partir d'un pays autre que celui où se trouvent les serveurs, les communications peuvent entraîner le transfert des données personnelles au-delà des frontières internationales. Il en est de même lorsqu'une assistance est fournie à partir d'un des sites mondiaux en dehors du pays d'origine.

Le site de l'université d'Ottawa[171] indique clairement que les renseignements personnels peuvent être stockés à l'extérieur du Canada et soumis aux lois de la juridiction où ils sont stockés, ce qui n'est pas contraire à la loi de l'Ontario sur l'accès à l'information et la protection de la vie privée. Mais plus encore, dans sa politique de vie privée, Respondus indique utiliser des serveurs AWS (c'est-à-dire Amazon Web Services) situés aux États-

[167] ProctorExam, *supra* note 44.
[168] Proctorio en ligne : Proctorio <https://proctorio.com/privacy>.
[169] Respondus, « Additional Privacy Information - Respondus Monitor » (s.d.) en ligne : *Respondus* <https://web.respondus.com/privacy/privacy-additional-monitor/>.
[170] Respondus, "Respondus Privacy Policy", en ligne : https://web.respondus.com/privacy-policy/.
[171] Université d'Ottawa, *supra* note 85.

Unis[172]. Selon les conditions contractuelles de Respondus[173], toutes les questions juridiques découlant ou liées à l'utilisation de Respondus Monitor doivent être interprétées conformément aux lois de l'État de Washington, sans tenir compte des principes de conflits de lois.

ProctorExam, mis en œuvre par Polytechnique Montréal[174], est une société néerlandaise régie par le Règlement général sur la protection des données (« RGPD »). Elle précise sur son site internet quelles sont les personnes pouvant avoir accès aux données[175]. Elle indique que le personnel autorisé par l'institution académique peut accéder à certaines parties des données, ainsi que le personnel de ProctorExam mandaté par l'institution. ProctorExam fait également appel à d'autres sociétés pour fournir son service. Toutefois, ProctorExam indique rester responsable de la manière dont les tiers traitent les données. Ainsi, les tiers concernés sont : Amazon Web Services qui stocke physiquement les données dans des centres de données situés dans l'Union européenne ; Google Cloud qui stocke également les données dans des centres de données situés dans l'Union européenne. L'obligation de conservation des données sur le territoire européen satisfait les exigences du droit de l'Union européenne.

Cependant, ProctorExam indique aussi que « si l'établissement a donné son accord, nous pouvons également utiliser des solutions tierces pour traiter certaines données ». Or, Polytechnique Montréal indique sur son site internet que la firme de surveillants mandatée par ProctorExam pour effectuer la révision des examens est basée aux États-Unis. Les données sont donc transférées du Canada vers l'Europe puis vers les États-Unis. Les flux internationaux de données en provenance de l'Union européenne sont soumis à des règles restrictives d'adéquation de la protection (art. 41 et s. du RGPD) mais rien n'est dit sur le respect de ces obligations légales. On ne sait pas en particulier quel est le fondement légal du transfert. Cela pourrait supposer en particulier le respect d'obligations contractuelles, telles les clauses contractuelles type adoptées par la Commission pour garantir un certain niveau de protection.

Examity[176], utilisé par l'université de Toronto[177], indique que « la Plateforme d'Examity est hébergée et exploitée aux États-Unis (" US "). Sauf si vous avez été informé autrement, en utilisant la Plateforme, vous consentez au transfert de vos informations personnelles aux États-Unis. Si vous accédez à la plate-forme à partir de l'extérieur des États-Unis, veuillez noter que le droit américain peut ne pas offrir les mêmes protections de la vie privée que le droit de votre juridiction ». Le site Examity renvoie en outre à un document intitulé « European Union and European Economic Area Resident Privacy Notice »[178] qui renvoie

[172] Respondus, *supra* note 125.
[173] Respondus, *supra* note 71.
[174] Polytechnique Montréal, *supra* note 45.
[175] Proctorexam, *supra* note 44.
[176] Exmity, *supra* note 42.
[177] University of Toronto, « How does online proctoring work? » (s.d.), en ligne : *University of Toronto,* <https://help.learn.utoronto.ca/hc/en-us/articles/115004994514-How-does-online-proctoring-work->.
[178] Examity, « Product Privacy Policy Appendix B », (s.d.), en ligne : *Examity* <https://www.examity.com/product-privacy-policy-appendix-b/>.

toutefois à l'accord bilatéral conclu entre l'Union européenne et les États-Unis dit « Privacy Shield » invalidé par la Cour de justice de l'Union européenne en 2020[179] !

Par ailleurs, il faut noter que si la loi du secteur public de l'Ontario n'impose pas d'obligation de stocker les données personnelles sur le territoire canadien, d'autres provinces ont au contraire adopté des règles restrictives en la matière comme la Colombie britannique[180] et la Nouvelle Écosse[181]. L'Alberta[182] impose une obligation d'information dans l'hypothèse d'un transfert international des données hors Canada. Au Québec, la réforme de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels par la loi 25 adoptée en septembre 2021[183] prévoit désormais que :

> « Avant de communiquer à l'extérieur du Québec un renseignement personnel, un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée. Il doit notamment tenir compte des éléments suivants : 1° la sensibilité du renseignement ; 2° la finalité de son utilisation ; 3° les mesures de protection, y compris celles qui sont contractuelles, dont le renseignement bénéficierait ; 4° le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.
>
> La communication peut s'effectuer si l'évaluation démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus. Elle doit faire l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.
>
> Il en est de même lorsque l'organisme public confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement ».

Rappelons que si la loi fédérale LPRPDE du secteur privé n'interdit pas le stockage des renseignements personnels en dehors du Canada, le Commissariat à la protection de la vie privée a à plusieurs reprises imposé une obligation d'information des personnes concernées sur le lieu de stockage[184].

---

[179] CJUE, 16 juil., 2020, aff. C-311/18, DPC c. Facebook et Schrems, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62018CJ0311&from=FR>.
[180] British Colombia: Freedom of Information and Protection of Privacy Act (FIPPA), R.S.B.C. 1996, c. 165.
[181] Nova Scotia: Personal Information International Disclosure Protection Act (PIIDPA), Chapter 3 of the Acts of 2006 amended 2010, c. 35, s. 43.
[182] Alberta: Personal Information Protection Act (PIPA), S.A. 2003, c. P-6.5.
[183] Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c 25.
[184] Par exemple : PIPEDA Case Summary #2005-313.

4. PROBLÈMES JURIDIQUES MAJEURS NON RÉSOLUS

L'analyse juridique précédente a révélé des problèmes majeurs dans la protection des renseignements personnels qui dépassent le cas particulier de leur utilisation dans le contexte de logiciels de surveillance d'examens. Il en est ainsi : des conditions de recueil du consentement (1), de la distinction entre les lois des secteurs privé et public (2), de la localisation des données aux États-Unis en présence d'entreprises américaines (3), des clauses d'élection du for (4) et enfin de l'extension des finalités à des fins d'entraînement des algorithmes (5).

4.1. Faiblesse d'un consentement peu libre, peu éclairé et non distinct

Les contrats conclus entre les étudiants et les entreprises technologiques[185] soulèvent de nombreuses questions. D'abord, ce sont des contrats d'adhésion qui ne font pas l'objet de négociation de la part des étudiants, placés dans une situation d'infériorité, sous le stress d'accepter l'utilisation des outils de surveillance au moment de passer leur examen.

Ensuite, le consentement au contrat lui-même n'est pas véritablement libre[186] puisque les étudiants sont placés dans la nécessité de devoir passer l'examen et d'accepter les conditions prévues par les enseignants. Même si certaines universités prévoient des solutions alternatives à l'utilisation de ces moyens automatiques de surveillance, le choix de refuser d'utiliser les technologies entraîne une rupture d'anonymat et potentiellement d'égalité. Dès lors que les étudiants ne seraient plus placés dans les mêmes conditions, ils pourraient difficilement subir exactement le même examen et ils pourraient se sentir contraint d'accepter l'outil de surveillance. On peut noter toutefois des efforts de certaines universités pour recueillir un consentement qui serait « libre et éclairé », comme l'Université Laval par exemple[187].

Enfin et surtout, ce consentement manifeste une acceptation pour deux objets différents : l'utilisation des logiciels et la collecte des renseignements personnels. Le consentement à la collecte des renseignements personnels n'est donc pas distinct du consentement au contrat. À l'heure actuelle, la plupart des lois au Canada n'exigent pas un consentement séparé, ce qui constitue une faiblesse de la protection des renseignements personnels.

---

[185] Voir par exemple l'université du Manitoba qui met en œuvre Respondus Monitor et indique clairement sur son site internet que les professeurs doivent informer leurs étudiants à qui il sera demandé « d'accepter les conditions de service, d'installer et de configurer les applications sur leurs ordinateurs et de se familiariser avec leur utilisation. Veuillez-vous assurer que vos élèves ont accès aux informations et aux ressources dont ils ont besoin pour se préparer bien avant tout quiz, test ou examen avec LockDown Browser ou LockDown Browser + Monitor activé », voir University of Manitoba, *supra* note 37.

[186] La qualité du consentement donnée par les étudiants requiert une évaluation quant aux normes du consentement qui émanent des régimes de droit privé canadien, puisque l'étudiant est obligé d'accepter les termes de conditions afin d'accéder à son examen.

[187] Université Laval, Consentement libre et éclairé, (s.d.) en ligne : *Université Laval* <https://www.enseigner.ulaval.ca/sites/default/files/consentement_a_lutilisation_de_proctorio.pdf >.

Toutefois, on peut noter une tendance au renforcement des exigences, peut-être sous l'influence du droit de l'Union européenne (article 4.11 du RGPD)[188]. Ainsi, l'article 8 de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* au Québec (2021, chapitre 25), dite loi 25, modifie la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1). Est inséré un article 53.1, selon lequel

> « un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé ».

Ces exigences nouvelles sont à saluer. Appliquées aux logiciels de surveillance d'examen, elles permettraient aux étudiants d'accepter l'utilisation des logiciels de surveillance pour pouvoir passer leur examen, tout en refusant, s'ils le souhaitent, la collecte et l'utilisation de leurs renseignements personnels. Certes, il ne serait pas possible de refuser la collecte et l'utilisation des renseignements directement utiles à l'opération de surveillance mais le refus signifierait que ces opérations ne seraient permises qu'à des fins strictement nécessaire à l'activité de surveillance à l'exclusion de toute autre finalité. En particulier, ne serait pas autorisée l'utilisation des renseignements personnels pour entraîner les algorithmes. Les entreprises technologiques seraient alors dans l'obligation d'obtenir un consentement explicite des personnes concernées pour réaliser de tels traitements sur leurs données.

4.2. Partenariats public-privé, lois sectorielles du public et du privé

La mise en œuvre par les universités de logiciels de surveillance d'examens proposés par des entreprises privées pose la question de l'impact d'un partenariat public-privé sur la protection des renseignements personnels. Ce faisant, la diversité des acteurs concernés par la collecte et l'échange des renseignements personnels va interroger sur l'application plurale des lois du secteur public mais aussi éventuellement du secteur privé.

Ainsi, si l'utilisation des logiciels de surveillance d'examens par les universités est régie par les lois provinciales du secteur public, applicables aux relations entre les universités et les étudiants, ainsi qu'aux relations entre les universités et les entreprises, la question se pose s'agissant des relations contractuelles entre les étudiants et les entreprises technologiques. On peut ainsi identifier trois types de relations contractuelles différentes qui sont interconnectées sans être totalement dépendantes les unes des autres, s'agissant du régime de protection des renseignements personnels. Les relations entre les étudiants et les entreprises technologiques seront partiellement régies par les règles du secteur privé puisque ce contrat ne fait pas intervenir un organisme public et qu'il a été constaté que les

[188] Le « consentement » de la personne concernée est « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

entreprises privées ne se contentent pas d'agir comme sous-traitant des universités publiques eu égard à certaines de leurs activités.

Seules trois provinces (Colombie-Britannique, Alberta et Québec) ont adopté des lois de protection des renseignements personnels du secteur privé, aussi faut-il alors s'en remettre à la loi fédérale du secteur privé, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Il est alors douteux que cette loi soit suffisamment protectrice, eu égard aux enjeux soulevés.

4.3. Entreprises américaines et localisation des données

La plupart des entreprises qui mettent sur le marché des logiciels de surveillance d'examen sont des entreprises américaines, ce qui pose la question du lieu de localisation des renseignements personnels, ainsi que celle de la loi applicable au contrat. La plupart d'entre elles imposent dans leurs conditions contractuelles le transfert des données sur le territoire des États américains. La plupart d'entre elles utilisent des services de cloud et en particulier les services d'Amazon aux États-Unis (AWS).

Cependant, s'agissant de la localisation des données, il faut noter que la plupart des lois sur les renseignements personnels du secteur public et privée au Canada n'exigent pas d'obligation de conservation de ces renseignements sur le territoire canadien, à l'exception de certaines lois provinciales précitées. Dès lors, il n'est pas étonnant de constater que les pratiques et les choix faits par les universités soient différents. L'Université Laval qui utilise Proctorio indique aux étudiants que les données sont stockées au Canada[189]. À l'inverse, l'Université d'Ottawa indique que les données sont stockées sur les serveurs de Respondus Monitor et la politique de confidentialité de ce dernier précise que Respondus utilise les serveurs d'AWS (Amazon Web Services) situés aux États-Unis[190]. Une telle solution est compatible avec la loi ontarienne du secteur public, alors que les universités d'autres provinces comme la Colombie-Britannique par exemple subit d'autres contraintes.

4.4. Entreprises américaines et clause d'élection du for

Quant à la loi applicable au contrat, elle relève des règles du conflit de loi et concerne le contrat conclu entre les étudiants et les entreprises technologiques. Ces relations contractuelles entre personnes privées sont soumises aux législations de protection des renseignements personnels du secteur privé. Cependant, les contrats d'adhésion imposés aux étudiants par les entreprises technologiques désignent la loi applicable au contrat sans leur laisser le choix. Les entreprises américaines prévoient dans leurs contrats l'application de la loi de l'État américain dans lequel elles ont leur siège social, excluant conséquemment l'application des lois canadiennes du secteur privé, qu'elles soient provinciales ou fédérales.

De son côté, la LPRPDE n'a pas de compétence extraterritoriale. Cependant, les entreprises technologiques américaines ne sont pas situées au Canada mais y opèrent, aussi l'enjeu est-il de savoir si le droit canadien pourrait néanmoins s'appliquer et si un lien de rattachement

[189] *Ibid*.
[190] Respondus, *supra* note 125.

pourrait être reconnu. Selon la jurisprudence, la LPRPDE s'applique aux organismes situés à l'extérieur du Canada, lorsqu'il existe des « liens réels et substantiels » avec le Canada[191].

Les facteurs de rattachement pertinents pour déterminer ces liens découlent notamment des facteurs énoncés dans la décision *A.T. c. Globe24h*[192] :
1) l'emplacement du public cible du site Web,
2) la source du contenu du site Web,
3) l'emplacement de l'opérateur du site Web et
4) l'emplacement du serveur hôte.

Par application de cette jurisprudence, un juge qui serait saisi du respect des lois sur la protection des renseignements personnels dans le contexte de l'utilisation d'un logiciel de surveillance d'examen pourrait vouloir se prévaloir de cette jurisprudence et, ce faisant, parvenir à appliquer les lois canadiennes. En outre, d'autres jurisprudences peuvent être utiles pour contester l'application de la clause d'élection du fort. Il en est ainsi de la jurisprudence relative à la compétence judiciaire dans un contexte numérique concernant des affaires visant un consommateur. Ainsi, dans l'affaire *Douez v. Facebook* (2017), la Cour a rejeté les efforts de Facebook pour bloquer un recours collectif en matière de protection de la vie privée exercé en Colombie-Britannique parce que ses propres conditions d'utilisation spécifiaient que les actions en justice devaient être intentées en Californie. La majorité a décidé que la clause ne devait pas être appliquée, compte tenu de l'inégalité du pouvoir de négociation entre les consommateurs et Facebook[193], combinée à l'importance du droit à la vie privée. Plus spécifiquement, l'inégalité flagrante de pouvoir de négociation entre les parties est perceptible, considérant notamment le fait que : (i) le contrat d'adhésion en ligne entre un consommateur individuel et une grande entreprise est présenté aux consommateurs sur une base "à prendre ou à laisser". Or, le choix de rester "hors ligne" n'est pas un choix réel à l'ère d'Internet.

S'agissant des logiciels de surveillance d'examen, l'inégalité est accrue par le fait que les étudiants n'aient pas le choix de ne passer l'examen à moins de décider d'échouer ou d'accepter des alternatives pas toujours clairement proposées et sources d'inégalité de traitement. En outre, le déséquilibre est renforcé du fait que les étudiants découvrent

---

[191] *Lawson c. Accusearch Inc.*, 2007 CF 125, para. 38 à 51; *A.T. c. Globe24h.com*, 2017 CF 114 (CanLII), [2017] 4 RCF 310, paragraphes 50 à 64, citant l'arrêt *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. Canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 RCS 427, aux paragraphes 54 à 63.

[192] *A.T. c. Globe24h.com*, 2017 CF 114 (CanLII), [2017] 4 RCF 310.

[193] Notons que la doctrine de l'iniquité vient du tribunal de l'équité en Angleterre et est utilisée pour écarter les accords injustes qui ont résulté d'une inégalité de pouvoir de négociation. L'objectif de cette doctrine est de protéger les personnes vulnérables dans le processus de passation des marchés contre les pertes résultant de l'accord injuste qui a été conclu. La doctrine exige à la fois une inégalité de pouvoir de négociation et un accord "déraisonnable" qui en résulte. Les contrats types ont un grand potentiel pour créer une inégalité de pouvoir de négociation et peuvent potentiellement renforcer l'avantage de la partie la plus forte au détriment de la partie la plus vulnérable. En particulier, les clauses qui imposent le choix de la loi, élection du for et les clauses d'arbitrage forcé violent les attentes raisonnables d'une partie en la privant de recours possibles. Tel est certainement le cas s'agissant des étudiants plus ou moins contraints d'accepter l'utilisation des logiciels de surveillance et le contrat qui s'y applique.

souvent les conditions générales d'utilisation des entreprises « à prendre ou à laisser » au moment de passer leur examen et ne peuvent s'informer avant d'accepter. Le rejet de la clause d'élection du for en raison du déséquilibre qu'elle créée pourrait donc s'envisager aisément dans le contexte des logiciels de surveillance d'examen.

Un autre facteur de la décision *Douez* suggère que la clause d'élection du for ne devrait pas être appliquée, en raison de problèmes pratiques de commodité et des coûts d'un litige dans la juridiction désignée par le contrat. Ainsi, les dépenses et les inconvénients liés au fait d'obliger les Britanno-Colombiens à plaider en Californie, comparés aux dépenses et aux inconvénients de Facebook, rendent plus pratique la mise à disposition des documents par Facebook pour inspection en Colombie-Britannique plutôt que d'obliger Mme Douez à se rendre en Californie pour faire valoir sa demande. Ce raisonnement pourrait aussi s'appliquer par analogie au cas des entreprises proposant des logiciels de surveillance d'examen.

Également, il est pertinent de rappeler l'enquête récente sur Clearview AI[194]. Cette entreprise américaine offrait les prestations d'un logiciel de reconnaissance faciale aux services de police sur le territoire canadien en mobilisant une base de données conçue à partir de milliard d'images en provenance des réseaux sociaux. La base de données inclut des images des Canadiens obtenues sans leur consentement express préalable. L'enquête conjointe, menée par le Commissariat à la vie privée du Canada et les Commissaires de la Colombie-Britannique, de l'Alberta et du Québec, a conclu que les activités de Clearview AI sur le territoire canadien représentent « des liens réels et substantiels avec le Canada »[195], ce qui a pour effet de donner application à la LPRPDE et aux lois provinciales du secteur privé. En application de cette loi, le Commissariat à la protection de la vie privée du Canada a pu conclure à la violation du principe du consentement.

Si le consentement des étudiants est bel et bien obtenu par les entreprises technologiques de surveillance d'examen, le raisonnement mis en œuvre dans cette affaire est toutefois utile s'agissant de la loi applicable afin de donner effet aux lois canadiennes. Dès lors, on peut considérer que le cas d'utilisation des logiciels de surveillance d'examen par des universités canadiennes conduisant à collecter des renseignements personnels d'étudiants situés au Canada devrait entraîner la mise en œuvre du droit canadien, non seulement dans les relations entre les universités et les entreprises (lois provinciales du secteur public applicables) mais aussi dans les relations entre les entreprises et les étudiants (lois provinciales et fédérale du secteur privé applicables). Une telle solution peut être déduite à l'heure actuelle de la jurisprudence mais il serait souhaitable qu'elle relève de la loi pour garantir une meilleure protection et sécurité juridique. Une réforme de la LPRPDE devrait

[194] Commissariat à la protection de la vie privée du Canada, Enquête conjointe sur Clearview AI, inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta - 2 février 2021, [Enquête sur Clearview AI], en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/>.
[195] Ibid, au para 28.

conduire à étendre son champ d'application territorial. Une solution législative éviterait l'aléa, le temps perdu et le coût d'un recours judiciaire.

Plus encore, tant dans l'affaire Clearview AI que dans le cas des logiciels de surveillance d'examen, est concernée la collecte de renseignements personnels de nature biométrique lors de leur processus de détection algorithmique. Or, selon l'enquête sur Clearview AI, les renseignements biométriques faciaux sont des renseignements « intrinsèquement liés à la personne »[196] et sont « particulièrement sensibles »[197]. Ce constat conduit à vouloir redoubler de moyens de protection et à rendre la loi canadienne applicable.

4.5. Entraînement des intelligences artificielle (IA) et défaut de transparence

Les entreprises technologiques proposant des outils de surveillance d'examens mettent en œuvre des solutions en intelligence artificielle, qu'il s'agisse de procédés de fouille de données ou de moyens de reconnaissance faciale. Pourtant, cet état de fait n'est pas toujours clairement indiqué comme tel. Proctorio affirme par exemple que ses techniques algorithmiques sont supérieures et plus efficaces à la surveillance humaine pour combler les biais et les erreurs humaines et détecter la tricherie. Il indique aussi sa capacité à s'améliorer temporellement, ce qui sous-entend seulement l'utilisation de dispositifs d'apprentissage automatique sans que cela soit clairement annoncé.

Les entreprises de logiciels de surveillance d'examen à distance devraient être plus transparentes quant au produit offert et aux méthodes mobilisées. En outre, le terme logiciel de surveillance (« *proctoring software* ») comprend une diversité d'outils et de techniques qui sont pourtant offerts sous le même nom, ce qui est trompeur pour les étudiants mais aussi pour les universités.

Le fonctionnement des logiciels de surveillance demeure, en grande partie, inconnu, ce qui est problématique pour les universités qui doivent assurer un certain contrôle sur les évaluations académiques et les méthodes mobilisées pour assurer l'intégrité académique. Les concepteurs de logiciels de surveillance ne font pas preuve de transparence envers les universités et, conséquemment, il existe une lacune vis-à-vis de la clarté et de l'interprétation des rapports, ainsi qu'une connaissance limitée quant à la fonctionnalité de ces logiciels conduisant à une diminution de contrôle sur les logiciels par le personnel universitaire[198].

En tout état de cause, il existe un défaut de transparence sur la nature et la quantité de renseignements personnels collectés, tout comme sur les systèmes d'IA mis en œuvre et leurs caractéristiques.

---

[196] *Ibid* au para 41
[197] *Ibid*.
[198] Neil Selwyn et al, *supra* note 9 aux pp 12-13.

5. CONCLUSION SOUS FORME DE RECOMMANDATIONS

Afin de prendre en considération les problématiques juridiques non résolues, plusieurs recommandations doivent être faites. Elles concernent essentiellement la loi LPRPDE et sont particulièrement utiles dans le contexte de projets de réforme. Il est à noter que les problèmes ici considérés n'étaient pas pris en compte dans le projet de loi C-11, aussi est-il indispensable de tenir compte de ces enjeux et, dans la mesure du possible, des propositions ici faites. Les futures propositions législatives retiendront l'attention.

Cinq recommandations majeures sont faites ici pour considérer des problèmes récurrents dans la mise en œuvre de la LPRDE, allant bien au-delà du cas des logiciels de surveillance d'examens.

5.1. Recommandation 1 : renforcer les conditions de consentement dans la LPRPDE

Si la mise en œuvre des logiciels de surveillance d'examen par les universités et la collecte des renseignements personnels se fait avec le consentement des étudiants, on a amplement vu que les conditions de recueil de ce consentement fragilise la protection voulue par la loi.

Dans le contexte d'application de la LPRPDE, il est nécessaire d'affirmer que :

« la collecte et le traitement des renseignements personnels doit nécessiter le recueil d'un consentement libre, éclairé et distinct de tout autre consentement ».

5.2. Recommandation 2 : revoir l'articulation des lois du secteur public /privé et la qualification des responsables

Alors que le droit, fédéral et provincial, canadien s'articule autour d'une distinction majeure entre le secteur public et le secteur privé, la mise en œuvre par des acteurs publics de technologies en tous genres, proposées par des entreprises privées, vient fragiliser cette distinction. La conclusion de contrats de licences par lesquels les entreprises privées collectent et réutilisent des renseignements personnels pour des usages différents de ceux pour lesquels ils ont été collectés à l'origine par les acteurs publics vient perturber la compréhension des missions publiques et le rôle joué par chacun. Partant, la qualification des parties et le partage des responsabilités dans un contexte de sous-traitance et d'utilisation secondaire des données par le sous-traitant doivent être clarifiés.

Il est nécessaire de mieux qualifier les acteurs publics et privés, responsables du respect des législations sur la protection des renseignements personnels. En cas de sous-traitance de certaines tâches administratives réalisées auprès d'entreprises privées proposant des solutions technologiques, il convient de préciser les responsabilités et les caractéristiques du sous-traitant qui doit agir au nom et pour le compte des acteurs publics. Dans l'hypothèse d'un usage secondaire des données par le sous-traitant, il convient de prévoir d'engager sa responsabilité pour le traitement secondaire dont les finalités dépassent le traitement initial et dès lors qu'il définit les moyens et les finalités de ce traitement secondaire.

La réforme de la LPRPDE doit prévoir des règles de responsabilités claires du sous-traitant et du responsable de traitement comme principal responsable. Il est également possible de prévoir des obligations à la charge du responsable de traitement dans le choix de son sous-traitant.

5.3. Recommandation 3 : encadrer les flux internationaux de renseignements personnels hors Canada

Les flux internationaux des renseignements personnels sont particulièrement à risque pour le Canada, alors que de nombreux acteurs privés et publics situés sur le territoire canadien utilisent des technologies américaines proposées par des entreprises qui collectent les données personnelles et les transfèrent aux États-Unis. Non seulement le niveau de protection est souvent plus faible mais en outre les lois de protection des renseignements personnels ont des champs d'application matériels et territoriaux complexes et souvent très parcellaires. Les Canadiens risquent donc d'être moins protégés et d'ignorer leurs droits.

Dans un contexte où l'Union européenne (RPGD) et le Québec (loi 25) ont mis en œuvre des dispositions pour s'assurer du niveau de protection en cas de transfert international des données soit par une analyse d'adéquation du niveau de protection soit par une étude des facteurs sur la vie privée, la loi fédérale sur le secteur privé doit aussi prévoir une telle protection.

La réforme de la LPRPDE doit prévoir des règles imposant un contrôle de la protection accordée aux personnes avant le transfert international des renseignements personnels.

5.4. Recommandation 4 : renforcer l'effet extraterritorial de la LPRPDE

Un des enjeux majeurs concernant les outils de surveillance d'examen est de s'assurer que la protection des lois Canadiennes puisse être accordée aux personnes résidant sur le territoire Canadien, dès lors que l'activité initiale et la collecte des données afférente s'y trouve. À l'heure actuelle, le droit contractuel prime à défaut de règles législatives imposant le respect du droit canadien. Dans le cadre des contrats d'adhésion mis en œuvre le plus souvent par les entreprises technologiques, les clauses d'élection du for conduisent nécessairement à désigner les lois des États américains où sont situées ces entreprises.

À l'instar de l'article 3 du RGPD qui prévoit un effet extraterritorial du droit de l'Union européenne, dès lors que les données collectées l'ont été sur son territoire, le droit fédéral canadien doit s'imposer dans le contexte de collecte des renseignements personnels sur le territoire canadien. Une telle disposition devrait valoir largement, y compris dans le contexte des activités numériques sur internet.

La réforme de la LPRPDE doit prévoir une règle d'extraterritorialité pour imposer son respect, dès lors que les données sont collectées sur le territoire canadien.

5.5. Recommandation 5 : exiger une étude des facteurs sur la vie privée (PIA) pour évaluer des systèmes d'IA impliquant des renseignements personnels

Il faut noter que les études des facteurs sur la vie privée (EFVP) constituent des pratiques dont la mise en œuvre est de plus en plus généralisée dans les lois. La réforme récente des lois de protection des renseignements personnels au Québec (loi 25) en est une illustration.

Notons également que l'Université de Colombie-Britannique a mis en œuvre une telle étude pour analyse l'impact de Proctorio sur la vie privée des étudiants[199] avant de décider son abandon.

L'obligation de mettre en œuvre une telle étude dans certaines circonstances à risque devrait être imposée dans la réforme de la LPRPDE. Imposer la mise en œuvre d'une telle analyse serait particulièrement nécessaire en cas de recours à des outils d'intelligence artificielle qui reposeraient sur une collecte massive de renseignements personnels.

199 https://privacymatters.ubc.ca/sites/privacymatters.ubc.ca/files/PIA01007%20%20Summary%20Report%20-%20PROCTORIO.pdf.

ANNEXES

Tableau 1 sur la collecte de renseignements personnels des logiciels de surveillance d'examen[200]

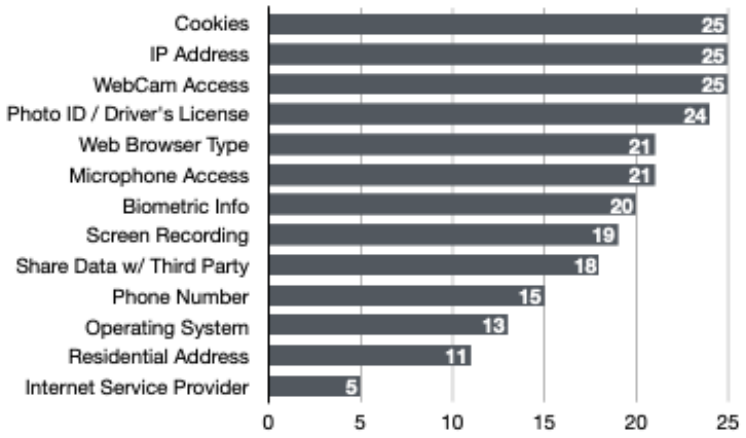

Figure 2: Data collection disclosed by exam proctoring services in their privacy policies ($n = 25$).

[200] (Balash et al, 2020, à la p.4) « Privacy Policies In addition to viewing permissions in the manifest file, we also reviewed the privacy policies of 25 exam proctoring services. […] Figure 2 presents the number of exam proctoring services (x-axis) that disclose certain data collection practices (y-axis). All 25 discuss setting cookies, collecting IP addresses, and accessing the webcam, and all but one note access to a photo ID to verify identity. Many policies also mention that the software will request access to the microphone, screen recordings, or collect other kinds of biometric information. Notably, 18 state that they share information with third parties. » - Balash et al, 2020, à la p.4

Tableau 2 sur l'utilisation de l'IA par les logiciels de surveillance d'examen[201]

Table 1. AI-based features in current proctoring platforms.

Tool	Face recognition	Motion detection	Anomaly detection	Behavioral analysis	Eye tracking	Voice detection
Mettl	Yes	–	Yes	Yes	Yes	Yes
ProctorU	Yes	–	Yes	Yes	–	–
Respondus	Yes	Yes	Yes	Yes	Yes	–
Examity	Yes	Yes	Yes	Yes	–	Yes
ProctorTrack	Yes	Yes	Yes	Yes	–	–
HonorLock	Yes	Yes	Yes	–	–	Yes

[201] Elshafey A.E., Anany M.R., Mohamed A.S., Sakr N., Aly S.G. (2021) Dr. Proctor: A Multi-modal AI-Based Platform for Remote Proctoring in Education. In: Roll I., McNamara D., Sosnovsky S., Luckin R., Dimitrova V. (eds) Artificial Intelligence in Education. AIED 2021. Lecture Notes in Computer Science, vol 12749 à la p 146, Springer, Cham. https://doi.org/10.1007/978-3-030-78270-2_26

Tableau 3 comparatif de logiciels de surveillance d'examen à distance (ProctorU, Respondus, Proctorio et AIProctor)[202]

Table 2: Evaluation matrix used in Phase 3

Proctoring Features	ProctorU	Respondus	Proctorio	AIProctor
Live human proctors available	Yes	No	**No**	No
Internet required	Yes	Yes	**Yes**	Yes
Secure/encrypted transferring of data	Yes	Yes	**Yes**	Yes
Student able to book exam time	Yes	Yes	**No**	Yes
Training provided	Yes	n/a	**Yes**	Yes
Proctoring provider certified	Yes	n/a	**Yes**	Yes
Students can interact with proctors	Yes	n/a	**Yes**	Yes
Student can message issues to proctors	Yes	n/a	**Yes**	No
Students get live exam instructions	Yes	n/a	**Yes**	No
Proctor able to see students screen	Yes	n/a	**Yes**	Yes
Stop proctor to view students screen	No	Yes	**n/a**	No
Recorded video reviewing option	No	Yes	**Yes**	No
Pause test/ cancel test	No	n/a	**Yes**	No
Automated proctoring	No	Yes	**Yes**	No
Keystroke checking	No	Yes	**Yes**	No
Audio recording	No	No	**Yes**	No
Browser lockdown	No	Yes	**Yes**	No
Authentication option	Yes	Yes	**Yes**	Yes
Web camera needed	Yes	Yes	**Yes**	Yes
Log reports	No	Yes	**Yes**	No
recording storage option	Yes	Yes	**Yes**	Yes
Test review option	No	Yes	**Yes**	No
Incident logs with date & time	No	Yes	**Yes**	No
Customising options for institution	No	Yes	**Yes**	No
Lockdown Features				
Available on both Windows and Mac	Yes	Yes	**Yes**	Yes
Plugin for browser	No	Yes	**Yes**	No
Avoids control options on the browser	No	Yes	**Yes**	No
Stops navigation (forward/back)	No	Yes	**Yes**	No
Stops concurrent tests	No	Yes	**Yes**	No
Stops right clicks using mouse	No	Yes	**Yes**	No
Stops printing	No	Yes	**Yes**	No

[202] Hussein, et al *supra* note 74 à la p 516.

Table 2: (Continued)

Proctoring Features	ProctorU	Respondus	Proctorio	AIProctor
Hides taskbar	No	Yes	**Yes**	No
Hides desktop	No	Yes	**Yes**	No
Stops minimising window	No	Yes	**Yes**	No
Stops maximising window	No	Yes	**Yes**	No
Stops copying & pasting	No	Yes	**Yes**	No
Stops other applications	No	Yes	**Yes**	No
Stops starting of other applications	No	Yes	**Yes**	No
Authentication options				
User required to authenticate	Yes	Yes	**Yes**	Yes
Username provided/required	Yes	Yes	**No**	Yes
Password provided/required	Yes	Yes	**No**	Yes
Student ID required	Yes	Yes	**Yes**	Yes
Keystroke analytics	No	No	**Yes**	No
Ability to do facial recognition	No	No	**Yes**	No
Ability to do voice recognition	No	No	**Yes**	No
Fingerprint scanning required	No	No	**No**	No
Iris scanner required/available	No	No	**No**	No
Webcam Features				
Web camera required	Yes	Yes	**Yes**	Yes
Room panning allowed	Yes	Yes	**Yes**	Yes

Tableau 4 : Tableau comparatif des fonctionnalités de Proctorio, Respondus LockDown Browser et Zoom[203]

	Proctorio* * Only to be used for accreditation purposes as of March 17, 2021. Learn more	Respondus LockDown Browser	Zoom
Platforms	Tablet, Desktop; PC, Apple, Linux, Chrome	Tablet, Apple; Desktop; PC	Tablet, PC; Desktop; Apple, Linux
Automated Authentication	✓	✗	✗
Live Authentication	✗	✗	✗
Automated Proctoring	✓	✗	✗
Live Proctoring	✗	✗	✓
Record Webcam/Microphone Feed	✓	✗	✗
Record Desktop Screen	✓	✗	✗
Record Web Traffic	✓	✗	✗
Record Physical Room	✓	✗	✗
Lock Down External Applications	✗	✓	✗
Disable Copying/Pasting of Text	✓	✓	✗
Disable New Tabs	✓	✓	✗
Disable Printing	✓	✓	✗
Force Completion of Exam	✓	✓	✗
Review Student Behaviour	✓	✗	✓
Live Chat Support	✓	✗	✗
Take Exams Remotely	✓	✗	✓
Free at UBC	✓	✓	✓
Canvas Supported	✓	✓	✓
FIPPA Compliant	✓	✓	✓

Icon Legend:
- Apple
- PC
- Linux
- Chrome
- Tablet
- Desktop

[203] The University of British Columbia, Faculty of Arts, Software for Securing & Proctoring Exams (s.d.), en ligne : <https://isit.arts.ubc.ca/software-for-securing-proctoring-exams/>.

BIBLIOGRAPHIE

Balash, David G., Kim, Dongkun, Shaibekova, Darika, Fainchtein, Rahel A., Sherr, Micah et Aviv, Adam J. (The George Washington University, Georgetown University) (2020), en ligne < https://arxiv.org/ftp/arxiv/papers/2106/2106.05917.pdf>.

Coghlan, Simon, Miller, Tim et Paterson, Jeannie, Good Proctor or "Big Brother"? AI Ethics and Online Exam Supervision Technologies, (2020), en ligne : <http://arxiv.org/abs/2011.07647v1>.

Hussein, Mohammed Juned et al. "An Evaluation of Online Proctoring Tools." Open Praxis, vol. 12, no. 4, International Council for Open and Distance Education (ICDE), 2020, pp. 509–25, en ligne <https://files.eric.ed.gov/fulltext/EJ1285031.pdf>.

Reisenwitz, T. H. (2020) 'Examining the Necessity of Proctoring Online Exams', Journal of Higher Education Theory & Practice, 20(1), pp. 118–124, en ligne : <https://articlegateway.com/index.php/JHETP/article/view/2782>.

Selwyn, Neil et O'Neill, Chris, Smith, Gavin, Andrejevic, Mark et Gu, Xin, « A necessary evil? The rise of online exam proctoring in Australian universities » 2021, 1-16, en ligne : <https://journals.sagepub.com/doi/pdf/10.1177/1329878X211005862>.

Slusky, Ludwig. "Cybersecurity of Online Proctoring Systems." Journal of International Technology and Information Management, vol. 29, no. 1, Jan. 2020, 56-86, en ligne : <https://www.semanticscholar.org/paper/Cybersecurity-of-Online-Proctoring-Systems-Slusky/80a084a512745c8b05c85a0870733d5cc435971c>.

Woldeab, Daniel et Brothen, Thomas (2021) Video Surveillance of Online Exam Proctoring: Exam Anxiety and Student Performance. International Journal of E-Learning & Distance Education, 36(1), 1–26, en ligne: <https://www.proquest.com/docview/2572618998?parentSessionId=zl%2BfEpWBBJvqZTbySIdGxUyimOQu0URzQYQ9uoPGi%2FY%3D&pq-origsite=primo&accountid=14701>.

Surveillance capitalistique, surveillance au travail

Ajunwa, Ifeoma and Crawford, Kate and Schultz, Jason, Limitless Worker Surveillance (March 10, 2016). Recommended Citation. Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, Limitless Worker Surveillance, 105 Cal. L. Rev. 735 (2017), Available at SSRN: https://ssrn.com/abstract=2746211

Vatcha, A., (2020). Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees. iSCHANNEL, 15(1), pp.4–9.

Bales, R. A., & Stone, K. V. (2020). The invisible web at work: Artificial intelligence and electronic surveillance in the workplace. Berkeley Journal of Employment and Labor Law, 41(1), 1-62.

Katsabian, Tammy (2020), The Telework Virus: How the COVID-19 Pandemic Has Affected Telework and Exposed Its Implications for Privacy and Equality. Available at SSRN: https://ssrn.com/abstract=3684702

Surveillance des étudiants :

Prévention de plagiat

Ross, J., & Macleod, H. (2018). Surveillance, (dis) trust and teaching with plagiarism detection technology. In M. Bajić, N. B. Dohn, M. de Laat, P. Jandrić, & T. Ryberg (Eds.), Proceedings of the 10th International Conference on Networked Learning. https://www.networkedlearningconference.org.uk/abstracts/papers/ross_25.pdf. Accessed 22 September 2020

Prévention des risques de suicide

Cyphert, Amy, Tinker-ing with Machine Learning: The Legality and Consequences of Online Surveillance of Students (May 2020). Nevada Law Journal, Vol. 20, 2020, WVU College of Law Research Paper No. 2020-007, Available at SSRN: https://ssrn.com/abstract=3602011

Risques d'attaques (shooting)

Fedders, Barbara, The Constant and Expanding Classroom: Surveillance in K-12 Public Schools (September 1, 2019). North Carolina Law Review, Vol. 97, No. 6, 2019, Available at SSRN: https://ssrn.com/abstract=3453358

Surveillance des professeurs

Edwards, Lilian and Martin, Laura and Henderson, Tristan, Employee Surveillance: The Road to Surveillance is Paved with Good Intentions (August 18, 2018). Available at SSRN: https://ssrn.com/abstract=3234382 or http://dx.doi.org/10.2139/ssrn.3234382

Notation des profs voir Cathy O'Neil

Reconnaissance faciale

Cavazos, J.G., Phillips, P., Castillo, C.D., & O'Toole, A. (2019). Accuracy comparison across face recognition algorithms: Where are we on measuring race bias? ArXiv, abs/1912.07398.

Mark Andrejevic & Neil Selwyn (2020) Facial recognition technology in schools: critical questions and concerns, Learning, Media and Technology, 45:2, 115-128, DOI: 10.1080/17439884.2020.1686014

- **Ses enjeux historiques et socio-ethniques**

  Damien Patrick Williams (2020): Fitting the description: historical and sociotechnical elements of facial recognition and anti-black surveillance, Journal of Responsible Innovation, DOI: 10.1080/23299460.2020.1831365

  Nance, J. (2016). Student Surveillance, Racial Inequalities, and Implicit Racial Bias.

  Opinion Article by Shea Swauger researcher at the University of Colorado Denver Software that monitors students during tests perpetuates inequality and violates their privacy | MIT Technology Review.pdf;

  https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/

- **Ses enjeux ethiques**

  Raji, Inioluwa & Gebru, Timnit & Mitchell, Margaret & Buolamwini, Joy & Lee, Joonseok & Denton, Emily. (2020). Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. 145-151. 10.1145/3375627.3375820.