Revue générale de droit

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 and Simon Robichaud-Durand

Volume 53, Number 1, 2023

URI: https://id.erudit.org/iderudit/1102332ar
DOI: https://doi.org/10.7202/1102332ar

See table of contents

Publisher(s)

Éditions Wilson & Lafleur, inc.

ISSN

0035-3086 (print)
2292-2512 (digital)

Explore this journal

Cite this article

Castets-Renard, C. & Robichaud-Durand, S. (2023). 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. *Revue générale de droit*, *53*(1), 207–245. https://doi.org/10.7202/1102332ar

Article abstract

While universities organized themselves during the pandemic to maintain the integrity of exams through, among other things, proctoring software, the continued use of these requires strengthening the protection of students' personal information. The current reform of the federal private sector law (Personal Information Protection and Electronic Documents Act) *is an opportunity to do so that should not be missed.*

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* et Simon Robichaud-Durand**

RÉSUMÉ

Alors que les universités se sont organisées pendant la pandémie pour maintenir l'intégrité des examens grâce notamment à des logiciels de surveillance, la poursuite de l'utilisation de ces derniers exige de renforcer la protection des renseignements personnels des étudiants. La réforme actuelle de la loi fédérale du secteur privé (Loi sur la protection des renseignements personnels et les documents électroniques) constitue une occasion de le faire à ne pas manquer.

MOTS-CLÉS :

Renseignements personnels, Loi sur la protection des renseignements personnels et les documents électroniques, *surveillance, pandémie de COVID-19, technologies de l'éducation.*

ABSTRACT

While universities organized themselves during the pandemic to maintain the integrity of exams through, among other things, proctoring software, the continued use of these requires strengthening the protection of students' personal information. The current reform of the federal private sector law (Personal Information Protection and Electronic Documents Act) *is an opportunity to do so that should not be missed.*

* Professeure, Faculté de droit civil de l'Université d'Ottawa, titulaire de la chaire de recherche Intelligence artificielle responsable à l'échelle mondiale.

** Étudiant à la maîtrise en droit et technologie, Faculté de droit de l'Université d'Ottawa, membre de la chaire de recherche Intelligence artificielle responsable à l'échelle mondiale.

Cette recherche a été financée par le « Programme des contributions » du Commissariat à la protection de la vie privée du Canada. Les auteurs remercient sincèrement le Commissariat. Le masculin pluriel a été utilisé pour désigner à la fois les hommes et les femmes. Le genre masculin a été adopté afin de faciliter la lecture, sans aucune intention discriminatoire.

KEYWORDS:

Personal information surveillance, Personal Information Protection and Electronic Documents Act, *COVID-19 pandemic, education technologies.*

SOMMAIRE

INTRODUCTION

De plus en plus de technologies sont utilisées dans le domaine de l'éducation *(Ed-Tech),* alors que ce secteur d'activité était déjà en plein essor avant même la pandémie. Les objectifs à atteindre sont variés : il peut s'agir de trier et sélectionner les candidats à l'entrée dans les universités ou grandes écoles ; de mesurer le rendement et la performance scolaire ; de déterminer les résultats finaux ; de surveiller les examens. Les logiciels de surveillance d'examens à distance sont aussi connus sous l'expression anglaise *proctoring software*, tels Respondus Monitor, ProctorU, Proctorio et Examity. Si ces logiciels ont été utilisés au Canada au cours des 20 dernières années, la pandémie a néanmoins accéléré l'usage de ces outils, dès lors que les étudiants sont plus portés à tricher lors d'un examen en ligne que lorsqu'ils passent un examen en personne. Les principales fautes relevées chez les étudiants 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. Le choix des universités en différents endroits du monde s'est porté sur les logiciels de surveillance d'examens, poussées qu'elles étaient par les fournisseurs de ces logiciels qui affirmaient que leurs outils pouvaient atténuer grandement les occasions de tricherie lors des évaluations à distance. Deux grandes catégories de solutions de surveillance sont observables : le blocage de l'ordinateur pour empêcher les étudiants d'utiliser un logiciel de navigation pendant l'examen, et l'activation d'une caméra pour qu'une surveillance « en temps réel » puisse se faire, dans le but de détecter des comportements pouvant être indicatifs de tricherie. Toutefois, le recours à ces outils n'est pas dénué de risques sociaux, éthiques et juridiques, en particulier quant à la protection des renseignements personnels des étudiants. La minimisation des risques d'atteinte à leur vie privée est un défi particulièrement délicat à relever pour les universités et les législateurs.

Nous verrons, dans une première partie, comment les technologies se sont immiscées dans le domaine de l'éducation et, en particulier, en vue de la surveillance d'examens par différents procédés. Ces outils posent de nombreux enjeux sociaux et éthiques (I), confirmés par une analyse empirique plus particulière de certains d'entre eux, utilisés par les universités canadiennes. La deuxième partie permettra de comprendre de façon plus précise les difficultés de mise en œuvre de ces logiciels de surveillance (II). La troisième partie exposera les difficultés juridiques en analysant les lois sur la protection des renseignements

personnels et leurs faiblesses (III). La quatrième partie présentera des propositions pour renforcer la protection des renseignements personnels dans un contexte où les universités facilitent l'accès aux données des étudiants à des entreprises américaines du secteur privé qui proposent ces outils de surveillance d'examens. Ces recommandations sont de nature à éclairer le débat dans la réforme actuelle de la législation fédérale sur la protection des renseignements personnels du secteur privé (*Loi sur la protection des renseignements personnels et les documents électroniques*[1]) (IV).

I. SURVEILLANCE TECHNOLOGIQUE DES EXAMENS

L'usage des technologies en éducation doit permettre d'atteindre des objectifs variés[2]. Il peut s'agir notamment : de trier et sélectionner les candidats à l'entrée dans les universités ou dans les grandes écoles[3] ; de mettre à disposition des ressources en ligne sur un campus virtuel[4] ; de mesurer le rendement et la performance scolaires[5] ; de déterminer un score de résultat final[6] ; de surveiller les examens. Ce dernier usage retiendra notre attention ici. Seront présentés les logiciels (A), les risques éthiques et sociaux (B), ainsi que juridiques (C), de même que la problématique, la méthodologie et le plan de l'étude (D).

1. LC 2000, c 5 [LPRPDE].

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 : <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. Par ex, « L'algorithme de tri Parcoursup pour accéder aux établissements d'enseignement supérieur » *Parcoursup*, en ligne : <www.arxiv.org/abs/2011.07647>.

4. Par ex, BrightSpace, qui collecte des renseignements personnels et des informations sur l'activité des utilisateurs.

5. Des systèmes d'intelligence artificielle (IA) ont été déployés afin de prédire le rendement scolaire, 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 (pdf) : *Melbourne Law School* <www.arxiv.org/abs/2011.07647>.

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

A. Présentation des logiciels de surveillance d'examens (vue générale)

La surveillance en éducation est devenue un nouveau terrain de la « surveillance capitalistique »[7]. Avant même la pandémie de COVID-19, la part estimée du marché des technologies en éducation (*Ed-Tech*) était évaluée en 2019 à 19 milliards de dollars américains[8]. En 2020, le secteur de l'apprentissage en ligne dépassait 100 milliards de dollars américains[9]. On s'attend, en outre, que de 2020 à 2027, le marché des logiciels de surveillance d'examens croisse de 16,4 % annuellement[10]. D'ici 2027, ce marché devrait atteindre une valeur de 10 milliards de dollars américains[11]. Certains auteurs notent un accroissement d'utilisation de 720 % depuis le début de la pandémie[12].

Les logiciels de surveillance d'examens à distance ne sont pas nouveaux au Canada[13]. Par exemple, l'Université Queen's a indiqué au début de la pandémie en 2020 qu'elle utilisait ces procédés depuis plusieurs années[14]. La pandémie a toutefois encouragé les universités à se doter de solutions de surveillance automatique et elles continuent à s'en servir du fait de leur utilité. La tricherie universitaire n'est certes pas propre à l'environnement virtuel, mais y est rendue plus facile et

---

7. Shoshana Zuboff, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power*, Londres, Profile Books, 2019.

8. Neil Selwyn et al, « A Necessary Evil ? The Rise of Online Exam Proctoring in Australian Universities » (2021)1 à la p 2, en ligne (pdf) : *Monash University* <www.journals.sagepub.com/doi/pdf/10.1177/1329878X211005862>.

9. Ludwig Slusky, « Cybersecurity of Online Proctoring Systems » (2020) 29 :1 Journal of International Technology and Information Management 56 à la p 57, en ligne (pdf) : <www.scholarworks.lib.csusb.edu/cgi/viewcontent.cgi ?article=1445&context=jitim>.

10. Selwyn et al, *supra* note 8 à la p 4.

11. Daniel Woldeab et Thomas Brothen, « Video Surveillance of Online Exam Proctoring : Exam Anxiety and Student Performance » (2021) 36 :1 International Journal of E-Learning & Distance Education 1 à la p 2, en ligne : <www.proquest.com/docview/2572618998 ?parentSessionId=zl%2BfEpWBBJvqZTbySldGxUyimOQu0URzQYQ9uoPGi %2FY %3D&pq-origsite=primo&accountid=14701>.

12. David G Balash et al, « Examining the Examiners : Students' Privacy and Security Perceptions of Online Proctoring Services » (2020) à la p 1, en ligne (pdf) : <www.arxiv.org/ftp/arxiv/papers/2106/2106.05917.pdf>.

13. Barbara Fedders, « The Constant and Expanding Classroom : Surveillance in K-12 Public Schools » (2019) 97 NC Rev 1673.

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

plus tentante[15], et ce, dans le monde entier[16], en comparaison avec des évaluations en présentiel[17]. Les principales fautes relevées chez les étudiants 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.

Pour garantir l'intégrité de leurs diplômes, les universités canadiennes ont opté pour l'utilisation de logiciels de surveillance d'examens à distance (*proctoring softwares* en anglais) présentés comme un moyen de limiter les occasions de tricherie[18]. Ces logiciels, tels que Respondus Monitor, ProctorU, Proctorio et Examity, proposent différentes solutions pour maintenir une certaine unité dans le temps et dans l'espace, laquelle caractérise la surveillance en présentiel. Ils tentent aussi de détecter des comportements de tricherie potentielle. C'est ainsi, par exemple, que le blocage de l'ordinateur empêche les étudiants d'utiliser un logiciel de navigation pendant l'examen. Il peut aussi leur être demandé d'activer une caméra pour permettre une surveillance « en temps réel ». Certains outils mettent en œuvre des systèmes d'intelligence artificielle (IA) dans l'espoir d'augmenter l'efficacité et la précision de la surveillance[19]. Ainsi, des systèmes d'IA utilisent des marqueurs biométriques, tels que des dispositifs de reconnaissance faciale, en combinaison avec les photos d'identification des étudiants[20]. D'autres systèmes permettent de repérer des comportements anormaux, comme la « disparition » du visage d'un étudiant ou la présence de deux personnes, au lieu d'une. D'autres techniques automatisées sont utilisées, telles que la biométrie de frappe (*biometric keystroke analysis*), le suivi des mouvements des yeux (*eye tracking*), la surveillance auditive (*audio monitoring*) et la détection faciale, pour chercher des indices de

15. Coghlan, Miller et Paterson, *supra* note 5 à la p 5.

16. Sheena Rossiter, « Cheating Becoming an Unexpected COVID-19 Side Effect for Universities », *CBC News Edmonton* (21 juin 2020), en ligne : <www.cbc.ca/news/canada/edmonton/cheating-becoming-an-unexpected-covid-19-side-effect-for-universities-1.5620442>.

17. Ludwig Slusky, *supra* note 9 à la p 57 ; Giacomo Panico, « University Cheating Might Be Up — But Don't Just Blame Students », *CBC News Ottawa* (19 juillet 2020), en ligne : <www.cbc.ca/news/canada/ottawa/university-cheating-might-be-up-but-don-t-just-blame-students-1.5618272>.

18. Timothy H Reisenwitz, « Examining the Necessity of Proctoring Online Exams » (2020) 20:1 Journal of Higher Education Theory & Practice 118 à la p 123, en ligne (pdf) : <www.na-business-press.com/JHETP/JHETP20-1/9_ReisenwitzT__20_1_.pdf>.

19. Coghlan, Miller et Paterson, *supra* note 5 à la p 1.

20. *Ibid* à la p 2.

tricherie ou d'utilisation de matériel non autorisé[21]. La détection et l'analyse des émotions à partir des expressions du visage sont aussi des possibilités offertes aux universités.

B. Enjeux éthiques et sociaux

Il faut admettre que les outils de surveillance en éducation présentent des avantages. Ils génèrent des économies en temps de déplacement et en argent pour passer les examens. Ils ont surtout permis de répondre à une demande urgente, lors de la déclaration de la pandémie de COVID-19 en mars 2020, alors que la fin du trimestre d'hiver et la période d'examen approchaient. Plus de deux ans plus tard, l'urgence passée, il est temps de considérer plus attentivement les risques sociaux et éthiques qu'ils engendrent.

La décision de faire appel aux logiciels de surveillance d'examens à distance a fait beaucoup de mécontentements parmi les étudiants à l'échelle mondiale. On a ainsi vu, en Australie, des manifestations d'étudiants s'opposant à l'usage de ces outils[22]. Les étudiants ont aussi exprimé leurs craintes aux États-Unis[23] et au Canada. Par exemple, une pétition a circulé en juillet 2020 à l'Université d'Ottawa[24]. Des inquiétudes se sont aussi manifestées au Manitoba[25]. À l'Université de la Colombie-Britannique, la décision a été prise de renoncer à l'utilisation des logiciels de surveillance, en raison notamment des mécontentements et des lettres ouvertes des étudiants[26]. Dans la plupart des cas,

21. *Ibid* aux pp 2–3.

22. *Ibid* ; Selwyn et al, *supra* note 8 au pp 1–2 ; Jake Evans, « ANU to Use Facial Detection Software on Student Computers in Response to Coronavirus Remote Exams », *ABC* (20 avril 2020), en ligne : <www.abc.net.au/news/2020-04-20/coronavirus-anu-to-use-ai-spying-software-on-student-computers/12164324>.

23. Shawn Hubler, « Keeping Online Testing Honest ? Or an Orwellian Overreach ? », *New York Times* (10 mai 2020), en ligne : <www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html>.

24. Giamoco Panico, « U of O Students Wary of "Extreme" Anti-Cheating Software », *CBC News Ottawa* (2 juillet 2020), en ligne : <www.cbc.ca/news/canada/ottawa/exam-surveillance-software-university-ottawa-1.5633134>.

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

26. Lauren Krugel, « "Creeped Out" Schools Turn to Technology in Pandemic to Catch Online Cheaters » *CTV News* (11 octobre 2020), en ligne : <www.ctvnews.ca/health/coronavirus/creeped-out-schools-turn-to-technology-in-pandemic-to-catch-online-cheaters-1.5141633> ; AMS Student Nest (UBC) « Open Letter Regarding the Usage of Proctorio » *AMS UBC* (3 juillet 2020), en ligne : <www.ams.ubc.ca/news/open-letter-regarding-the-usage-of-proctorio/>.

les tensions se sont apaisées, grâce aux efforts des universités pour tenir compte des craintes exprimées et renforcer la protection des informations des étudiants. La pandémie se prolongeant, le recours aux logiciels de surveillance a pu être allégé et devenir parfois, aujourd'hui, un simple accommodement proposé aux étudiants trop éloignés des centres d'examen. Par exemple, l'Université de Toronto[27] offre les services d'*Examity* aux étudiants inscrits à des cours en ligne, qui ne vivent pas à moins de 30 kilomètres d'un centre d'examen canadien, incluant tous les étudiants internationaux.

Certaines solutions ponctuellement mises en place pendant la pandémie sont ainsi susceptibles d'être maintenues. Or, différents risques ont été relevés. Ces outils ont une incidence sur la santé mentale des étudiants. Le site de l'Université du Manitoba indique que « l'utilisation de Respondus […] s'accompagne de contraintes possibles telles que […] le risque d'une anxiété accrue »[28]. De nombreux candidats font part de l'augmentation de l'anxiété liée aux examens[29] quand il s'agit d'installer un outil de surveillance et de maintenir une (voire deux) caméra constamment allumée pendant toute la durée de l'examen[30]. Les usagers sont sous une surveillance constante[31] et craignent que certains de leurs mouvements soient indûment signalés comme suspects, conduisant à de fausses accusations de malhonnêteté universitaire[32]. Même les auteurs en faveur de l'adoption des logiciels de surveillance soulignent l'intensification de l'angoisse chez les étudiants[33].

Également, ces outils rompent l'égalité entre les étudiants, engendrant une possible discrimination liée à la race ou à l'ethnicité, au

---

27. University of Toronto, « How Does Online Proctoring Work » (s.d.), en ligne : *University of Toronto* <www.help.learn.utoronto.ca/hc/en-us/articles/115004994514-How-does-online-proctoring-work->.

28. University of Manitoba, « Respondus Provides Assessment Tools to Create, Manage and Monitor Online Exams in UM Learn » (s.d.), en ligne : *University of Manitoba* <www.umanitoba.ca/centre-advancement-teaching-learning/technologies/respondus>.

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

30. Jessica Wong, « Post-Secondary Students Call for Changes to Online Exam Rules as Cheating Concerns Rise », *CBC News* (25 octobre 2020), en ligne : <www.cbc.ca/news/canada/post-secondary-assessment-integrity-proctoring-1.5767953>.

31. 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 Coghlan, Miller et Paterson, *supra* note 5 à la p 2.

32. Wong, *supra* note 30.

33. Reisenwitz, *supra* note 18 à la p 123.

handicap, aux facteurs socioéconomiques ou au territoire (conditions d'accès à Internet). Ainsi, plusieurs recherches ont démontré que les outils de reconnaissance faciale reconnaissent mal les peaux sombres[34], ce qui est le cas aussi des logiciels de surveillance d'examens[35]. Les algorithmes de reconnaissance faciale utilisés étant en effet souvent les mêmes d'une application à une autre, on y constate donc des difficultés identiques.

Il faut ajouter que les étudiants en situation de handicap rencontrent des difficultés supplémentaires[36]. Certains rapportent que le logiciel spécialisé de lecture d'écran qu'ils utilisent habituellement peut s'avérer incompatible avec un logiciel de surveillance à distance[37]. Certains programmes d'accessibilité de lecteur d'écran, tels que JAWS, Windows-Eyes ou VoiceOver, par exemple, sont compatibles avec un outil comme Respondus, mais pas nécessairement avec d'autres outils d'accessibilité. Si les étudiants ont du mal à télécharger le logiciel ou s'ils ne peuvent 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 au moyen du service de dialogue en direct 24 heures sur 24 et 7 jours sur 7, ce qui est certainement anxiogène au moment même de passer leur examen. Plus largement, se pose la question de la prise en compte des accommodements particuliers dont bénéficient de nombreux 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 d'y réunir toutes les conditions matérielles. L'inégalité entre les étudiants résulte alors de facteurs économiques et sociaux, mais aussi

---

34. Voir les travaux de Joy Buolamwini, chercheuse au MIT et fondatrice de l'Algorithmic Justice League, en ligne : <www.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 : <www.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 : <www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use> ; Ruha Benjamin, *Race After Technology : Abolitionist Tools for the New Jim Code*, Cambridge, Polity, 2019.

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

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

37. Wong, *supra* note 30.

parfois territoriaux[38]. Les étudiants doivent avoir un accès[39] performant au réseau Internet[40], s'équiper d'une *webcaméra* et d'un microphone fonctionnels à activer sur l'ordinateur à tout moment pendant l'évaluation. Ce matériel doit être suffisamment récent pour être compatible avec les logiciels de surveillance ; or, certains étudiants pourraient rencontrer des difficultés à satisfaire à ces exigences. Quant à l'accès à Internet, il est parfois précisé que l'utilisation d'une *webcaméra* ne comporte pas d'exigence particulière relativement au débit de la bande passante en kbps, la qualité d'enregistrement pouvant s'ajuster automatiquement lorsqu'une connexion plus lente est détectée ; toutefois, à l'inverse, lorsque l'étudiant utilise une connexion Internet partagée, il doit s'assurer que pendant l'examen, les co-usagers n'utilisent pas des services exigeants en bande passante (tels que les films en ligne, les jeux, le partage de fichiers, etc.). Également, au moment de l'examen, de nombreux étudiants sont retournés chez leurs parents et se trouvent parfois loin des centres urbains. Bien qu'Internet soit très accessible dans les provinces, le gouvernement canadien relève que 6 % des ménages canadiens sont toujours sans accès à Internet pour diverses raisons, telles que le coût de l'abonnement à Internet ou encore celui de l'équipement nécessaire[41]. En outre, seuls 45,6 % des collectivités rurales ont accès à une connexion rapide d'au moins 50 Mbps de téléchargement et de 10 Mbps de téléversement[42]. D'ailleurs, une publication gouvernementale souligne que les personnes situées dans un milieu urbain sont plus portées à participer à des activités de formation ou

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

39. Associated Press, « Million of Kids Are Struggling in School Because They Don't Have Internet Access at Home », *Market Watch* (10 juin 2019), en ligne : <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>.

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

41. Statistique Canada, « Accès à Internet au Canada, 2020 », *Le Quotidien* (31 mai 2021), en ligne (pdf) : <www.150.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 », *Le Quotidien* (5 mai 2021), en ligne : <www.150.statcan.gc.ca/n1/daily-quotidien/210531/cg-d001-fra.htm>.

42. Conseil de la radiodiffusion et des télécommunications canadiennes, « Fonds pour la large bande. Combler le fossé numérique au Canada » *CRTC* (2021), en ligne : <www.crtc.gc.ca/fra/internet/internet.htm>.

d'apprentissage en ligne que celles qui vivent en milieu rural[43]. Par ailleurs, faire peser sur l'étudiant la responsabilité de la performance d'un équipement pour le bon fonctionnement d'un logiciel de surveillance pose la question du déséquilibre entre les étudiants et celle du rôle des universités.

Plus globalement, ces technologies sont proposées par des acteurs privés non soumis à une mission publique d'éducation. Non seulement la logique du service au public leur échappe, mais en outre, ils sont portés à déployer leurs outils sur différents marchés et à profiter des apports générés par l'entraînement des systèmes de surveillance et collecte des données. Une technologie, telle la reconnaissance faciale, peut être utilisée pour des usages variés comme le contrôle aux frontières ou le maintien de l'ordre. D'aucuns soutiennent que l'intégration de ces logiciels durant la pandémie pourrait servir de « preuve de concept » de moyens de surveillance[44]. La pandémie a accéléré l'utilisation des systèmes automatiques de surveillance et a probablement été aussi un facteur de banalisation.

C. Problématiques, méthodologie et plan

Les risques sociaux et éthiques ainsi soulevés fondent les principales questions de la recherche en droit : quels sont les principaux risques juridiques posés par ces outils ? Les lois de protection des renseignements personnels assurent-elles une protection suffisante ? Si tel n'est pas le cas, quelles modifications de ces lois faudrait-il encourager ? Pour répondre à ces questions, nous avons employé une méthodologie à la fois empirique et théorique. La **recherche empirique** a consisté à répertorier 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) (partie II). L'**analyse théorique** des documents contractuels a été mise à l'épreuve du droit canadien et spécialement des lois de protection des renseignements personnels du secteur public au Canada. L'étude porte sur les lois provinciales de protection des renseignements

43. Statistique Canada, « Accès à Internet au Canada », *supra* note 41.

44. Selwyn et al, *supra* note 8 à la p 12.

personnels pour le secteur privé et sur la LPRPDE[45] (partie III). Les limites répertoriées dans la LPRPDE justifient les propositions d'amélioration à l'adresse du législateur (partie IV).

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

Plusieurs entreprises proposent leurs outils de surveillance d'examens, tels Respondus Monitor, Proctorio, ProctorU, ProctorExam, Examity, ProctorTrack, le plus souvent intégrés au système de gestion de l'apprentissage (*Online Learning Platform* ou D2L). Alors qu'il existe une grande variété de logiciels, nous nous concentrerons sur les logiciels automatisés (*automated proctoring*) qui réduisent au minimum l'intervention humaine, tant pour la surveillance que pour la révision des examens. Ainsi, ces logiciels vont notifier aux responsables de l'enseignement les incidents potentiels de tricherie ou des comportements jugés anormaux, afin qu'un contrôle humain soit effectué pour déterminer s'il y a eu réellement de la tricherie[46]. Ces logiciels permettent d'authentifier l'étudiant, d'analyser ses comportements, de limiter les capacités de son ordinateur et de générer un rapport[47]. Certains de ces outils eux sont totalement automatisés, alors que d'autres sont hybrides, combinant une surveillance humaine et des fonctionnalités automatisées[48].

Trois outils de surveillance d'examens seront présentés dans l'objectif de comprendre leur fonctionnement et de rechercher les risques effectifs concernant la protection de la vie privée et des renseignements personnels : (A) Respondus, utilisé à l'Université d'Ottawa ; (B) Proctor U, utilisé à l'Université de Toronto ; et (C) Proctorio, choisi par l'Université Laval et l'Université de la Colombie-Britannique.

---

45. *Supra* note 1.

46. Mohammed Juned Hussein et al, « An Evaluation of Online Proctoring Tools, Open Praxis » (2020) 12 :4 *International Council for Open and Distance Education* (ICDE) 509 à la p 510, en ligne (pdf) : <www.files.eric.ed.gov/fulltext/EJ1285031.pdf>.

47. *Ibid*.

48. « *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* », Slusky, *supra* note 9 à la p 71.

A. Respondus à l'Université d'Ottawa

Respondus Inc est une entreprise américaine établie à Redmond, dans l'État de Washington[49]. Son outil est utilisé notamment par l'Université du Manitoba[50] et l'Université d'Ottawa[51]. L'Université d'Ottawa a communiqué sur son site Internet les conditions d'utilisation de l'outil. Deux types de paramétrage sont disponibles : LockDown Browser et Respondus Monitor. LockDown Browser n'est pas un système de surveillance, mais un navigateur personnalisé qui verrouille l'environnement d'examen dans Brightspace (campus virtuel), de façon à empêcher les étudiants d'aller chercher des informations ailleurs, notamment sur les sites Web. Il 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 transmis. 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.

Respondus Monitor est en revanche une solution de surveillance entièrement automatisée. Lorsque cette fonction est activée pendant un examen en ligne, les étudiants sont tenus d'utiliser une *webcaméra* et un microphone avec le navigateur LockDown Browser. Par la suite, le professeur a accès aux événements anormaux signalés par le système et aux résultats de la surveillance en vue de faire un examen plus approfondi des détails de l'évaluation, y compris des vidéos enregistrées[52]. En principe, seuls les enseignants peuvent accéder aux informations sur les séances d'examen et visionner les vidéos enregistrées.

B. Proctor U à l'Université de Toronto

Fondée en 2008, ProctorU est une compagnie qui offre des services de surveillance universitaire et professionnelle. La firme est actuellement basée à Birmingham, dans l'État de l'Alabama. Plusieurs

49. Respondus, « Webinars » (s.d.), en ligne : *Respondus* <www.web.respondus.com/webinars/>.

50. *Supra* note 28.

51. Université d'Ottawa, « Respondus » (s.d.), en ligne : Université d'Ottawa <https://saea-tlss.uottawa.ca/fr/technologies-denseignement/integrite-academique-ouriginal-et-respondus/en-savoir-plus-sur-respondus>.

52. Respondus, « Webinars », *supra* note 49.

universités, telles que l'Université de Toronto[53], l'Université de Waterloo[54], l'Université d'Athabasca (Alberta)[55], l'Université Thompson Rivers (Colombie-Britannique)[56] et l'Université Memorial (Terre-Neuve-et-Labrador)[57]. En janvier 2020, ProctorU et la firme canadienne Yardstick Assessment Strategies ont fusionné sous le nom de Meazure Learning, tout en continuant à mener leurs activités sous leur nom respectif[58]. Jusqu'au mois de mai 2021, ProctorU offrait trois différents services : ProctorU Auto, ProctorU Live+ et ProctorU Pro[59]. ProctorU Auto était l'option automatisée qui déployait un dispositif d'IA pour signaler des comportements jugés suspects, tout en enregistrant le déroulement de l'examen, afin qu'il puisse être visionné au besoin[60]. Un examen sous la surveillance de ProctorU Auto requiert que l'étudiant détienne une pièce d'identité gouvernementale et soit situé dans un environnement silencieux, bien éclairé et privé[61]. De plus, avant la tenue de l'examen, 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[62].

ProctorU Live+ est une option combinant un surveillant humain et un dispositif d'IA pour assurer la surveillance d'examens[63]. ProctorU Pro

---

53. University of Toronto, « ProctorU : Privacy and Security Information Notice for Students » (s.d.), en ligne : *University of Toronto* <www.teaching.utoronto.ca/resources/proctoru-privacy-and-security-information-notice-for-students/>.

54. University of Waterloo, « Online Proctoring FAQs » (s.d.), en ligne : *University of Waterloo* <www.uwaterloo.ca/extended-learning/learn-online/write-exams/online-proctoring-faqs>.

55. Athabasca University, « Using ProctorU for Online Exams » (s.d.), en ligne : *Athabasca University* <www.athabascau.ca/support-services/exam-services-support/using-proctoru-for-online-exams.html>.

56. Thompson Rivers University, « ProctorU — Open Learning » (s.d.), en ligne : *Thompson Rivers University* <www.tru.ca/distance/faq/faq-proctoru.html>.

57. Memorial University, « Online Proctoring » (s.d.), en ligne : *Memorial University* <www.citl.mun.ca/TeachingSupport/TeachOnline/OnlineProctoring.php>.

58. Meazure Learning, « ProctorU Merges With Yardstick to Form New "End-to-End" Testing Company », *Edsurge* (14 janvier 2020), en ligne : <www.edsurge.com/news/2020-01-14-proctoru-merges-with-yardstick-to-form-new-end-to-end-testing-company-meazure-learning>.

59. ProctorU Platform Support, « Do You Know All About Our Three Tiers of Proctoring… » (7 décembre 2018), en ligne : *Twitter* <www.twitter.com/ProctorUSupport/status/1071157226621059072>.

60. Ava Abbott, « What Is ProctorU, How It Works and Makes Money ? » (s.d.), en ligne : *Business Strategy Hub* <www.bstrategyhub.com/what-is-proctoru-how-it-works-and-makes-money/>.

61. ProctorU, « ProctorU Auto Demofor Test Takers » (30 mars 2018), en ligne (vidéo) : *YouTube* <www.youtube.com/watch ?v=eTFDrRVQzO8>.

62. *Ibid*.

63. Abbott, *supra* note 60.

était une version plus performante de ProctorU Live+, qui comportait davantage de paramètres pouvant être modifiés, ainsi que des surveillants humains « les mieux entraînés », offerts par ProctorU[64]. Cependant, le 24 mai 2021, Meazure Learning a annoncé que ProctorU cesserait d'offrir des options qui mobilisent uniquement l'IA pour générer les rapports d'incidents (ProctorU Auto) et assurerait qu'une vérification du rapport généré par l'IA serait effectuée par une personne[65]. En effet, selon ProctorU, l'utilisation exclusive de l'IA pour générer les rapports d'incidents était parfois injuste pour les étudiants[66]. Ce changement de position de l'entreprise doit permettre de faire face à la multiplication des articles négatifs portant sur les logiciels de surveillance[67]. 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, affirmant se servir désormais d'une « technologie avancée », déployée avec une intervention humaine[68].

Par ailleurs, ProctorU offre Review+, par lequel le processus d'authentification et les vérifications postérieures d'examens sont faits par des surveillants humains, en plus de l'automatisation de la surveillance[69]. Review+ génère un rapport d'incidents à l'intention des

---

64. *Ibid.*

65. Meazure Learning, « ProctorU to Discontinue Exam Integrity Services That Rely Exclusively On AI » (24 mai 2021), en ligne : *Meazure Learning* <www.meazurelearning.com/resources/proctoru-to-discontinue-exam-integrity-services-that-rely-exclusively-on-ai> ; Lindsay McKenzie, « Time to Rethink AI Proctoring ? » (28 mai 2021), en ligne : *Inside Higher Ed* <www.insidehighered.com/news/2021/05/28/are-colleges-checking-ais-work-remote-exam-proctoring> ; Scott Jaschik, « ProctorU Abandons Business Based Solely on AI » (24 mai 2021), en ligne : *Inside Higher Ed* <www.insidehighered.com/news/2021/05/24/proctoru-abandons-business-based-solely-ai> ; Rhea Kelly, « ProctorU Gets Rid of AI-Only Proctoring », *Campus Techonology* (24 mai 2021) en ligne : <www.campustechnology.com/articles/2021/05/24/proctoru-gets-rid-of-ai-only-proctoring.aspx>.

66. *Ibid.*

67. McKenzie, *supra* note 65.

68. *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* [notre soulignement].

Meazure Learning, « Live+ » (s.d.), en ligne : *Meazure Learning* <www.meazurelearning.com/products/proctoru-online-proctoring/live-plus>.

69. *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+ » (s.d), en ligne : *Meazure Learning* <www.meazurelearning.com/products/proctoru-online-proctoring/review-plus>.

professeurs ou superviseurs[70] ; c'est l'option suggérée pour des examens à enjeux moyens et faibles[71]. Finalement, ProctorU offre l'option Record +, qui assure l'authentification des examens de manière automatisée, ainsi qu'une surveillance d'examens automatisée visant à détecter des comportements suspects, vérifiés ensuite par un surveillant certifié avant la délivrance d'un rapport d'incident[72].

C. Proctorio à l'Université Laval et l'Université de la Colombie-Britannique

Proctorio est un logiciel de surveillance automatisé proposé par une entreprise américaine située en Arizona. Il a notamment été mis en œuvre par l'Université Laval[73], l'Université Concordia[74] et l'Université de la Colombie-Britannique. Il mobilise des formules algorithmiques, telles que l'apprentissage automatique et la reconnaissance faciale, afin de détecter des comportements indicatifs de tricherie[75]. Selon des communications universitaires, Proctorio est doté de fonctions telles que l'authentification automatisée, la surveillance automatisée, l'enregistrement vidéo et l'enregistrement audio, l'enregistrement de la salle physique et l'examen des comportements étudiants[76]. Ces options permettent la surveillance en temps réel et la surveillance par enregistrement[77]. Proctorio affirme que ses techniques algorithmiques sont

---

70. *Ibid*.

71. *Ibid*.

72. *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, « *Record +* » (s.d.), en ligne : *Meazure Learning* <www.meazurelearning.com/products/proctoru-online-proctoring/record-plus>.

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

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

75. 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* <www.theverge.com/2020/10/22/21526792/proctorio-online-test-proctoring-lawsuit-universities-students-coronavirus>.

76. University of British Columbia, « Software for Securing & Proctoring Exams » (s.d.), en ligne : *University of British Columbia* <www.isit.arts.ubc.ca/software-for-securing-proctoring-exams/>.

77. *Ibid*.

supérieures et plus efficaces que la surveillance humaine en ce qui concerne la détection de la tricherie universitaire[78]. Toutefois, Proctorio a été accusée d'utiliser des algorithmes discriminatoires envers les étudiants des minorités visibles[79] et on a en effet constaté que Proctorio met en œuvre un algorithme de source ouverte, reconnu comme étant discriminatoire. Selon certaines analyses, 57 % des tentatives d'authentification par les individus à la peau noire sont infructueuses[80]. De plus, les meilleurs taux d'authentification dans tous les groupes d'ethnicité sont inférieurs à 75 %[81], ce qui signifie que le taux d'erreur est élevé.

Proctorio a été utilisé par l'Université de la Colombie-Britannique (UBC). Toutefois, en mars 2021, à la suite d'un vote des Sénats de l'UBC Vancouver et de l'UBC Okanagan, l'Université a annoncé qu'elle interdisait l'utilisation de logiciels de surveillance automatisée, tels que Proctorio, dans tous les programmes, à l'exception de ceux d'accréditation[82]. Les professeurs qui prévoyaient utiliser de tels outils pour surveiller des examens dans le cadre de cours qui ne sont pas visés par l'exemption sont invités à chercher d'autres outils ou méthodes d'évaluation. L'outil a fait l'objet d'une analyse d'impact sur la vie privée, et son abandon pourrait être justifié par des résultats insatisfaisants[83].

III. ANALYSE JURIDIQUE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les risques sociaux et éthiques déjà mentionnés sont d'autant plus alarmants que l'on peut aussi s'interroger sur les enjeux juridiques, liés en particulier à l'invasion de la vie privée par ces outils[84]. Outre le

78. Coghlan, Miller et Paterson, *supra* note 5 à la p 4.

79. *Ibid ;* Todd Feathers, « Proctorio Is Using Racist Algorithms to Detect Faces » (4 août 2021), en ligne : *Vice* <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* <www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning>.

80. Feathers, *supra* note 79.

81. Clark, *supra* note 79.

82. University of British Columbia, « UBC Senate Motions on Use of Remote Proctoring Software » (18 mars 2021), en ligne : *University of British Columbia* <www.lthub.ubc.ca/2021/03/18/ubcv-senate-motion-proctoring/>.

83. University of British Columbia, « Privacy Impact Assessment (PIA) », en ligne : *University of British Columbia* <www.privacymatters.ubc.ca/sites/privacymatters.ubc.ca/files/PIA>.

84. Patil et Bromwich, *supra* note 35.

nombre considérable de données susceptibles d'être recueillies par ces procédés, certains de ces outils collectent des données biométriques sensibles, associées à un système d'IA, pour vérifier la correspondance des images des étudiants et des bases de données avec les candidats postés devant la caméra. Les informations collectées sont non seulement des renseignements personnels permettant d'identifier des élèves, mais il peut aussi s'agir d'indicateurs pour inférer des performances pouvant donner lieu à des profilages discriminants. Cette collecte de données donne un avantage concurrentiel à ces entreprises pour proposer par la suite d'autres outils d'évaluation des performances ou encore de détection des humeurs par lecture automatique des expressions du visage, par exemple pour rechercher les habiletés des personnes à gérer le stress. Le risque d'hypersurveillance est réel, en particulier dans le domaine de l'IA émotionnelle. Par ailleurs, alors que les prestataires de services 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 continuent à s'appliquer et surtout, si elles sont en mesure d'assurer 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.

Si on comprend l'intérêt de recourir à ces outils, leurs fonctionnalités nous obligent à nous interroger sur la collecte massive de renseignements personnels, *a fortiori* quand des technologies d'IA sont utilisées. Plusieurs questions juridiques se posent alors tenant à : la détermination des lois de protection des renseignements personnels applicables (A) ; l'identification des renseignements personnels collectés et leur conservation (B) ; le consentement lié à la collecte des renseignements personnels et celui lié à l'utilisation du système de surveillance (C) ; les transferts internationaux de renseignements personnels vers les États-Unis (D).

A. 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 domaine de l'éducation. Dès lors que l'éducation relève de la compétence des provinces, les lois provinciales de protection des renseignements personnels du

secteur public sont en principe applicables[85]. L'application des lois du secteur public ne fait aucun doute s'agissant des universités, puisque les lois du secteur privé s'appliquent uniquement dans l'hypothèse où l'organisation exerce une activité commerciale en dehors de son activité essentielle. La collecte et l'utilisation de données personnelles pour la surveillance d'examens relèvent de la mission des universités et ne requièrent pas le consentement des personnes concernées, suivant les lois provinciales du secteur public[86], qui reprennent le modèle fédéral de la *Loi sur la protection des renseignements personnels*[87]. En principe, les organismes du secteur public ne peuvent utiliser les renseignements personnels que pour des usages limités[88] : en considération de la finalité pour laquelle l'information a été collectée ou pour un usage cohérent avec cette finalité ; en considération d'une finalité pour laquelle l'information peut être divulguée à cet organisme public ; quand la personne concernée a consenti à l'utilisation.

---

85. 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* <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/>.

86. Par ex, au Québec, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1 [*Loi sur l'accès* québécoise], art 64 (collecte des renseignements personnels) : « Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion. »

87. LRC (1985), c P-21 [LPRP].

88. Par ex, *Loi sur l'accès* québécoise, *supra* note 86, art 65.1 (utilisation des renseignements personnels) :

> Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli. L'organisme public peut toutefois utiliser un tel renseignement à une autre fin avec le consentement de la personne concernée ou, sans son consentement, dans les seuls cas suivants : 1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli ; 2° lorsque son utilisation est manifestement au bénéfice de la personne concernée ; 3° lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi. Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli [notre soulignement].

À noter que la *Loi sur l'accès* québécoise n'a pas été modifiée sur ce point par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, RLRQ 2021 c 25 [*Loi 25*]. Si une obligation d'information de la personne concernée pèse désormais sur « quiconque recueille des renseignements personnels », cette obligation ne s'applique que si la collecte se fait « au nom d'un organisme public », ce qui n'est pas le cas concernant les logiciels de surveillance d'examens.

Par ailleurs, les lois provinciales du secteur public reprennent le critère du contrôle posé par la LPRP[89]. Elles s'appliquent aux renseignements personnels et aux documents qui relèvent d'un organisme ou d'une institution publique. Le contrôle n'a toutefois pas besoin d'être absolu, direct ou permanent. La Cour d'appel fédérale a ainsi jugé, dans l'affaire *Société canadienne des postes c Canada (Ministre des Travaux publics)*[90], que l'expression « relevant de » doit faire l'objet d'une interprétation souple et libérale. Par exemple, les renseignements détenus par un mandataire d'un organisme public relèvent de l'organisme public lui-même, et la loi du secteur public continue à s'appliquer.

Cette qualification est centrale s'agissant du recours aux outils de surveillance d'examens, puisque les universités font appel à des entreprises privées pour mettre en œuvre ces outils et organisent ainsi la sous-traitance de cette activité. Cependant, cette jurisprudence ne s'applique que partiellement à ce cas. En effet, les universités confient le traitement de renseignements personnels à des entreprises tierces pour l'exécution d'une mission du secteur public consistant à surveiller les examens. Ces entreprises, pour cette partie de leurs activités, peuvent être considérées comme mandataires agissant sous le contrôle des universités. Suivant la politique de confidentialité de ProctorU[91] : « […] [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 » [notre traduction]. 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 et de reconnaissance faciale. Les conditions générales d'utilisation ou les politiques de confidentialité de ces entreprises précisent ainsi que les renseignements personnels pourront être utilisés pour des activités d'apprentissage automatique, afin d'améliorer leurs services. Dans sa politique de

---

89. Par ex, *Loi sur l'accès* québécoise, art 64 : « Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion. »

Voir aussi, *Loi sur l'accès à l'information et à la protection de la vie privée*, LRO 1990, c F.31 [*Loi sur l'accès* ontarienne], art 38(2) :

> 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.

90. 1995 CAF 241.

91. ProctorU, « Privacy Policy » (s.d.), en ligne : *ProctorU* <www.proctoru.com/privacy-policy>.

confidentialité[92], Respondus affirme utiliser les renseignements personnels notamment pour comprendre et analyser la manière dont les étudiants utilisent les services et les produits. La finalité dépasse la surveillance d'examens pour permettre l'entraînement des systèmes d'IA. D'ailleurs, les entreprises sont en relation contractuelle avec les étudiants pour collecter directement auprès d'eux des renseignements personnels auxquels les universités elles-mêmes n'ont pas accès et pour obtenir le consentement des étudiants pour le traitement des renseignements personnels à des fins commerciales. Dès lors, on ne peut plus considérer que les universités sont encore « en contrôle », s'agissant de l'utilisation des renseignements personnels pour une finalité de collecte des renseignements qui se fait, au moins partiellement, en dehors du mandat confié.

En conséquence, si les universités imposent à leurs prestataires de services des conditions de protection des renseignements personnels, en s'appuyant sur les lois provinciales du secteur public et sur leurs propres politiques de confidentialité, cela ne vaut que pour la partie de l'activité qu'elles contrôlent, en lien avec la mission d'éducation. En revanche, s'agissant des finalités technologiques et commerciales poursuivies par ces entreprises, la collecte des renseignements personnels s'exécute sous le contrôle de ces dernières, qui doivent être tenues responsables de leurs agissements. Cette interprétation est confirmée par les entreprises technologiques qui mènent des activités dans l'Union européenne et sont soumises au Règlement (UE) 2016/679 de protection des données personnelles[93]. Ces entreprises établissent elles-mêmes une différence de règles juridiques applicables selon leurs activités de traitement et admettent être sous-traitantes ou responsables de traitement selon qu'elles dépassent ou non la mission de surveillance qui leur est confiée. Par exemple, ProctorExamen[94], entreprise basée aux Pays-Bas, indique agir à titre de « responsable de traitement », quand les données sont traitées en dehors de l'activité de test. Les entreprises technologiques déterminent alors les finalités des traitements et mettent les moyens nécessaires, ce qui fait d'elles des

92. Respondus, « Additional Privacy Information — Respondus Monitor » (s.d.), en ligne : *Respondus* <www.web.respondus.com/privacy/privacy-additional-monitor/>.

93. *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* [RGPD].

94. Proctor, « Exam, Legal & Privacy » (s.d.), en ligne : <www.proctorexam.com/privacy-and-data-security/>.

« responsables de traitement » au sens du RGPD (art 4(7)). Il en est de même de Proctorio[95] qui, sur son site Internet, distingue deux activités 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 » [notre traduction]. Dans ces cas, l'université contrôle les informations. Mais Proctorio est responsable du traitement lorsque les étudiants saisissent directement des renseignements personnels dans un formulaire sur le site Web de Proctorio ou fournissent des renseignements personnels par l'entremise des services clients ou des produits de Proctorio. À l'inverse, d'autres entreprises cherchent à rejeter toute responsabilité. Respondus indique ce qui suit sur son site :

> [e]n termes de GDPR [ou RGPD], 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[96].

Si cette analyse est correcte pour une partie des activités menées par ces entreprises, elle ne l'est pas pour les traitements secondaires des données.

Dès lors, les traitements de renseignements personnels effectués sous le contrôle des entreprises technologiques sont régis par les lois provinciales du **secteur privé**. Or, seules trois provinces (Québec, Colombie-Britannique et Alberta) ont adopté de telles lois, qui sont considérées comme essentiellement similaires à la LPRPDE, et répondant au critère de son article 26(2)(b)[97]. À défaut, il faut alors s'en remettre à la LPRPDE.

---

95. Proctorio, « Privacy Policy », en ligne : <www.proctorio.com/privacy>.

96. S*upra* note 92.

97. Art 26(2)(b) LPRPDE. La similarité des lois provinciales a été reconnue par le *Décret d'exclusion visant des organisations de la province de Québec*, DORS/2003-374, 19 novembre 2003, le *Décret d'exclusion visant des organisations de la Colombie-Britannique*, DORS/2004-220, 12 octobre 2004, DORS/2004-219, et le *Décret d'exclusion visant des organisations de la province d'Alberta,* DORS/2004/219, 12 octobre 2004. Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, régit le traitement des renseignements personnels du secteur privé. En Colombie-Britannique, il s'agit de la *Personal Information Protection Act*, SBC 2003, c 63, et en Alberta, de la *Personal Information Protection Act*, SA 2003, c P-6.5.

B. Identification des renseignements personnels collectés et conservés

L'utilisation des logiciels de surveillance d'examens conduit à une importante collecte de renseignements personnels. 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 renseignements personnels, tel le nom. Outre les renseignements directement collectés auprès des étudiants lors de l'accès au service (au moyen, notamment, du compte, du formulaire de contact, du bulletin d'information et des concours ou enquêtes), des informations supplémentaires sont aussi recueillies pour assurer les performances nécessaires et optimales du système de surveillance. On note ainsi que Respondus Monitor collecte des données concernant l'activité, y compris les mouvements des yeux et le temps pris pour répondre à des questions précises lors d'une évaluation.

Respondus Monitor[98] traite en outre d'autres données provenant de la séance d'examen, telles que : la date et l'heure auxquelles l'utilisateur commence et termine une séance d'examen ; l'heure à laquelle il répond à chaque question d'examen ; le temps passé pour 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 séance d'examen (y compris l'heure et la durée de toute déconnexion d'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. Plus inquiétant encore, Respondus Monitor suit en permanence les applications et les processus qui sont exécutés sur le dispositif informatique pendant une séance 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. D'autres données sont inférées en enregistrant la manière dont l'étudiant interagit avec Respondus Monitor, par exemple en recevant des rapports d'erreur ou des données d'utilisation provenant d'un logiciel fonctionnant sur l'appareil. Il est aussi indiqué dans ses politiques que Respondus Monitor

98. *Supra* note 92.

peut analyser les enregistrements par l'intermédiaire de processus automatisés, afin de générer des données supplémentaires, dérivées des enregistrements et associées à des étudiants individuels. Ces informations supplémentaires comprennent la création d'un modèle temporaire d'identifiant facial, utilisé pour déterminer si l'étudiant qui a commencé l'examen diffère de la personne dans l'image vidéo traitée par le service Respondus Monitor.

La liste des données qui relèvent du droit à la protection des renseignements personnels est longue, mais n'est pas exhaustive. Les renseignements personnels effectivement collectés ne sont pas tous énumérés, ce qui porte atteinte au droit à l'information des personnes dont les renseignements sont collectés, ainsi qu'au principe du consentement. À la lecture des conditions contractuelles générales, les imprécisions font douter de leur conformité avec les lois de protection des renseignements personnels, en particulier leurs finalités trop larges. Ainsi, les principes de minimisation, de nécessité et de proportionnalité ne semblent pas respectés.

Quant à la conservation des données, les lois provinciales de protection des renseignements personnels dans le secteur public reconnaissent des droits de suppression[99]. La politique de confidentialité de Respondus[100] précise 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 en vertu d'obligations similaires applicables aux activités commerciales ou de la durée nécessaire 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 règne une certaine imprécision quant à la durée de conservation des données, en particulier en ce qui concerne les « objectifs commerciaux légitimes ». Ce flou semble être en contradiction avec les politiques de confidentialité des universités. Par exemple, l'Université d'Ottawa[101] indique sur son site Internet que « [l]es vidéos des sessions [*sic*] d'examen sont stockées dans les serveurs Respondus

99. *Loi sur l'accès* ontarienne, *supra* note 89, art 40(1) : « L'institution qui s'est servie des renseignements personnels les conserve durant le délai prescrit par les règlements afin de fournir l'occasion au particulier concerné par ces renseignements d'y obtenir lui-même accès. »

100. *Ibid*.

101. Université d'Ottawa, « Respondus » , *supra* note 51, sections FAQ pour les professeurs et les étudiants.

pendant un an » à compter de la fin du trimestre, en fonction du délai de contestation possible des notes en cas de litige. Polytechnique Montréal utilise ProctorExam[102] 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. Les conditions d'accès, de mise à jour et de suppression des données varient selon le système et l'université et peuvent s'avérer ambiguës ou contradictoires.

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

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

S'agissant d'abord du consentement à la collecte des renseignements personnels dans les relations entre les universités et les étudiants, les lois du **secteur public**, tant provinciales que fédérale, ne consacrent pas un 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 est réalisée dans un des buts suivants : autorisation de la loi ; réalisation d'un programme ou d'une activité d'un organisme public ; mise en application des lois[103]. En conséquence, la loi permet aux universités de collecter les renseignements personnels des étudiants dans le cadre de leur mission. 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[104]. Ils sont utilisés aux fins

102. Polytechnique Montréal, « Mention légale relative à la protection des renseignements personnels » (s.d.), en ligne (pdf) : *Polytechnique Montréal* : <www.share.polymtl.ca/alfresco/service/api/path/content%3Bcm:content/workspace/SpacesStore/Company%2520Home/Sites/etudes-web/documentLibrary/examens-finaux/Mention_legale_Proctor_Exam_Accommodement_Finaux.pdf%3Fa%3Dtrue%26guest%3Dtrue&sa=U&ved=2ahUKEwiD-eqH3ND7AhWuD1kFHRkKCgoQFnoECAAQAQ&usg=AOvVaw3-Cwv5R1VYpCXUH31knm9f>.

103. Par ex, *Loi sur l'accès* ontarienne, art 40(1), *supra* note 89.

104. SO 1965, C.137.

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[105]. Au demeurant, la plupart des universités, comme l'Université d'Ottawa[106], prévoient un système de consentement de l'étudiant qui accepte les politiques de confidentialité, sans y être légalement tenues puisque la *Loi sur l'accès* ontarienne autorise la collecte[107].

Mais les entreprises technologiques souhaitant utiliser les données pour entraîner des algorithmes font alors un usage secondaire des données, ce qui requiert le consentement des personnes, conformément aux lois (fédérale et provinciales) du secteur public et du secteur privé. Dès lors, les conditions générales d'utilisation des entreprises technologiques font logiquement reposer l'utilisation et la collecte des renseignements personnels sur le consentement exprimé par les étudiants, à l'instar de Proctorio[108]. Cependant, un consentement unique est le plus souvent requis, englobant à la fois l'accord pour l'utilisation du service et la collecte des renseignements personnels, de telle sorte que les étudiants n'ont pas clairement conscience de la collecte de leurs renseignements personnels, encore moins de leur nature, de leur quantité, ni de l'utilisation qui en sera faite par la suite. Ils en ont d'autant moins connaissance que les politiques de confidentialité ne sont pas claires et exhaustives s'agissant de la nature des informations ainsi recueillies. On peut en conséquence douter du caractère libre et éclairé du consentement au traitement des renseignements personnels. En comparaison avec le droit européen de la protection des données personnelles, l'article 4(1) du RGPD définit le consentement comme étant

---

105. Université d'Ottawa, « Règlement 90 — Accès à l'information et la protection des renseignements personnels » (s.d), en ligne : *Université d'Ottawa* <www.uottawa.ca/notre-universite/politiques-reglements/reglement-90-acces-linformation-et-la-protection-des-renseignements-personnels#:~:text=Les%20membres%20de%20la%20communaut%C3%A9%20universitaire%20qui%20manipulent%20des%20renseignements,le%20jugement%20de%20l'Universit%C3%A9>.

106. Université d'Ottawa, « Respondus », *supra* note 51.

107. L'article 38(2) de la *Loi sur l'accès* ontarienne, *supra* note 89, 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.

108. Par ex, voir Université Laval, « Surveillance d'examen en télésurveillance avec Proctorio », *supra n*ote 73.

« toute manifestation de volonté, libre, *spécifique*, éclairée et univoque »[109]. L'exigence de spécificité du consentement découle clairement de l'article 7(2)2 du RGPD, qui exige que :

> [...] si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions.

En outre, l'article 7(4)4 du RGPD énonce que l'appréciation d'un consentement libre se fait en examinant la subordination du consentement au traitement de données personnelles non nécessaire à l'exécution d'un contrat[110]. Ainsi, il est clair que, dans le cadre du RGPD, un consentement non distinct, c'est-à-dire non séparé d'un autre consentement, notamment contractuel, n'est pas suffisant et remet en cause le caractère libre.

Le consentement à la mise en œuvre du système de surveillance d'examens est en revanche nécessaire au moment de l'installation des outils. Ainsi, la société Respondus prévoit que l'étudiant accepte les conditions d'utilisation de l'entreprise lors de l'installation du système, puis qu'il les vérifie et les accepte de nouveau avant chaque examen. Au demeurant, la société se réserve un droit de modification unilatérale et à tout moment des politiques de confidentialité[111]. Les étudiants sont invités à revoir les modalités à chaque début d'examen, ce qui ne paraît pas très réaliste. 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 commencer l'examen. Le consentement est donc directement lié à l'utilisation du système. Par exemple, à l'Université d'Ottawa[112], en cas de refus, le professeur doit prévoir des solutions de rechange pour la gestion des examens et des évaluations universitaires.

L'Université Laval prévoit pour sa part que l'étudiant est libre de choisir les examens en télésurveillance ou en présentiel[113]. Mais on comprend, par ailleurs, que l'examen de l'étudiant qui refuserait le

---

109. Art 4(1) RGPD, *supra* note 93 [nos italiques].

110. *Ibid,* arts 7(2)2 et 7(4)4.

111. Respondus, « Terms of Use – Respondus Monitor (Student) » (s.d.), en ligne : *Respondus* <www.web.respondus.com/tou-monitor-student/>.

112. Université d'Ottawa, « Respondus », *supra* note 51.

113. Université Laval, « Surveillance d'examen en télésurveillance avec Proctorio », *supra n*ote 73.

système ne pourra être identique à celui des autres étudiants, ce qui pose la question d'une rupture d'égalité entre ces derniers. De façon plus générale, les étudiants sont placés 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. Ce déséquilibre des pouvoirs fait douter d'une expression libre du consentement.

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

La plupart des entreprises proposant des services de surveillance d'examens sont situées aux États-Unis. Le site de l'Université d'Ottawa[114] indique clairement que les renseignements personnels peuvent être stockés à l'extérieur du Canada et soumis aux lois de l'État où ils le sont. Cette disposition n'est pas contraire à la *Loi sur l'accès* ontarienne[115], qui ne prévoit aucune obligation en la matière. Dans sa politique en matière de vie privée, Respondus indique utiliser des serveurs AWS (Amazon Web Services) situés aux États-Unis[116]. Selon les conditions contractuelles de Respondus[117], toutes les questions juridiques découlant de l'utilisation de Respondus Monitor ou qui y sont liées doivent être interprétées conformément aux lois de l'État de Washington, cela sans tenir compte des principes de conflit de lois du droit international privé.

Pour sa part, ProctorExam, mis en œuvre par Polytechnique Montréal[118], est un logiciel d'une société néerlandaise régie par le droit de l'Union européenne, et en particulier par le RGPD. Son site Internet[119] indique qu'elle fait appel à d'autres sociétés pour fournir son service, tout en restant responsable de la manière dont les tiers traitent les données. Parmi ces derniers, Amazon Web Services et Google Cloud stockent physiquement les données dans des centres situés dans l'Union européenne. L'obligation de conservation des données sur le territoire européen satisfait alors aux exigences du droit de l'Union. Cependant, ProctorExam indique aussi que « si l'établissement a donné son accord,

---

114. Université d'Ottawa, « Respondus », *supra* note 51.

115. *Supra* note 89.

116. Respondus, « Terms of Use — Respondus Monitor (Student) » (s.d.), en ligne : *Respondus* <www.web.respondus.com/tou-monitor-student/>.

117. *Ibid*.

118. Polytechnique Montréal, « Mention légale relative à la protection des renseignements personnels », *supra* note 102.

119. Proctor, « Exam, Legal & Privacy », *supra* note 94.

nous pouvons également utiliser des solutions tierces pour traiter certaines données ». 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 alors transférées du Canada vers l'Europe, puis vers les États-Unis. Les flux internationaux de données en provenance de l'Union européenne vers des pays hors de l'Union sont en principe soumis à des règles restrictives d'adéquation de la protection (arts 41 et s RGPD), mais rien n'est dit sur le respect de ces obligations.

Examity[120], utilisé par l'Université de Toronto[121], indique que la plateforme est hébergée et exploitée aux États-Unis. Sauf information contraire, les étudiants consentent au transfert de leurs renseignements personnels aux États-Unis. Si l'accès à la plateforme se fait à partir de l'extérieur des États-Unis, celle-ci indique que « le droit américain peut ne pas offrir les mêmes protections de la vie privée que le droit de votre juridiction » [notre traduction]. Le site Examity renvoie en outre à un document intitulé « *European Union and European Economic Area Resident Privacy Notice* »[122], qui fait référence à l'accord bilatéral conclu entre l'Union européenne et les États-Unis, le *Privacy Shield*, invalidé toutefois par la Cour de justice de l'Union européenne en 2020[123] ! La violation du droit de l'Union, qui exige le niveau de protection le plus élevé dans le monde, fait douter du respect des autres droits.

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[124] et

---

120. Examity, « Privacy & Security » (s.d.), en ligne : *Examity* <www.examity.com/features/privacy- and-security/>.

121. University of Toronto, « How Does Online Proctoring Work ? » (s.d.), en ligne : *University of Toronto* <www.help.learn.utoronto.ca/hc/en-us/articles/115004994514-How-does-online-proctoring-work->.

122. Examity, « Product Privacy Policy Appendix B » (s.d.), en ligne : *Examity* <www.examity.com/product-privacy-policy-appendix-b/>.

123. Cour de justice de l'Union européenne (CJUE), 16 juillet 2020, affaire C-311/18, *DPC v Facebook Ireland Ltd et Schrems*, en ligne : <www.dataprotection.ie/en/dpc-guidance/law/judgments/dpc-v-facebook-ireland-limited-schrems-july-2020>.

124. Colombie-Britannique : *Freedom of Information and Protection of Privacy Act* [RSBC 1996], c 165, art 33.1 [FIPPA] : « *A public body may disclose personal information outside of Canada only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for this Act* ».

la Nouvelle-Écosse[125]. L'Alberta[126] impose une obligation d'information dans l'hypothèse d'un transfert international des données hors du Canada.

La réforme de la *Loi sur l'accès* québécoise par la *Loi 25*, adoptée en septembre 2021[127], prévoit des dispositions sur les flux de données à l'extérieur du Québec. L'article 70.1 établit ce qui suit :

> 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

---

125. Nouvelle Écosse : *Personal Information International Disclosure Protection Act of* 2006, c 3, amendée en 2010, c 35, s 43, art 5(1) :
A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada (…).

126. Alberta*: Personal Information Protection Act*, SA 2003, c P-6.5, art 13.1 :
Notification respecting service provider outside Canada
(1) Subject to the regulations, an organization that uses a service provider outside Canada to collect personal information about an individual for or on behalf of the organization with the consent of the individual must notify the individual in accordance with subsection (3).
(2) Subject to the regulations, an organization that, directly or indirectly, transfers to a service provider outside Canada personal information about an individual that was collected with the individual's consent must notify the individual in accordance with subsection (3).
(3) An organization referred to in subsection (1) or (2) must, before or at the time of collecting or transferring the information, notify the individual in writing or orally of
(a) the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
(b) the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.
(…)

127. *Supra* note 88.

> 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.

L'Université Laval utilise Proctorio et indique aux étudiants que les données sont stockées au Canada[128]. Par ailleurs, si la LPRPDE n'interdit pas le stockage des renseignements personnels en dehors du Canada, le Commissariat à la protection de la vie privée du Canada a, à plusieurs reprises, imposé une obligation d'information au bénéfice des personnes concernées au sujet du lieu de stockage[129].

L'analyse juridique de la protection des renseignements personnels révèle ainsi des sujets d'inquiétude qui nécessitent des améliorations du droit.

IV. PROPOSITIONS

Les analyses empirique et juridique révèlent des problèmes majeurs dans la protection des renseignements personnels, qui dépassent le cas particulier des logiciels de surveillance d'examens. Plusieurs recommandations peuvent être faites concernant la modification de la LPRPDE dans un contexte où sa réforme est envisagée par le Projet de loi C-27[130]. Des améliorations pourraient concerner : les conditions de validité du consentement (A) ; la distinction entre les lois du secteur privé et celles du secteur public (B) ; la localisation des données aux États-Unis en présence d'entreprises américaines (C) ; et les clauses d'élection du for (D).

---

128. *Ibid.*

129. Par ex, Commissariat à la protection de la vie privée au Canada, « Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA PATRIOT Act* », Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2005-313.

130. PL C-27, *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, 1re sess, 44e lég, Canada, 2021, (première lecture le 16 juin 2022) en ligne : <www.parl.ca/legisinfo/fr/projet-de-loi/44-1/c-27> [Projet de loi C-27].

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

Les contrats conclus entre les étudiants et les entreprises technologiques 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 et sous le stress d'accepter l'utilisation des outils de surveillance au moment de passer leur examen. Le consentement au contrat lui-même n'est pas véritablement libre puisque les étudiants n'ont pas le choix de passer l'examen et d'accepter les conditions. Même si certaines universités prévoient des solutions de rechange aux moyens automatiques de surveillance, le refus de les utiliser entraîne une rupture d'anonymat et potentiellement d'égalité. Les étudiants pourraient donc se sentir contraints *de facto* d'accepter l'outil de surveillance. On peut noter toutefois les efforts de certaines universités, comme l'Université Laval[131], pour favoriser un consentement qui serait « libre et éclairé ».

Surtout, le consentement exprime une acceptation de deux objets différents : l'utilisation des logiciels et la collecte des renseignements personnels. Le consentement à la collecte des renseignements personnels n'est pas distinct de celui à l'utilisation du système. À l'heure actuelle, la plupart des lois au Canada n'exige pas un consentement spécifique, ce qui constitue une faiblesse quant à la protection des renseignements personnels.

Toutefois, on note une tendance au renforcement des exigences, probablement sous l'influence du droit de l'Union européenne[132]. L'article 8 de la *Loi 25* modifie la *Loi sur l'accès* québécoise, en y insérant l'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

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

132. Selon l'art. 4.11 RGPD, 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.

> requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé [nos italiques].

Ces exigences nouvelles sont à saluer, spécialement celle d'un consentement **distinct.** Appliquées aux logiciels de surveillance d'examens, ces exigences permettraient aux étudiants d'accepter l'utilisation de ces logiciels pour pouvoir passer leur examen, tout en ayant le choix de refuser la collecte et l'utilisation de leurs renseignements personnels. Certes, ils ne pourraient pas refuser la collecte et l'utilisation des renseignements nécessaires à l'activité de surveillance, mais pourraient exclure toute autre finalité. En particulier, ne serait pas autorisée l'utilisation des renseignements personnels à des fins secondaires, comme l'entraînement des algorithmes. Les entreprises technologiques seraient alors dans l'obligation d'obtenir un consentement spécifique des personnes concernées pour réaliser de tels traitements sur leurs données.

Proposition 1 : imposer un consentement distinct dans la réforme de la LPRPDE

La réforme de la LPRPDE pourrait s'inspirer de la *Loi 25* du Québec en exigeant un consentement distinct concernant l'utilisation des renseignements personnels dans le secteur privé. Il faudrait affirmer que : « La collecte et le traitement des renseignements personnels doivent nécessiter un consentement libre, éclairé et *distinct* de tout autre consentement » [nos italiques][133].

B. Inadaptation des lois sectorielles du public et du privé *versus* partenariats public-privé

Les logiciels de surveillance d'examens mis en œuvre par les universités sont proposés et conçus par des entreprises. L'utilisation de ces outils repose donc sur un partenariat public-privé et incite à se questionner sur la protection des renseignements personnels. Ainsi, si l'utilisation des logiciels de surveillance d'examens par les universités est régie par les lois provinciales du secteur public, qui s'appliquent aux relations entre les universités et les étudiants, ainsi qu'aux relations entre les universités et les entreprises, les relations contractuelles entre les étudiants et les entreprises technologiques sont quant à elles régies

133. Art. 110 de la *Loi 25*, qui modifie l'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé, supra* note 97.

par les lois du secteur privé puisque ce contrat ne fait intervenir aucun organisme public. En outre, nous avons précédemment précisé que les entreprises privées, quant à certaines de leurs activités, ne se contentent pas d'agir comme mandataires des universités publiques, ce qui suppose que les lois du secteur public sont alors exclues au profit de celles du secteur privé. Seules trois provinces (Colombie-Britannique, Alberta et Québec) ont adopté des lois de protection des renseignements personnels du secteur privé, alors que c'est la LPRPDE régissant le secteur privé qui s'applique dans les autres provinces. Cette loi présente de nombreuses faiblesses structurelles et substantielles, ce qui conduit le législateur à envisager sa réforme. En attendant, on peut émettre des doutes sur la protection effective des étudiants dans le contexte de la surveillance automatique des examens.

Plus globalement, alors que le droit canadien, fédéral et provincial, 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 proposées par des entreprises 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 perturbe la compréhension des missions publiques et le rôle joué par chacun. Cela vient aussi remettre en cause la bonne compréhension de l'utilisation des données et leur traçabilité, ainsi que la légitimité même des traitements secondaires. Le consentement recueilli auprès des personnes concernées ne semble pas suffire à permettre une bonne compréhension et une bonne application des lois. En outre, les exigences de protection des renseignements personnels contenues dans les contrats de partenariat dépendent des rapports de force, souvent déséquilibrés, entre les acteurs publics et les entreprises technologiques. Les acteurs publics, devenus dépendants des technologies, subissent une asymétrie de pouvoirs qui limite la protection effective des renseignements personnels.

Par ailleurs, le rôle joué par les acteurs publics et privés par rapport aux données n'est pas toujours très clair. La qualification des opérateurs doit être précisée, en particulier pour déterminer qui est responsable de la conformité avec la législation. Plusieurs hypothèses peuvent être envisagées : une coresponsabilité, une responsabilité unique des acteurs publics, ou encore une responsabilité principale des acteurs publics et une responsabilité secondaire des acteurs privés dans une relation de sous-traitance. La qualification des parties et le partage des

responsabilités dans un contexte de sous-traitance et d'utilisation secondaire des données par une entreprise tierce doivent être clarifiés dans la loi elle-même. Compte tenu du risque de déséquilibre entre les parties, ces qualifications ne peuvent en effet être laissées à la seule négociation contractuelle.

Proposition 2 : préciser la qualification des responsables des secteurs publics et privés

La réforme de la LPRPDE doit prévoir des règles claires de responsabilité des institutions et des fournisseurs de services (sous-traitant) responsable du traitement et du sous-traitant, lequel agit au nom du premier et pour son compte. En cas de délégation de certaines tâches administratives réalisées par des entreprises sous-traitantes utilisant des solutions technologiques, la loi devrait imposer aux parties d'apporter des précisions contractuelles sur les caractéristiques de la mission et les obligations des parties (institutions et sous-traitants). Le responsable du traitement doit aussi être rendu responsable du choix du sous-traitant.

Dans l'hypothèse d'un usage secondaire des données par le sous-traitant, ce dernier devrait devenir responsable du traitement dès lors qu'il définit lui-même les moyens et les finalités de ce traitement secondaire.

C. Entreprises américaines et localisation des données à l'extérieur du Canada

La plupart des entreprises qui mettent sur le marché des logiciels de surveillance d'examens sont américaines, ce qui pose la question du lieu de localisation du stockage des renseignements personnels. Ces entreprises imposent dans leurs conditions contractuelles le transfert des données sur les territoires d'États américains et utilisent des services de *nuage informatique*, en particulier ceux d'Amazon, aux États-Unis (AWS). Non seulement le niveau de protection y est souvent plus faible, mais 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 leurs droits, tout simplement ignorés.

En cas de transfert international des données, l'Union européenne (arts 41 et s RPGD) a mis en œuvre des dispositions pour s'assurer du

niveau de protection en exigeant une analyse d'adéquation. Au Québec, l'article 70.1 de la *Loi 25* prévoit une étude des facteurs sur la vie privée (EFVP) pour autoriser un tel transfert. La réforme de la LPRPDE devrait tenir compte de ce risque.

Proposition 3 : encadrer les flux internationaux de renseignements personnels à l'extérieur du Canada

Les flux transfrontaliers de renseignements personnels devraient être soumis à de nouvelles conditions établies par la LPRPDE. Par souci de cohérence, la solution retenue au Québec pourrait être suivie. Le législateur fédéral devrait imposer l'obligation de réaliser une EFVP avant tout transfert des renseignements personnels en dehors du territoire du Canada.

D. Entreprises américaines et clause d'élection du for aux États-Unis

Quant à la loi applicable au contrat conclu entre les étudiants et les entreprises technologiques, elle relève des règles du conflit de lois. Cependant, les contrats d'adhésion imposés aux étudiants par les entreprises technologiques américaines désignent la loi de l'État américain dans lequel elles ont leur siège social, sans laisser le choix. Ces contrats excluent conséquemment l'application des lois canadiennes.

De son côté, la LPRPDE n'a pas de compétence extraterritoriale. Cependant, les entreprises technologiques américaines ne sont pas situées au Canada, mais y mènent des activités commerciales ; aussi l'enjeu est-il de savoir si un lien de rattachement pourrait être reconnu afin d'appliquer le droit canadien. 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[134].

Les facteurs de rattachement pertinents pour déterminer ces liens sont ceux qui sont énoncés dans la décision *AT c Globe24h.com*[135] : 1) l'emplacement du public cible du site Web ; 2) la source du contenu

134. *Lawson c Accusearch Inc,* 2007 CF 125 aux para 38 à 51 ; *AT c Globe24h.com*, 2017 CF 114, [2017] 4 RCF 310, aux para 50 à 64 *[AT]*, citant l'arrêt *Société canadienne des auteurs, compositeurs et éditeurs de musique c Association canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 RCS 427 aux para 54–63.

135. *AT*, *supra* note 134.

du site Web ; 3) l'emplacement de l'opérateur du site Web ; 4) l'emplacement du serveur hôte.

Un juge qui serait saisi d'un litige touchant le respect des lois sur la protection des renseignements personnels dans le contexte de l'utilisation d'un logiciel de surveillance d'examens pourrait s'appuyer sur cette jurisprudence et, ce faisant, parvenir à appliquer les lois canadiennes. La jurisprudence relative à la compétence judiciaire dans un contexte numérique concernant des affaires visant un consommateur pourrait également être utile pour contester l'application de la clause d'élection du for. Ainsi, dans l'affaire *Douez v Facebook*[136], 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, alors 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[137], combinée à l'importance du droit à la vie privée.

S'agissant des logiciels de surveillance d'examens, l'inégalité est accrue par le fait que les étudiants n'ont pas le choix de passer l'examen, à moins de décider d'échouer ou d'accepter des solutions de rechange qui ne sont pas toujours clairement proposées et sont source d'inégalité de traitement. En outre, le déséquilibre est renforcé du fait que ce n'est qu'au moment de passer leur examen que, souvent, les étudiants découvrent les conditions générales d'utilisation des entreprises, qui sont « à prendre ou à laisser », et qu'ils ne peuvent s'informer avant de les accepter. Le rejet de la clause d'élection du for en raison du déséquilibre contractuel qu'elle créée pourrait donc être envisagée aisément dans le contexte des logiciels de surveillance d'examens.

La décision *Douez* suggère aussi 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. Ce raisonnement pourrait aussi s'appliquer par analogie au cas

136. 2017 CSC 33, [2017] 1 RCS 751 [*Douez*].

137. La doctrine de l'iniquité vient du tribunal de l'équité en Angleterre et est utilisée pour écarter les accords injustes résultant d'une inégalité de pouvoir de négociation. La doctrine exige à la fois une inégalité de pouvoir de négociation et que l'accord qui en résulte soit « déraisonnable ». Les contrats types peuvent créer une inégalité de pouvoir de négociation, en particulier, les clauses qui imposent le choix de la loi, l'élection du for et les clauses d'arbitrage forcé qui violent les attentes raisonnables d'une partie en la privant de recours possibles.

des entreprises technologiques américaines bien plus en mesure de supporter les coûts d'un litige à l'étranger que les étudiants.

Un autre exemple trouve sa source dans l'enquête concernant l'entreprise Clearview AI[138]. Cette entreprise américaine offrait les prestations d'un logiciel de reconnaissance faciale aux services de police, notamment sur le territoire canadien, en mobilisant une base de données conçue à partir de milliard d'images de visages de personnes, prélevées sur les réseaux sociaux. La base de données inclut des images de 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 »[139], 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 conclu à la violation du principe du consentement des personnes concernées.

Si le consentement des étudiants est en revanche bel et bien obtenu par les entreprises technologiques dans le cadre de la surveillance d'examens, le raisonnement mis en œuvre dans cette affaire est tout de même utile pour donner effet aux lois canadiennes. On peut ainsi considérer que l'utilisation des logiciels de surveillance d'examens par des universités canadiennes, qui conduisent à collecter des renseignements personnels d'étudiants situés au Canada, devrait entraîner la mise en œuvre du droit canadien dans les relations entre les universités et les entreprises (lois provinciales du secteur public) et dans les relations entre les entreprises et les étudiants (lois provinciales et fédérale du secteur privé). Plus encore, tant dans l'affaire *Clearview AI* que dans le cas des logiciels de surveillance d'examens, les renseignements personnels de nature biométrique sont « intrinsèquement liés à la

---

138. 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* [*Clearview AI*] (2 février 2021) *Commissariat à la protection de la vie privée du Canada*, en ligne : <www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/>.

139. *Ibid* au para 28.

personne »[140] et « particulièrement sensibles »[141]. Ils méritent donc une forte protection en droit canadien.

L'application des lois canadiennes a pu être déduite dans les affaires précitées, mais il serait souhaitable que cette solution relève de la loi pour garantir une meilleure sécurité juridique. Une solution législative éviterait les aléas, le temps perdu et le coût d'un recours judiciaire. À l'heure actuelle, le droit contractuel prime à défaut de lois, et les clauses d'élection du for conduisent nécessairement à désigner les lois d'États américains où les entreprises sont situées.

Proposition 4 : donner un effet extraterritorial à la LPRPDE

Une réforme de la LPRPDE devrait conduire à étendre son champ d'application territorial. 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, la LPRPDE devrait s'appliquer dans le contexte de collecte des renseignements personnels sur le territoire canadien. Une telle disposition devrait valoir largement, et inclure les activités numériques.

CONCLUSION

La LPRPDE présente de nombreuses faiblesses structurelles et substantielles conduisant à envisager sa réforme. Le Projet de loi C-27 a été déposé le 16 juin 2022 (et est en deuxième lecture à la Chambre des communes au moment de la rédaction de cet article), et sera débattu dans les prochains mois. Il ne tient cependant pas compte des difficultés soulevées dans la présente analyse ; aussi faut-il plaider pour que les propositions faites soient entendues.

140. *Ibid* au para 41.

141. *Ibid*.