Université de Genève – Utilisation du logiciel X.

Recommandation du 16 novembre 2020

Mots clés : Examens universitaires, données personnelles, biométrie, base légale, proportionnalité, vidéosurveillance, sous-traitance, hébergement de données personnelles, for, droit applicable, secret de fonction

Contexte : Evaluation en ligne par la plateforme X. pour les étudiants de la Geneva School of Economics and Management (GSEM) de l'Université de Genève

Bases juridiques : art. 56 al. 5 LIPAD

1. Contexte

1.1 Du projet initial

Le 28 avril 2020, l'Université de Genève (UNIGE) a pris contact avec le Préposé cantonal à la protection des données et à la transparence afin d'obtenir des conseils concernant l'utilisation du logiciel X. par la GSEM pour la passation d'examens à distance.

Il était expliqué que ce logiciel permet d'activer des mesures anti-triche, à savoir :

- Identification de l'étudiant par rapport à une photo qui sera prise lors de sa première connexion
- Prise de photo chaque 3 secondes
- Détection de l'absence de l'étudiant devant la caméra
- Détection de la présence d'une personne différente devant la caméra
- Dans le cas des examens close-book, blocage des raccourcis clavier et de l'accès au navigateur, ainsi qu'au disque dur (fonctionnalités semblables à celles du SEB – Safe Exam Browser)
- En cas de non-conformité aux mesures, une alerte sera envoyée au professeur qui la signalera aux administrateurs qui pourront visionner le déroulement de l'examen a posteriori.

Les données personnelles traitées via ce logiciel sont les suivantes : prénom, nom, adresse email, numéro d'étudiant/candidat, programme de rattachement, établissement de rattachement, réponses à une évaluation, notes d'évaluation, document d'identité, captation photographique, adresse IP, données de connexion, données biométriques (photographies du visage).

X. est une société française ayant son siège à Paris.

Le projet de contrat entre l'UNIGE et X. (licence d'utilisation de la plateforme web X. et du logiciel X.) prévoyait à son art. 17, concernant le stockage des données et leur mise à disposition, que « *Le Concédant stockera les données, à savoir les sujets des évaluations, le contenu des copies des évaluations des Utilisateurs Logiciel ainsi que les photographies des Utilisateurs Logiciel et/ou de leur(s) document(s) d'identité remontées par webcam, sur ses serveurs et tiendra à la disposition du Client ces dites données. […] Le Concédant s'engage à stocker les données pendant une période de deux (2) ans à compter de la réception de celles-ci sur son serveur à l'exception des photographies des Utilisateurs Logiciel prises par webcam en cours d'examen pour lesquelles le Concédant s'engage à les stocker pendant une période de deux (2) mois à compter de la réception de celles-ci sur son serveur. A l'issue de la période de stockage, sauf demande contraire du Client, les données seront supprimées. Dans le cas où le Client souhaiterait conserver les données au-delà de la période de stockage, un devis de stockage des données lui sera communiqué. Dans le cas où le Client souhaiterait que les données lui soient reversées sur un serveur autre que celui du Concédant, et ce, indifféremment, avant ou après l'arrivée du terme de la période de stockage, un coût pourra être supporté par le Client. Le Concédant communiquera alors au Client une proposition commerciale adaptée* ».

L'art. 18 du projet de contrat avait trait à la protection des données personnelles : « *Il est rappelé que la Plateforme a pour objet de permettre au Client d'organiser et d'administrer des sessions d'évaluation dématérialisée en salle et/ou à distance dans le cadre d'une formation pédagogique initiale ou continue. Dans ce cadre, le Concédant s'engage à traiter toute donnée à caractère personnel de l'Utilisateur Plateforme et de l'Utilisateur Logiciel en conformité avec la réglementation en vigueur applicable au traitement de ces données, conformément aux dispositions précisées en Annexe 1 ».*

Le contrat prévoyait que le droit français est applicable et qu'en cas de litige, les tribunaux français sont compétents.

L'Annexe 1 au contrat précisait notamment les obligations du sous-traitant en termes de confidentialité, l'exercice des droits des personnes concernées, le fait que toute sous-traitance ultérieure est soumise à l'approbation du responsable de traitement (ici l'UNIGE) et que des mesures de pseudonymisation et de chiffrement seront prises.

L'UNIGE avait émis une directive d'application sur les évaluations en ligne pour les étudiants qui les informe que « *durant l'épreuve : 1. La caméra interne ou externe connectée à votre ordinateur sera allumée et des photos seront prises aléatoirement à des intervalles très réguliers. 2. S'il ne s'agit pas d'un examen ouvert (OpenBook), l'accès à toutes autres applications, navigateurs Web et disque dur sera bloqué. Au cas où vous quittez votre poste ou vous êtes accompagné par des tierces personnes des alertes seront envoyées à votre professeur.* », ainsi que « *Tous les enregistrements pris durant les épreuves seront complétement détruits 2 mois après la réception du relevé de notes* ».

Aucune indication n'était communiquée quant au fait que des données biométriques seraient traitées.

Au début de la passation de l'examen, les étudiants devaient expressément accepter les prises de vue. Les étudiants avaient la possibilité d'opter pour un examen en présentiel, s'ils ne souhaitaient pas utiliser la formule prévue à distance.

1.2 De l'avis du 30 avril 2020 et des discussions subséquentes

Dans le très bref délai qui leur a été imparti, les Préposés ont rendu un avis daté du 30 avril 2020[1], dans lequel ils se sont déclarés défavorables à l'utilisation du logiciel X. selon les modalités décrites dans le cadre de la passation des examens à distance à l'UNIGE. En substance, ils ont estimé que : la solution proposée impliquait le traitement de données biométriques par un sous-traitant, par le biais de photographies des étudiants prises toutes les trois secondes, ce qui s'apparentait fortement à de la vidéosurveillance ; la question du respect du principe de la licéité du traitement de données personnelles sensibles (biométrie) se posait ; la solution retenue apparaissait problématique au regard du principe de la proportionnalité ; la soumission du contrat au droit français et tout litige à la compétence des tribunaux français posait problème ; la question de la soumission des copies d'examens au secret de fonction devait être analysée davantage.

Par la suite, l'UNIGE a émis le souhait de rencontrer les Préposés afin d'exposer les modifications qui ont suivi leur avis du 30 avril 2020. Une réunion s'est tenue le 7 mai 2020 en présence des Préposés, du Recteur, du Doyen de la GSEM, de la Directrice des affaires juridiques (et responsable LIPAD) et du chargé de communication de l'UNIGE. A la suite de la séance, les Préposés ont écrit avoir noté que :

- Il a été renoncé à ce que des photographies soient prises toutes les 3 secondes, ce qui s'apparentait à de la vidéosurveillance. A la place, une photographie sera prise environ toutes les 5 minutes, dans le but de prévenir la triche

- Les examens auront lieu « *open book* », ce qui implique que les fonctionnalités de l'ordinateur de l'étudiant ne seront pas bloquées et donc pas affectées

- De nouvelles informations vont être communiquées aux étudiants sur ces modalités, ainsi qu'une information expresse concernant l'utilisation de la biométrie

- les étudiants pourront choisir de passer l'examen en présentiel à Uni-Mail le même jour à la place d'utiliser le logiciel X.

- L'Université a vérifié auprès de X. le système de chiffrement et il lui a été confirmé que tant les données en transit que les données « *at rest* » étaient chiffrées ; s'agissant de la gestion des clés, le contrat avec X. sera amendé de sorte d'inclure l'engagement de X. que les clés ne seront utilisées qu'avec le consentement exprès de l'UNIGE et qu'un procès-verbal des accès sera tenu

- L'UNIGE négocie pour que le droit suisse soit applicable, avec un for en Suisse

- Les étudiants qui voudront obtenir une copie des images prises pendant les examens pourront envoyer un courriel au Service aux Etudiants de la Faculté (service-etudiants-gsem@unige.ch) à partir de leur adresse email UNIGE tout en précisant dans l'email s'il s'agit de toutes les photos de la session d'examens ou bien d'un examen en particulier auxquelles ils voudraient avoir accès. Ils seront informés de ceci par courriel avant l'examen.

- Seuls le responsable du service étudiants, le responsable de l'IT et le doyen auront accès aux images, en cas d'alerte

- Les photographies et les données biométriques seront détruites dans les deux mois après la fin de la passation des examens.

Les Préposés ont relevé les changements effectués. Ils ont toutefois vivement regretté que l'UNIGE ne renonce pas à utiliser de la biométrie dans le cadre d'une passation d'examens. Ils ont confirmé ne pas pouvoir valider le système utilisé, le choix étant de l'unique responsabilité de l'UNIGE. Par ailleurs, s'agissant des modalités techniques du logiciel X., il

[1] https://www.ge.ch/ppdt/doc/documentation/Avis-30-avril-2020-unige.pdf

appartenait également à l'UNIGE de s'assurer que les exigences de sécurité étaient remplies. Les Préposés ont aussi pris note du fait que le système était utilisé au vu des circonstances extraordinaires liées à la situation sanitaire et que l'UNIGE n'entendait pas poursuivre ce système en situation normale. Enfin, il convenait d'ajouter le droit d'accès des étudiants à leurs photographies et qu'un nouveau consentement éclairé devait intervenir.

De nombreux contacts sont par la suite intervenus entre les Préposés et l'UNIGE.

Le 29 septembre 2020, une nouvelle rencontre entre les Préposés et l'UNIGE s'est déroulée. La vice-Rectrice, la Directrice au Rectorat, la Directrice des affaires juridiques (et responsable LIPAD), le Chef de projet informatique et l'Adjoint au Rectorat y ont participé. Ils ont expliqué aux Préposés que dans le contexte de la pandémie de COVID-19, l'UNIGE a dû accélérer fortement le développement des examens en ligne et à distance et qu'un seul examen peut concerner jusqu'à 600 étudiants simultanément. Ils ont rappelé l'importance que les diplômes de l'UNIGE ne perdent pas de leur crédibilité, ce qui serait le cas si la fraude ne pouvait pas être prévenue. L'UNIGE a indiqué rechercher actuellement la solution la plus adaptée, qui permette à la fois de prévenir la fraude tout en respectant les règles de protection des données. L'UNIGE a encore souligné qu'en termes de santé publique, elle souhaitait tout mettre en œuvre pour que des étudiants en quarantaine ou en isolement puissent passer les examens à distance. A défaut, on pouvait craindre un non-respect de la quarantaine ou de l'isolement pour ne pas perdre une année d'études. La question de l'utilisation du logiciel X. dans le cadre de la crise sanitaire qui perdurait était donc toujours d'actualité, notamment pour les grandes cohortes d'étudiants.

Le 2 novembre 2020, les Préposés ont rencontré la Directrice des affaires juridiques (et responsable LIPAD), deux représentantes de la GSEM et Me Nicolas Capt, co-auteur (avec Me Alexis Constantincopoulos) d'une note juridique datée du 29 octobre 2020 adressée à la GSEM[2]. Ils ont pu prendre connaissance de cette dernière.

Ils ont relevé les mesures prises pour la prochaine session d'examens (janvier 2021)[3] :

- Encadrement du système de e-proctoring : adoption d'une directive d'exploitation du système de e-proctoring régulant, notamment, de manière claire et contraignante, le fonctionnement général du système, les types de données collectées, les finalités du traitement, la récolte du consentement, le droit d'accès, la procédure en cas de soupçon de fraude, le calendrier de conservation et le lieu d'hébergement des données

- Etudiants : information améliorée et permettant d'assurer le respect des principes de reconnaissabilité de la collecte et de la bonne foi, notamment par le biais de la directive d'exploitation du système de e-proctoring, laquelle sera activement mise à disposition des étudiants avant toute récolte de consentement ; mise en place d'une solution alternative (passation des examens en présentiel) pour les étudiants refusant de passer leurs examens à distance, la force majeure étant toutefois réservée (état d'urgence sanitaire éventuel)

- Aspects techniques et contractuels : changement du lieu d'hébergement des données traitées par la solution X. : les données de surveillance seront désormais exclusivement hébergées sur les serveurs de l'UNIGE et non plus en France auprès d'A. ; amendement du contrat de licence entre la GSEM et X. en ce sens que le for juridique est désormais à Genève ; minimisation de la collecte et du traitement (renonciation à collecter/traiter les données personnelles non essentielles) ; images prises à intervalles aléatoires et captation du son ; pas de fonction de fermeture automatique des pages et applications (fonction « *kill all* ») mais obligation de n'avoir aucune autre page ou application ouverte durant tout l'examen (à défaut, l'examen ne démarre pas ou s'interrompt).

[2] Nicolas Capt/Alexis Contantacopoulos, Note juridique du 29 octobre 2020.
[3] Nicolas Capt/Alexis Contantacopoulos, Note juridique du 29 octobre 2020, p. 8.

Le projet de directive d'exploitation du système de e-proctoring prévoit les modalités anti-fraude suivantes :

- Identification de l'étudiant par comparaison à une photographie prise lors de sa première connexion
- Prise aléatoire de photographies par la caméra de l'ordinateur de l'étudiant
- Captation du son par le micro de l'ordinateur de l'étudiant
- Détection de l'absence de l'étudiant devant la caméra, de la présence de tierces personnes dans le champ de la caméra ou de sons anormaux
- Pour les examens à livres fermés, impossibilité pour l'étudiant de commencer l'examen s'il n'a pas fermé l'ensemble des pages et applications et lors de l'examen, impossibilité pour l'étudiant de quitter le mode plein écran
- Envoi automatisé de notifications à l'équipe en charge du e-proctoring en cas d'anomalies détectées.

La directive précise que les données personnelles collectées sont les nom et prénom de l'étudiant, son adresse e-mail, son numéro d'étudiant, la classe, le programme et son établissement de rattachement, la langue, les réponses à l'évaluation, ainsi que la note, un document d'identité, la captation de photographie et de son, son adresse IP et les données de connexion.

En outre, selon la directive, le traitement biométrique ne fait pas l'objet d'un quelconque enregistrement et les données de surveillance sont stockées en Suisse, alors que dans un premier temps, les données d'examen sont stockées de manière chiffrées auprès du prestataire d'hébergement de X., A., et dans un second temps, sur les serveurs de l'UNIGE.

Les données sont automatiquement détruites dans un délai de 60 jours à compter de la réception par l'étudiant du relevé de notes relatif à l'examen considéré, sous réserve des cas de suspicion de fraude.

Le droit d'accès par l'étudiant à ses données personnelles est consacré. Il est prévu que son consentement soit demandé et, s'il ne consent pas, une évaluation en présentiel est possible, la directive réservant toutefois les cas de force majeure liés au Covid-19, prévoyant que dans la mesure du possible, des solutions alternatives seront proposées.

En complément de la note juridique du 29 octobre 2020, une note juridique et technique complémentaire concernant les techniques biométriques utilisées dans le contexte du dispositif d'e-proctoring X. a été adressée aux Préposés par Me Capt en date du 4 novembre 2020. Il y est précisé que le dispositif prévu ne procède qu'à des vérifications biométriques, soit à un processus d'authentification par comparaison d'une photographie de référence prise lors de la première connexion au système avec des photographies prises au début et au cours de l'examen. Il ne s'agit par contre pas de comparer les captations photographiques avec une base de données.

2. Les règles de protection des données personnelles

Les règles posées par la LIPAD concernant la collecte et le traitement de données personnelles sont les suivantes :

Notion de donnée personnelle et de donnée personnelle sensible

Par données personnelles, il faut comprendre : « *toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable* » (art. 4 litt. a LIPAD).

Par données personnelles sensibles, on entend les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles, la santé, la sphère intime ou l'appartenance ethnique, des mesures d'aide sociale, des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD).

Principes généraux relatifs à la protection des données personnelles

La LIPAD[4] énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 38 LIPAD) :

- Base légale (art. 35 al. 1 et 2 LIPAD)

Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. En outre, la loi stipule que lorsqu'il s'agit de traiter de données personnelles sensibles ou de profils de la personnalité, la tâche considérée doit soit être définie clairement par la loi, soit être absolument indispensable à l'accomplissement de la tâche en cause soit encore être nécessaire et, si c'est le cas, intervenir avec le consentement – libre et éclairé – de la personne concernée.

- Bonne foi (art. 38 LIPAD)

Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

- Proportionnalité (art. 36 LIPAD)

En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi. Plus précisément, le principe de la proportionnalité se compose de trois volets : la règle d'aptitude ou d'adéquation qui exige que le moyen choisi soit propre à atteindre le but visé, la règle de nécessité qui impose qu'entre plusieurs moyens adaptés, on choisisse celui qui porte l'atteinte la moins grave aux intérêts en cause et finalement la règle de la proportionnalité au sens étroit qui exige la mise en balance des effets de la mesure choisie sur la situation des personnes concernées avec le résultat escompté du point de vue du but visé[5]. Découle du principe de la proportionnalité que la collecte de données sensibles doit en principe intervenir à titre subsidiaire, lorsque le but peut être atteint avec des données « ordinaires »[6].

- Finalité (art. 35 al. 1 LIPAD)

Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

[4] Loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 ; RSGe A 2 08.
[5] Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2010, N. 665.
[6] Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2010, N. 676.

- Reconnaissabilité de la collecte (art. 38 LIPAD)

La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

- Exactitude (art. 36 LIPAD)

Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

- Sécurité des données (art. 37 LIPAD)

Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

- Destruction des données (art. 40 LIPAD)

Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi. Ce dernier principe touche précisément le droit à l'oubli, selon lequel, dans un cas particulier, certaines informations n'ont plus à faire l'objet d'un traitement par l'institution publique concernée.

S'agissant de la sous-traitance de données personnelles, selon l'art. 13A RIPAD[7] :

[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.

[6] Le Préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.

[7] Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 21 décembre 2011 ; RSGe A 2 08.01.

3. Appréciation

3.1 Préambule – De la situation sanitaire

A titre liminaire, les Préposés constatent la situation sanitaire particulière au sens de l'art. 6 de la loi fédérale sur la lutte contre les maladies transmissibles de l'homme du 28 septembre 2012[8] du fait de l'épidémie de COVID-19.

Ils relèvent également que par arrêté d'application de l'ordonnance fédérale sur les mesures destinées à lutter contre l'épidémie de COVID-19 en situation particulière du 19 juin 2020 et sur les mesures de protection de la population[9], le Conseil d'Etat de la République et canton de Genève a déclaré le 1er novembre 2020 l'état de nécessité, au sens de l'art. 113 de la Constitution de la République et canton de Genève du 14 octobre 2012[10].

L'article 10 dudit arrêté prévoit ce qui suit :

Article 10 – Ecole du degré tertiaire et autres établissements de formation

[1] Les activités présentielles dans les écoles du degré tertiaire sont interdites.

[2] Les activités présentielles dans les autres lieux qui dispensent de la formation de manière régulière ou occasionnelle sont autorisées si elles concernent des enfants âgés de moins de 12 ans, moyennant un plan de protection.

[3] Les activités didactiques indispensables pour la filière de formation et pour lesquelles la présence sur place est nécessaire peuvent être maintenues moyennant un plan de protection.

Les mesures prévues par cet arrêté ont effet jusqu'au 29 novembre 2020 à minuit et pourront être prolongées en cas de besoin, selon l'art. 21 al. 2 de l'arrêté.

L'utilisation des contrôles de connaissance à distance par l'UNIGE est donc nécessaire au vu de la situation sanitaire actuelle, étant précisé que la durée de cette situation est difficile à estimer.

Dans ce cadre, les Préposés comprennent qu'il appartient à l'UNIGE de s'assurer, avant et pendant un examen, de l'identité des étudiants qui le passent, afin de prévenir la triche de manière efficace et de ne pas amoindrir la crédibilité des diplômes délivrés.

Ils relèvent que le système proposé a donc trait à une période particulière et qu'il constitue une « *solution temporaire pour la session d'examens de janvier/février 2021, voire également de la session de juin/juillet 2021 et la séance de rattrapage août/septembre 2021)*[11] ». Il ne s'agit donc pas d'envisager son déploiement pérenne.

A cet égard, les Préposés constatent la disparité des solutions proposées pour la passation d'examens à distance au sein de l'UNIGE. Ils ont toutefois été informés du fait qu'une démarche globale parallèle à celle initiée par la GSEM a été mise en place, afin de trouver rapidement une solution durable à l'ensemble des facultés.

---

[8] Loi sur les épidémies, LEp ; RS 818.101.
[9] https://www.ge.ch/document/arrete-application-ordonnance-federale-mesures-destinees-lutter-contre-epidemie-covid-19-situation-particuliere-du-19-juin-2020-mesures-protection-population-du-1er-novembre-2020
[10] Cst-GE ; RSGe A 2 00.
[11] Nicolas Capt/Alexis Contantacopoulos, Note juridique du 29 octobre 2020, p. 1.

3.2 Le traitement biométrique de données personnelles

L'art. 4 litt. b LIPAD liste exhaustivement les données personnelles sensibles. Les données biométriques ne sont pas mentionnées. Il convient cependant de noter que le volet « protection des données » de la LIPAD, entré en vigueur le 1er janvier 2010, résulte d'un processus législatif initié le 7 juin 2006 par le dépôt d'un projet de loi sur la protection des données personnelles[12]. Or, le terme « biométrie », longtemps utilisé dans le seul sens d' « étude quantitative des êtres vivants », n'est aussi usité dans le sens plus restrictif d'« identification des personnes » que depuis le début du 21ème siècle.

Le même constat peut être fait au niveau du droit fédéral : l'art. 3 litt. c LPD[13] (texte entré en vigueur le 1er juillet 1993), relatif aux données personnelles sensibles, n'évoque pas non plus les données biométriques.

De la sorte, *de lege lata*, et malgré le potentiel de risques qu'elles présentent, les données biométriques constituent des données « ordinaires », étant précisé que certaines de ces données sont plus délicates que d'autres[14]. Il en va précisément ainsi des données biométriques, qui font partie de l'identité biologique et physique de l'individu et qui peuvent révéler des informations sur la race ou l'appartenance ethnique, en particulier l'empreinte du visage, même une fois numérisée[15].

Le traitement des données biométriques requiert en conséquence une attention particulière.

Si la LPD et la LIPAD ne considèrent par les données biométriques comme des données personnelles sensibles, au niveau international, la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+[16]) ou encore le RGPD[17] catégorisent les données biométriques aux fins d'identifier une personne physique de manière unique comme des données sensibles (art. 6 al. 1 Convention 108+ ; art. 9 al. 1 RGPD).

Par ailleurs, le 25 septembre 2020, la nouvelle LPD a été adoptée par les deux chambres fédérales. Selon l'art. 5 litt. a ch. 4 nLPD, les données biométriques identifiant une personne physique de manière univoque constituent des données personnelles sensibles[18]. Selon le message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, « *Par données biométriques, on entend ici les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de la voix. Ces données doivent impérativement résulter d'un traitement*

[12] PL 9870 ; LPDP (MGC 2005-2006 X A 8448 ss).
[13] Loi fédérale sur la protection des données du 19 juin 1992 ; RS 235.1.
[14] Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2010, N. 2254.
[15] Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2010, N. 2257 et N. 2278.
[16] La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ("Convention 108" ; RS 0.235.1), signée à Strasbourg le 28 janvier 1981, est entrée en vigueur pour la Suisse le 1er février 1998. L'arrêté fédéral portant approbation du Protocole d'amendement (STCE n°223) à la Convention 108 a été approuvé le 19 juin 2020 par l'Assemblée fédérale (FF 2020 5559 s.). La Convention 108+ devrait prochainement entrer en vigueur.
[17] 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 (Règlement général sur la protection des données, JO L 119 du 4 mai 2016, pp. 1 ss). Le texte est entré en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne. Ses dispositions sont directement applicables sur le territoire de l'Union européenne depuis le 25 mai 2018.
[18] FF 2020 7399.

technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel ne sera en principe pas le cas, par exemple, de simples photographies »[19].

Le Préposé fédéral n'a pas attendu la révision de la loi pour se pencher sur la problématique de la biométrie. Le 11 avril 2006, il a rendu un rapport concernant le relevé de données biométriques pour l'acquisition d'un abonnement des établissements de sports et de détente de Schaffhouse. A cette occasion, il a notamment recommandé qu'une solution de rechange, sans relevé de données biométriques, soit proposée aux clients aux mêmes coûts, et que les données biométriques des autres clients, au lieu d'être enregistrées de façon centralisée, soient stockées sur une carte à puce conservée par l'abonné. Il a également insisté sur la nécessité de fixer des délais d'effacement des données et des modèles qui se rapportent aux clients, de même que sur l'importance de rendre anonymes les données transactionnelles[20]. Il sied de souligner que les établissements visés par ce rapport relevaient du secteur privé, de sorte que la licéité du traitement n'exige pas de base légale, comme cela est le cas pour des institutions publiques.

Dans son 15ème rapport d'activités 2007/2008, le Préposé fédéral relevait notamment (p. 17 s.) : « *L'utilisation restreinte et réglementée de données biométriques pour permettre une meilleure authentification des personnes dans le cadre des contrôles d'identité et pour renforcer la sécurité des documents d'identité n'est pas contraire aux principes de protection des données. Par contre, l'utilisation de ces mêmes données à des fins d'identification est plus problématique et soulève de notre part des réserves* »[21]. Pour lui, un tel traitement de données sensibles est admissible si les finalités et les droits d'accès à ces données sont suffisamment détaillés au niveau d'une base légale au sens formel.

Dans son Guide relatif aux systèmes de reconnaissance biométrique de septembre 2009, le Préposé fédéral a examiné si les données biométriques sont des données sensibles au sens de l'art. 3 lit. c LPD (point 3.3.4) en ces termes : « *Les données biométriques sont des données personnelles. Selon les caractéristiques biométriques traitées, les données biométriques sont susceptibles de contenir des informations complémentaires relatives à la race ou à la santé ; dans ce cas il s'agit de données sensibles au sens de l'art. 3 lit. c LPD. A la lumière des recherches scientifiques menées à ce jour, l'empreinte digitale, la* ***géométrie de la main et du visage****, la numérisation de l'iris et la reconnaissance vocale entre autres contiennent des informations complémentaires relatives à la race ou la santé* » [22].

Dans un Avis 3/2012 du 27 avril 2012 sur l'évolution des technologies biométriques[23], le groupe de travail Article 29 sur la protection des données (WP 193) rappelle que le traitement des données biométriques dans un système biométrique implique en général différents processus comme l'inscription, le stockage et l'établissement de correspondances :

« - ***L'inscription de données biométriques*** *englobe tous les processus qui se déroulent au sein d'un système biométrique afin d'extraire les données biométriques d'une source biométrique et de relier ces données à une personne. La quantité et la qualité des données nécessaires durant la phase d'inscription doivent être suffisantes pour permettre une identification, une authentification, une catégorisation ou une vérification précises sans enregistrer trop de données. Le volume de données extraites d'une source biométrique au*

[19] FF 2017 6641.
[20] https://www.edoeb.admin.ch/edoeb/fr/home/actualites/medias/communiques-de-presse--archives/communiques-de-presse-2006/le-prepose-federal-a-la-protection-des-donnees-et-a-la-transpare.html
[21] https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/anciens-rapports/15eme-rapport-d-activites-2007-2008.html
[22] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/guide-relatif-aux-systemes-de-reconnaissance-biometrique.html
[23] Consulté sur https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp193_fr.pdf

cours de la phase d'inscription doit être suffisant pour permettre le traitement et le niveau de résultats du système biométrique. (…)

*- Le **stockage des données biométriques** : les données recueillies au cours de la phase d'inscription peuvent être stockées localement dans le centre d'opération où l'inscription a eu lieu (par ex., dans un lecteur) pour une utilisation ultérieure ou sur un dispositif porté par une personne (par ex., sur une carte à puce) ou elles peuvent être envoyées ou stockées dans une base de données centralisée accessible par un ou plusieurs systèmes biométriques.*

*- **L'établissement de correspondances biométriques** est le processus qui consiste à comparer des données/modèles biométriques (entrés pendant la phase d'inscription) avec les données/modèles biométriques collectés à partir d'un nouvel échantillon à des fins d'identification, de vérification/authentification ou de catégorisation »*[24].

Cet avis précise encore les éléments suivants, nécessaires à la bonne compréhension du système :

« ***Identification biométrique**. L'identification d'une personne par le biais d'un système biométrique consiste généralement à comparer les données biométriques d'une personne (acquises au moment de l'identification) avec plusieurs modèles biométriques stockés dans une base de données (autrement dit, un processus de comparaison « un-à-plusieurs »).*

***Vérification/authentification biométrique**. La vérification d'une personne par un système biométrique consiste généralement à comparer les données biométriques d'une personne (acquises au moment de la vérification) et un modèle biométrique unique stocké dans un dispositif (autrement dit, un processus de comparaison « un-à-un »)* »[25].

Un certain nombre de mesures techniques et opérationnelles sont recommandées[26], étant précisé que cet avis a été émis avant l'entrée en vigueur du RGPD.

Finalement, dans un avis du 20 mai 2020 sur le sujet, la CNIL relevait : « *En revanche, n'apparaissent à priori pas proportionnés au regard de la finalité poursuivie : les dispositifs de surveillance permettant de prendre le contrôle à distance de l'ordinateur personnel de l'étudiant (notamment pour vérifier l'accès aux courriels ou aux réseaux sociaux) ; les dispositifs de surveillance reposant sur des traitements biométriques (exemple : reconnaissance faciale via une webcam). Les traitements de reconnaissance faciale sont des dispositifs de nature biométrique particulièrement intrusifs, qui présentent des risques importants d'atteinte à la vie privée et aux libertés individuelles des personnes concernées. Les données biométriques, de manière générale, sont uniques et permettent d'identifier un individu à partir de ses caractéristiques physiques ou biologiques. Elles font, pour cette raison, l'objet d'une protection renforcée dans les textes européens et nationaux. L'utilisation de dispositifs de reconnaissance faciale ou d'autres dispositifs biométriques à des fins de surveillance des examens n'apparaît pas conforme au principe de proportionnalité, au regard de l'impact pour les droits et libertés des personnes par rapport à la finalité poursuivie. En tout état de cause, le traitement des données biométriques étant par principe interdit par le RGPD, de tels dispositifs nécessiteraient une disposition légale particulière* »[27].

[24] Avis 3/2012 du 27 avril 2012 sur l'évolution des technologies biométriques du groupe de travail Article 29 sur la protection des données (WP 193), p. 5.
[25] Avis 3/2012 du 27 avril 2012 sur l'évolution des technologies biométriques du groupe de travail Article 29 sur la protection des données (WP 193), p. 6.
[26] Avis 3/2012 du 27 avril 2012 sur l'évolution des technologies biométriques du groupe de travail Article 29 sur la protection des données (WP 193), pp. 34 ss.
[27] https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil

3.3 L'exigence de base légale

La LIPAD prévoit un régime différencié s'agissant des exigences de base légale, selon que les données traitées sont des données personnelles sensibles ou non : dans la première hypothèse, l'art. 35 al. 2 LIPAD exige qu'une loi définisse clairement la tâche considérée et que le traitement en question soit absolument indispensable à l'accomplissement de cette tâche ou qu'il soit nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée.

De la sorte, il sied d'examiner si l'UNIGE dispose d'une **base légale suffisante** pour traiter des données biométriques dans le cadre de la surveillance des examens. S'agissant des bases légales relatives aux examens au sein de l'Université et à la surveillance des étudiants dans ce contexte, l'on peut relever les dispositions suivantes : l'art. 2 al. 1 LU[28], relatif à la mission de l'institution, prévoit qu'elle est un service public dédié notamment à l'enseignement supérieur de base et approfondi ainsi que la formation continue. A teneur de l'art. 70 al. 1 du statut de l'Université[29], trois sessions d'examens sont organisées par année en règle générale. L'art. 66 du statut de l'Université stipule que les règlements d'études fixent les modalités d'examen et les conditions d'obtention de chaque titre universitaire relevant de la formation de base, de la formation approfondie et de la formation continue. Selon l'art. 72 al. 1 dudit statut, la fraude, le plagiat et leur tentative constituent des infractions graves à l'éthique de l'Université et à l'intégrité de la recherche. L'al. 2 précise que les règlements d'études fixent les sanctions académiques et la procédure. La surveillance de la fraude et du plagiat fait donc partie des missions de l'UNIGE. Il n'y a toutefois pas de base légale détaillée portant sur la manière dont cette surveillance peut intervenir.

Dès lors, cette surveillance ne peut pas inclure le traitement de données sensibles, faute de base légale formelle telle que l'art. 35 al. 2 LIPAD l'exige. Le consentement des étudiants ne saurait suppléer au manque de base légale formelle[30]. S'il est vrai que les données biométriques ne sont à ce jour pas considérées comme des données personnelles sensibles par la LIPAD, les Préposés sont d'avis qu'il convient, au vu de la nature desdites données et des changements législatifs probables, d'être très vigilant dans leur traitement.

Ainsi, les Préposés doutent que les bases légales susmentionnées soient aptes à leur faire considérer que le principe de la licéité du traitement est respecté. Même si les données biométriques ne sont actuellement pas considérées par la LIPAD comme des données personnelles sensibles, ils expriment, au vu des développements récents intervenus mentionnés *supra*, leur réticence de principe à leur usage et sont d'avis, conformément à l'art. 35 al. 2 LIPAD, qu'une loi au sens formel à cet égard est indispensable ou le sera à brève échéance. En conséquence, les Préposés invitent l'UNIGE à se doter rapidement d'une base légale expresse autorisant le recours à de la biométrie, faute de quoi le système devra être abandonné.

En outre, ils attirent l'attention de l'UNIGE sur l'éventuelle application extraterritoriale du RGPD dans le cas d'espèce, selon la publicité faite sur le territoire de l'Union européenne pour les cours concernés ou d'éventuels programmes d'échanges avec l'Union européenne. N'ayant pas d'information à cet égard, les Préposés ne peuvent se prononcer sur cette question.

On peut finalement se demander si le fait que la Suisse se trouve actuellement dans une situation particulière au sens de l'art. 6 LEp et que l'état de nécessité au sens de l'art. 113

[28] Loi sur l'université du 13 juin 2008 ; RSGe C 1 30.
[29] http://www.unige.ch/rectorat/static/statut_universite.pdf
[30] Au surplus, les Préposés émettent de sérieux doutes sur le fait que les étudiants puissent, dans un tel cas, émettre un consentement explicite, libre et éclairé.

Cst-GE a été déclaré est de nature à modifier les exigences en termes de base légale. En effet, la déclaration de l'état de nécessité donne des compétences spéciales au Conseil d'Etat pour prendre des mesures pour protéger la population. Toutefois, vu l'incertitude actuelle de la qualification des données biométriques comme des données personnelles sensibles, la question de savoir si un arrêté du Conseil d'Etat pourrait suppléer temporairement à l'absence de base légale formelle pour la surveillance d'examens via le logiciel X. peut rester ouverte.

La prise en compte de cette situation particulière interviendra en tous les cas également dans le cadre de l'examen de la proportionnalité des mesures retenues.

3.4 L'examen à l'aune de la proportionnalité

Au regard du principe de la **proportionnalité**, la solution retenue apparaît comme problématique, en tous les cas hors situation d'urgence sanitaire. S'il est légitime que, dans le cadre de la passation d'examens, des mesures d'identification, de prévention et de contrôle de la triche interviennent, ces mesures doivent être mises en perspective avec l'intrusion dans la sphère privée qu'elles peuvent causer.

Conformément à la règle d'aptitude, le moyen choisi doit être propre à atteindre le but visé. L'on peut considérer ici que tel est le cas du système envisagé, étant précisé que la fiabilité du traitement biométrique opéré (marge d'erreur du système utilisé) n'a pas pu faire l'objet d'un examen par le Préposé cantonal.

La règle de nécessité impose qu'entre plusieurs moyens adaptés pour obtenir le résultat escompté, celui qui porte l'atteinte la moins grave aux intérêts en cause soit choisi. Finalement la règle de la proportionnalité au sens étroit exige la mise en balance des effets de la mesure choisie sur la situation des personnes concernées avec le résultat escompté du point de vue du but visé.

Pour la passation d'examens à distance, des mesures moins intrusives que celles impliquant des données biométriques avaient été examinées par l'UNIGE comme le contrôle, via Zoom, des cartes d'étudiants, qui n'a pas été retenu car trop difficile à mettre en place pour des grandes cohortes d'étudiants, ou encore l'utilisation d'un module complémentaire pour Moodle, mais qui nécessitait des ordinateurs institutionnels et ne pouvait être utilisé sur les PC des étudiants. En outre, la surveillance en direct par Zoom d'examens rassemblant environ 600 étudiants aurait nécessité la présence d'un nombre tel de surveillants que l'UNIGE explique ne pas pouvoir recourir à un tel système. Finalement, l'UNIGE considère qu'un enregistrement via Zoom des sessions d'examens à visionner a posteriori lui demanderait un effort disproportionné et serait plus attentatoire à la personnalité des étudiants, car cela impliquerait la collecte de plus de données personnelles[31]. Faute de trouver une solution alternative satisfaisante, l'UNIGE a opté pour certains types d'examens, notamment ceux visant un grand nombre d'étudiants, pour la solution qui fait l'objet de la présente appréciation.

Les Préposés ne remettent pas en cause le caractère légitime d'une forme de surveillance lors de la passation des examens. Ils relèvent toutefois que la solution la moins intrusive possible pour atteindre le but visé doit être retenue. Or, pour bon nombre d'examens, il n'est pas disproportionné pour l'UNIGE de déployer un certain nombre d'assistants qui seraient à même de surveiller les étudiants via de la vidéosurveillance en direct, mode de surveillance qui s'apparente le plus à ce qui se déroule en présentiel. Ainsi une captation d'images et de son, sans traitement biométrique, afin de s'assurer que l'étudiant ne communique pas avec un tiers et demeure devant son ordinateur pendant la durée de l'examen permet de prévenir

[31] Nicolas Capt/Alexis Contantacopoulos, Note juridique du 29 octobre 2020, p. 5.

bon nombre de situations de fraude. En France, la Commission nationale de l'informatique et des libertés (CNIL) estime d'ailleurs que « *la surveillance vidéo en temps réel pendant la durée de l'examen* » et « *la prise de photographies ou de flux vidéo ou sons de manière ponctuelle ou aléatoire* »[32] n'apparaissent pas disproportionnés.

Les Préposés partagent cette analyse dans la mesure où il s'agit du mode de surveillance d'un examen à distance qui s'apparente le plus à celui que les étudiants connaissent en présentiel.

Ainsi, selon les Préposés, tant la vidéosurveillance en temps réel que la collecte envisagée d'images et de son paraissent appropriées à atteindre l'objectif d'intérêt public consistant à éviter la triche (adéquation) et semblent de surcroît être à même de conduire lutter efficacement contre la fraude (nécessité). Enfin, dès lors que seules les données nécessaires sont traitées, qu'un calendrier de conservation strict est instauré et qu'un cercle restreint de personnes autorisé à accéder aux données est défini, la collecte envisagée entretient un rapport raisonnable avec le but à atteindre (proportionnalité au sens étroit). Dès lors, limitée à la captation de son et d'images, elle répond tant aux exigences de la proportionnalité que de la légalité. En effet, la surveillance de la fraude et du plagiat fait partie des missions de l'UNIGE. Dans le cas de figure où cette surveillance se limite à la captation de son et d'image, sans traitement biométrique, elle entre donc la mission de l'UNIGE et remplit les exigences de base légale posées par l'art. 35 al. 1 LIPAD. Les questions de reconnaissabilité de la collecte et de sécurité des données doivent évidemment être respectées.

Ce mode doit être privilégié en tous les cas pour les cohortes d'étudiants qui le permettent.

Il convient alors d'examiner si, pour les examens qui visent un très grand nombre d'étudiants et pour lesquels la fraude, au vu de la nature de la matière évaluée, peut être plus facile à réaliser, l'utilisation de X. avec traitement biométrique des données saurait être utilisée et serait conforme au principe de la proportionnalité, dans la mesure où il conviendrait de considérer que les moyens de surveillance susmentionnés ne seraient pas adéquats.

Comme déjà mentionné, la CNIL s'est prononcée sur ces questions et a retenu que « *n'apparaissent à priori pas proportionnés au regard de la finalité poursuivie : les dispositifs de surveillance permettant de prendre le contrôle à distance de l'ordinateur personnel de l'étudiant (notamment pour vérifier l'accès aux courriels ou aux réseaux sociaux) ; les dispositifs de surveillance reposant sur des traitements biométriques (exemple : reconnaissance faciale via une webcam). Les traitements de reconnaissance faciale sont des dispositifs de nature biométrique particulièrement intrusifs, qui présentent des risques importants d'atteinte à la vie privée et aux libertés individuelles des personnes concernées. Les données biométriques, de manière générale, sont uniques et permettent d'identifier un individu à partir de ses caractéristiques physiques ou biologiques. Elles font, pour cette raison, l'objet d'une protection renforcée dans les textes européens et nationaux. L'utilisation de dispositifs de reconnaissance faciale ou d'autres dispositifs biométriques à des fins de surveillance des examens n'apparaît pas conforme au principe de proportionnalité, au regard de l'impact pour les droits et libertés des personnes par rapport à la finalité poursuivie* »[33].

Les Préposés ont pris note des mesures mises en place par l'UNIGE par rapport au système initial, de sorte à limiter l'atteinte aux droits des étudiants en cas d'utilisation du logiciel X. En particulier, il n'y a plus une prise de contrôle à distance de l'ordinateur personnel de l'étudiant, mais, pour les examens à livres fermés uniquement, l'impossibilité pour l'étudiant de commencer l'examen s'il n'a pas fermé l'ensemble des pages et applications, et lors de

[32] https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil
[33] https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil

l'examen, l'impossibilité pour l'étudiant de quitter le mode plein écran. Ils ont également relevé que les données de surveillance seront désormais exclusivement hébergées sur les serveurs de l'UNIGE et non plus en France auprès d'A.

Par ailleurs, ils comprennent que le système de traitement biométrique utilisé est un système non pas d'identification biométrique, mais de vérification biométrique (comparaison *« un à un »*), ce qui comporte moins de dangers pour les libertés individuelles. Ils ont également constaté que l'information faite aux étudiants a été renforcée, les délais de destruction des données prévus sont de 60 jours sauf soupçon de fraude et les personnes habilitées à visionner les images sont limitées à 3. Finalement, il reste aux étudiants la possibilité d'opter pour un autre mode d'examen, qui ne recourrait pas à un traitement biométrique.

Les Préposés sont d'avis que, malgré toutes ces cautèles, l'utilisation en soi de traitements biométriques à des fins de surveillance des examens n'apparaît pas conforme au principe de proportionnalité au sens étroit, au regard de l'impact pour les droits et libertés des personnes par rapport à la finalité poursuivie, ce, à tout le moins en période « *normale* ».

Toutefois, les Préposés sont conscients que la situation actuelle pose des défis spécifiques aux institutions publiques, qui doivent faire preuve d'une flexibilité et d'une agilité accrues pour répondre à des intérêts parfois contradictoires. Ils notent également qu'il est dans l'intérêt des étudiants de pouvoir passer leurs examens dans les délais prévus et que lesdits examens bénéficient d'une reconnaissance de validité. Ainsi, ils considèrent que dans le cadre de la situation extraordinaire ou particulière au sens de la LEp, l'examen de la proportionnalité doit être adapté en conséquence et la pondération des intérêts doit prendre en compte le caractère extraordinaire de la situation. L'association Privatim[34] l'avait par ailleurs relevé dans le cadre de l'utilisation d'outils de collaboration digitale durant la première vague de la Covid-19[35]. Ainsi, les Préposés considèrent qu'une utilisation du logiciel X. pendant la crise sanitaire est tolérable, même si le respect des règles de protection des données personnelles ne peut pas être considéré comme parfaitement respecté. Cette tolérance ne saurait toutefois s'appliquer à tous les examens de l'UNIGE, mais uniquement à ceux qui remplissent au moins les deux critères cumulatifs suivants : un nombre d'étudiants rendant impossible un autre moyen de surveillance moins intrusif (soit des cohortes dépassant les 200 étudiants) et des examens dont la typologie implique que la fraude est plus facile à réaliser (ex : examen sous forme de QCM).

3.5 La sécurité des données

3.5.1 Le recours à un sous-traitant

Dans leur avis du 30 avril 2020, les Préposés ont estimé, au vu du projet de contrat entre l'UNIGE et X., que les conditions de l'art. 13A al. 2 à 6 RIPAD semblaient respectées (stockage des données dans l'Union européenne (pays avec un niveau de protection adéquat), possibilité réservées de faire des audits, sous-traitance en cascade soumise à l'approbation écrite de l'UNIGE).

Ils avaient cependant relevé que la gestion des examens à distance par l'intermédiaire d'un sous-traitant (société A.), amené à traiter les données personnelles des étudiants posait problème. Ils avaient rappelé qu'une analyse telle que la propose Privatim dans son « Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud »[36] faisait apparaître un certain nombre de facteurs de risques : droit applicable et for en France, traitement des données en France, pas de certification ISO du sous-traitant pour le moment,

[34] L'association Privatim est la Conférence des Préposé(e)s suisses à la protection des données.
[35] https://www.privatim.ch/fr/collaboration-digitale-pendant-la-crise-du-corona/
[36] https://www.privatim.ch/wp-content/uploads/2019/12/privatim_Aide-memoire_Cloud_v2_1_20191217.pdf

sous-traitant du sous-traitant potentiellement soumis au Cloud Act, indications à ce jour encore lacunaires concernant le chiffrement (par qui est-il effectué ? par l'UNIGE ou par le fournisseur, auquel cas il faudrait alors au moins prévoir contractuellement qu'il s'engage à ne les utiliser qu'avec le consentement exprès de l'organe public, ainsi que tenir un procès-verbal des accès, notamment).

Les Préposés saluent le fait que, dorénavant, les données de surveillance (photographies et son) seront exclusivement hébergées sur les serveurs de l'UNIGE. X. ne pourra accéder à ces données que pendant la session d'examens et uniquement à des fins de support informatique (pour autant que l'UNIGE donne son consentement et qu'un journal des accès soit tenu) ; elle n'aura plus aucun accès aux données de surveillance dès la fin de la session[37].

Par ailleurs, les copies d'examens, corrigées automatiquement ou semi-automatiquement par le logiciel, sont initialement stockées auprès d'A., prestataire d'hébergement de X., de manière chiffrée, puis sur les serveurs de l'UNIGE, une fois que l'enseignant a validé la correction et exporté le tableau des points[38].

Etant entendu que le stockage des copies d'examens par X. intervient de manière temporaire et seulement à des fins techniques, le système proposé semble prévoir des cautèles importantes au regard de la sécurité des données. Toutefois, les Préposés n'ayant pas connaissance des termes contractuels entre X. et son hébergeur notamment, ils ne peuvent se prononcer sur ce point de manière définitive, à ce stade.

En outre, ces derniers prennent note à satisfaction du fait que, dorénavant, le for juridique se situe à Genève. En revanche, il demeure peu heureux que le contrat demeure soumis au droit français.

3.5.2 Le respect du secret de fonction

Dans leur avis du 30 avril 2020, les Préposés ont laissé en suspens, vu la brève échéance qui leur était impartie, la question de savoir si les copies d'examens étaient couvertes par le secret de fonction. Si tel était le cas, il conviendrait d'examiner dans quelle mesure la sous-traitance de ces données serait compatible avec l'art. 13A al. 1 RIPAD.

Aux termes de l'art. 28 al. 1 du Règlement sur le personnel de l'Université[39], « *[1] Les membres du corps enseignant sont soumis au secret de fonction pour toutes les informations dont ils ont connaissance dans l'exercice de leurs fonctions dans la mesure où la loi sur l'information du public et l'accès aux documents, du 5 octobre 2001, ne leur permet pas de les communiquer à autrui. [2] L'obligation de garder le secret subsiste après la cessation des rapports de service. [3] La violation du secret de fonction est sanctionnée par l'article 320 du code pénal. [4] L'article 11 du code de procédure pénale, du 29 septembre 1977, est réservé. [5] L'autorité supérieure habilitée à lever le secret de fonction des membres du corps enseignant et des vice-recteurs au sens de l'article 320, chiffre 2 du code pénal est le recteur. Le conseiller d'Etat en charge du département de l'instruction publique est compétent pour lever le secret de fonction du recteur* ».

Au vu de cette définition, les Préposés sont d'avis que les copies d'examens doivent être considérées comme des informations soumises au secret de fonction.

[37] Nicolas Capt/Alexis Contantacopoulos, Note juridique du 29 octobre 2020, p. 7.
[38] Nicolas Capt/Alexis Contantacopoulos, Note juridique du 29 octobre 2020, p. 7.
[39] https://www.unige.ch/rectorat/static/reglement_personnel.pdf

En l'occurrence, si les données personnelles chiffrées seront conservées sur les serveurs de l'UNIGE, deux employés de X. pourront avoir un accès temporaire aux données, pendant la session d'examens, à des fins de support informatique seulement (pour autant que l'UNIGE donne son consentement et qu'un journal des accès soit tenu).

Se pose donc la question de savoir si le fait que les étudiants consentent à l'utilisation de X. est compatible avec le respect de l'art. 13A al. 1 RIPAD. En effet, « *Le consentement préalable de l'individu concerné par le contenu du secret peut en principe constituer un fait justificatif à la violation d'un secret. Pour que le consentement donné par l'individu soit valable, il doit en outre être donné librement. Cela signifie que l'individu ne doit pas avoir subi de menace ou de pression déraisonnable de la part de l'auteur, et qu'il ne doit pas subir de préjudice en raison de son refus. Le recours au consentement fonctionne bien pour le secret professionnel, mais rarement pour le secret de fonction. La doctrine admet certes de manière exceptionnelle qu'un consentement est suffisant pour permettre de lever le secret de fonction lorsque seul l'intérêt privé de celui qui consent est en jeu et à l'exclusion d'un quelconque intérêt public au maintien du secret* »[40].

Les Préposés restent perplexes sur la notion de consentement donné librement. Toutefois, il existe une solution alternative consistant en la passation des examens en présentiel et dans le cas présent, l'intérêt privé de celui qui consent est central, de sorte que de manière exceptionnelle, au vu de la situation particulière à laquelle l'UNIGE est confrontée et du type de données personnelles dont il est question (copies d'examens sans données sensibles), l'on peut considérer ce consentement comme suffisant. Dans cette appréciation encore, le rôle du contexte sanitaire joue un rôle clé.

4. Conclusion

Au vu de ce qui précède, les Préposés considèrent que l'utilisation d'un logiciel d'e-proctoring tel que X., faisant usage de technologie biométrique, n'est pas proportionnée dans le cadre de la passation d'examens académiques au regard de l'intrusion qu'elle implique dans la sphère privée des personnes concernées.

Néanmoins, ils relèvent qu'en cas de situation particulière ou extraordinaire au sens de la loi sur les épidémies, la pondération des intérêts doit prendre en compte le caractère extraordinaire de la situation. Dès lors, ils estiment que l'utilisation du logiciel X. est tolérable, dans ce contexte uniquement, et moyennant le strict respect des conditions cumulatives suivantes :

- L'examen visé concerne un nombre d'étudiants rendant impossible un autre moyen de surveillance moins intrusif (soit des cohortes dépassant les 200 étudiants)

- L'examen visé a une typologie qui implique que la fraude est relativement facile à réaliser en envoyant un tiers à la place de l'étudiant (ex : examen sous forme de QCM)

- Un étudiant ne souhaitant pas se voir imposer un traitement biométrique de ses données se voit offrir un choix alternatif (passation de l'examen en présentiel ou autre), quelles que soient les contraintes liées à la situation sanitaire

- Le strict respect des mesures prises par l'UNIGE par rapport au système initial et mentionnées ci-dessus (à savoir notamment l'encadrement du système d'e-proctoring via l'adoption d'une directive d'exploitation, une information détaillée aux

[40] Sylvain Métille, L'utilisation de l'informatique en nuage par l'administration publique, PJA 2019, p. 615. Cf. également CR CP II-Jean-Marc Verniory, N 52 ad art. 320.

étudiants, et les changements apportés au contrat liant l'UNIGE à X., ainsi que toute autre mesure présentée dans le but de limiter l'atteinte aux droits des personnes concernées telle le strict délai de conservation des données ou la limitation du visionnement des images).

Ainsi, au vu de ce qui précède, les Préposés recommandent donc à l'UNIGE de renoncer à l'utilisation du logiciel X., sauf durant la période particulière ou extraordinaire au sens de la loi sur les épidémies, mais pas au-delà de la session de juin-juillet 2021, et dans le strict respect des conditions susmentionnées.

Pour rappel, selon l'art. 56 al. 5 LIPAD, si cette recommandation est rejetée ou n'est pas suivie, les Préposés peuvent porter l'affaire, pour prise de position, auprès des instances mentionnées à l'art. 50 al. 2, puis recourir contre la prise de position de ladite instance, laquelle est assimilée à une décision au sens de l'art. 4 PA[41].

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal

[41] Loi sur la procédure administrative du 12 septembre 1985 ; RSGe E 5 10.