Université de Genève – Projet d'utilisation du logiciel X.

Avis du 30 avril 2020

Mots clés: Données personnelles, biométrie, base légale, proportionnalité, sous-traitance

Contexte: Evaluation en ligne par la plateforme X. pour les étudiants de la GSEM

Bases juridiques: art. 56 al. 3 litt. c LIPAD

1. Contexte

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

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 1, 3 et 4, 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.) prévoit 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 contrat a 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 prévoit que le droit français est applicable et qu'en cas de litige, les tribunaux français sont compétents.

L'Annexe 1 au contrat précise 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 a 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'est communiquée quant au fait que des données biométriques sont traitées.

Au début de la passation de l'examen, l'étudiant devra expressément accepter les prises de vue.

Les étudiants ont la possibilité d'opter pour un examen en présentiel, s'ils ne souhaitent pas utiliser la formule prévue à distance.

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

La LIPAD 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.

- 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.

- 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 :

[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.

3. Appréciation

Les Préposés retiennent que la solution ici envisagée par l'UNIGE a pour but de permettre d'organiser des examens à distance tout en prévenant la fraude de manière efficace. Cette solution implique le traitement de données biométriques par un sous-traitant, par le biais de photographies des étudiants prises toutes les trois secondes. Cette solution, bien qu'elle ne constitue pas formellement de la vidéosurveillance, s'y apparente énormément.

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.

Si les données biométriques ne figurent pas dans la liste des données sensibles au sens de l'art. 4 litt. b LIPAD, il sied de souligner que des processus de révisions des lois de protection des données ont été entamés depuis plusieurs années. Parmi ces projets, la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108+) ou encore le RGPD 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). Le projet de loi relatif à la modification de la LPD prévoit également que la notion de données sensibles soit étendue aux données biométriques (FF 2017 p. 6594). Ainsi, bien que la LIPAD n'ait pas expressément listé les données biométriques comme des données sensibles, le traitement de ce type de données requiert une attention particulière.

Pour rappel, la biométrie regroupe l'ensemble des techniques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales, en l'espèce, le visage. Selon la CNIL, « *ces caractéristiques ont la particularité d'être uniques et, pour la plupart, permanentes. Elles sont en effet produites par le corps lui-même et le caractérisent de façon définitive. Elles peuvent être utilisées pour suivre et identifier un individu, même à son insu. Contrairement à un mot de passe, ces données peuvent ne pas être communiquées consciemment et ne peuvent pas être modifiées, y compris en cas de compromission* »[1].

Ainsi, 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'article 2 alinéa 1 de la loi sur l'Université (LU), relatif à la mission de l'UNIGE, 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'article 70 alinéa 1 du statut de l'Université, trois sessions d'examens sont organisées par année en règle générale. L'article 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'article 72 alinéa 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'alinéa 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'Université. 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. S'il est vrai que les données biométriques ne sont à ce jour pas considérées comme des données 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. Toutefois, vu que les données biométriques ne sont actuellement pas considérées par la LIPAD comme des données sensibles, cette question peut être laissée ouverte.

Au regard du principe de la **proportionnalité**, la solution retenue apparaît comme problématique. S'il est légitime que, dans le cadre de la passation d'examens, des mesures

[1] https://www.cnil.fr/fr/biometrie-disposition-de-particuliers-quels-sont-les-principes-respecter

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.

Comme mentionné préalablement, les mesures de contrôle envisagées impliquent d'une part des données biométriques et d'autre part une prise de photos à intervalle régulier (toutes les trois secondes) qui s'apparente à de la vidéosurveillance.

Pour la passation d'examens à distance, des mesures moins intrusives 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 vu le grand nombre d'étudiants concernés, 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. Faute de trouver une solution alternative, l'UNIGE a opté pour certains types d'examens pour la solution qui fait l'objet de la présente appréciation.

Les Préposés comprennent les difficultés auxquelles sont confrontées les universités et hautes écoles s'agissant de la passation d'examens dans le contexte du covid-19. Ils sont conscients qu'il s'agit d'une situation exceptionnelle qui requiert beaucoup de flexibilité et de capacité d'adaptation. Ils relèvent, comme susmentionné, que le caractère légitime d'une forme de surveillance lors de la passation des examens n'est évidemment pas remis en cause. Toutefois, le principe de la proportionnalité comporte certaines exigences dont il n'est pas possible de faire fi, même dans le cadre de la situation exceptionnelle actuelle. Or, conformément au principe de proportionnalité, l'UNIGE ne peut collecter et traiter que les données qui sont objectivement nécessaires pour atteindre le but poursuivi, pour autant que le traitement demeure dans un rapport raisonnable entre le résultat (légitime) recherché (contrôle de la triche) et le moyen utilisé, tout en préservant le plus possible les droits des personnes concernées. En l'espèce, l'utilisation de données biométriques couplé à un système qui s'apparente à de la vidéosurveillance ne préserve pas suffisamment les droits des personnes concernées ; le moyen apparaît comme disproportionné par rapport au résultat escompté.

En outre, d'autres difficultés apparaissent au niveau de la reconnaissabilité de la collecte et de la bonne foi. Les documents présentés aux étudiants ne laissent notamment pas suffisamment apparaître que des données biométriques sont en jeu.

Finalement, les Préposés relèvent que la gestion de cet examen à distance intervient par l'intermédiaire d'un **sous-traitant** qui sera donc amené à traiter les données personnelles des étudiants. Dans le cadre de l'examen préliminaire que le bref temps mis à disposition de l'autorité a permis, il apparaît que, au vu du projet de contrat entre l'UNIGE et X., les conditions de l'art. 13 A al. 2 à 6 RIPAD semblent 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), même s'il est peu heureux que le contrat soit soumis au droit français et tout litige à la compétence des tribunaux français. Toutefois, une analyse telle que la propose PRIVATIM[2] dans son « aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud » fait 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, 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).

[2] https://www.privatim.ch/wp-content/uploads/2019/12/privatim_Aide-memoire_Cloud_v2_1_20191217.pdf

En outre, une question que les Préposés laissent en suspens, vu la brève échéance qui leur est impartie, a trait à celle de savoir si les copies d'examens sont 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.

4. Conclusion

Au vu de ce qui précède et bien qu'une option alternative de passation des examens soit laissée au choix des étudiants, **les Préposés sont défavorables** à l'utilisation du logiciel X. selon les modalités décrites dans le cadre de la passation des examens à distance à l'UNIGE.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal