_swissprivacy.law

La légalité de la surveillance numérique des examens universitaires à distance

Alexandre Flückiger, le 10 décembre 2020

La surveillance d'examens à distance à l'aide d'outils informatiques constitue indubitablement une restriction aux droits fondamentaux des étudiantes et étudiants. Dans cette contribution, le prof. Alexandre Flückiger examine cette problématique très actuelle sous l'angle de la base légale nécessaire pour une telle restriction (art. 36 Cst.). Sans préjuger la question de la proportionnalité, il parvient à la conclusion qu'à défaut d'une base légale formelle claire, une surveillance recourant à la biométrie, à l'intelligence artificielle ou à l'enregistrement vidéo nécessite un consentement explicite, libre et éclairé des personnes examinées. Une base légale matérielle ne peut suffire que pour une surveillance vidéo simple sans enregistrement, pour autant qu'elle émane des instances participatives de l'Université.

1 Introduction : la recommandation des préposés à la protection des données et à la transparence

Les préposés genevois à la protection des données et à la transparence ont rendu le 16 novembre 2020 une recommandation autorisant l'usage d'un logiciel couplant biométrie, intelligence artificielle et enregistrement sonore et vidéo afin d'automatiser la vérification d'identité et la surveillance des examens à l'Université de Genève (en l'espèce l'outil de *e-proctoring* TestWe)[1].

Les préposés recommandent ce logiciel pour les seules sessions de janvier/février et de juin/juillet 2021 à condition de n'être utilisé que pour les examens « dont la typologie implique que la fraude est plus facile à réaliser » (notamment QCM) et réunissant plus de 200 personnes. Les préposés recommandent également d'adopter une directive d'exploitation, de donner une information détaillée aux destinataires, d'adapter le contrat, de limiter le délai de conservation des données ainsi que du visionnement des images. Dans tous les cas, les personnes examinées devraient disposer d'un droit à passer l'examen sous un mode alternatif (examen en présentiel ou autre) quelles que soient les contraintes liées à la situation sanitaire.

Dans la mesure où une telle surveillance restreint les droits fondamentaux des personnes

examinées, celle-ci doit être prise dans l'intérêt public, reposer sur une base légale et rester proportionnée (art. 43 Cst. GE ; art. 36 Cst.).

2 L'intérêt public à prévenir la fraude

Sous l'angle de l'intérêt public, la mise en œuvre des règles prévenant la fraude universitaire s'impose. Un établissement de formation ne saurait les rendre illusoires au risque de miner la qualité de sa formation, d'éroder la confiance dans la qualité de ses diplômes, de mettre en danger le public en délivrant des titres n'attestant pas des connaissances réelles de leurs titulaires ou d'éluder les principes d'équité et d'égalité des chances entre personnes examinées[2]. La surveillance électronique fait indubitablement partie des moyens envisageables pour atteindre ce but.

3 La base légale en général

3.1 L'échelle des atteintes

Sous l'angle de la base légale, il importe de distinguer selon les différentes modalités de surveillance électronique pour évaluer le degré d'atteinte.

I – L'atteinte est la plus grave en présence d'une webcam enregistrant son et image, assistée par un contrôle enregistré et automatisé :

1. de l'identité par a) des moyens biométriques classiques (reconnaissance faciale, de l'iris ou de l'empreinte vocale) ou b) de biométrie comportementale (« *behavioral biometrics* » telle l'analyse du profil de frappe au clavier) ;
2. des comportements par des algorithmes d'intelligence artificielle profilant des comportements potentiellement suspects. Les données peuvent provenir a) d'une webcam dans la pièce qui vérifie par exemple l'absence de la personne examinée devant la caméra ou la présence d'une autre personne, qui analyse la posture (mains sous la table, autres postures anormales) ou les déplacements oculaires, voire qui détecte des sons, des objets ou d'autres changements insolites. Ces données peuvent être affinées b) par des caméras spéciales et des procédés d'intelligence artificielle (*computer vision*) susceptibles de détecter des dispositifs cachés comme l'objectif d'une caméra dans un bouton ou les ondes radio d'un appareil émetteur. Enfin, les données peuvent résulter c) de dispositifs de surveillance biométriques portables (montres intelligentes, bracelets de fitness) qui analysent les mouvements, le pouls ou la température corporelle des candidats et candidates[3].

3. de l'environnement de travail (enregistrement, vérification, prise de contrôle ou blocage de l'accès sur l'ordinateur personnel au disque dur, aux messageries, aux réseaux sociaux ou à d'autres programmes).

II – En l'absence des automatismes de surveillance précédents, mais en présence d'un suivi en temps réel par caméra comprenant un enregistrement sonore et vidéo, l'atteinte n'est pas aussi importante mais reste d'une certaine gravité.

III – L'atteinte est la plus faible en présence d'une seule surveillance vidéo en temps réel sans enregistrement.

3.2 La surveillance par vidéo, biométrie et intelligence artificielle

De la gradation précédente découlent les conséquences suivantes : plus l'atteinte est grave, plus la densité et le niveau normatifs doivent être élevés. Bien que la légalité s'applique moins strictement pour le corps estudiantin qui est dans un rapport de droit spécial avec l'État, une base légale formelle reste exigible si l'atteinte est grave[4].

Tel est le cas de l'hypothèse I-i. Les contrôles biométriques comprennent des données personnelles sensibles nécessitant une base légale formelle en droit de la protection des données européen (UE et Conseil de l'Europe)[5] et - bientôt - fédéral (art. 5 let. c ch. 4 nLPD[6]). Cela démontre le caractère potentiellement grave de l'atteinte. Les projets de lois, de même que le droit étranger ou international, pouvant être utilisés à titre interprétatif[7] et la lacune du droit cantonal n'étant sur ce point pas délibérée, les données biométriques doivent être considérées comme sensibles au sens de l'art. 4 let. b LIPAD et doivent donc reposer sur une base légale formelle claire ou un consentement explicite (art. 35 al. 2 LIPAD). Les procédés de biométrie comportementale semblent quant à eux plutôt relever d'un profilage de la personnalité, exigeant également une base légale formelle.

Une base légale formelle est également exigible pour les hypothèses I-ii et I-iii. Le déclenchement d'alarmes en cas de gestes suspects ou d'accès prohibé à l'environnement de travail laisse présumer d'une attitude frauduleuse qui conduit potentiellement à un renversement du fardeau de la preuve. Le logiciel établit par ailleurs un profil algorithmique des étudiantes et étudiants en détectant les comportements suspects. L'enregistrement de telles données permettrait ainsi d'établir un profilage simple, voire « à risque élevé », de la personne examinée au sens de l'art. 5 let. f et g nLPD. Dans le cas de figure où chaque incidence de comportement anormal devait entraîner automatiquement un point de pénalité par exemple, il conviendrait d'appliquer par analogie les règles prévues dans le futur droit fédéral sur les

décisions individuelles automatisées (cf. art. 21 nLPD). Ce type de surveillance pose également problème pour les personnes souffrant de handicaps, ne disposant pas d'un environnement suffisamment tranquille ou présentant des comportements atypiques, une couleur de peau particulière ou des caractéristiques physiques compliquant l'identification biométrique[8]. La loi formelle doit par ailleurs être suffisamment dense pour préserver la confidentialité des données et empêcher les abus[9], par exemple par l'énumération des critères de suspicion sur lesquels les algorithmes ont le droit de se reposer. Le fait de ne supprimer que l'identification biométrique ne permet donc pas d'éviter l'exigence d'une base légale formelle pour de tels systèmes, sous réserve de l'hypothèse d'un consentement explicite, libre et éclairé.

Dans les trois subdivisions de l'hypothèse I, on peut s'inspirer par analogie de la vidéosurveillance du domaine public où le Tribunal fédéral a reconnu, à la suite de la doctrine, que l'atteinte aux droits fondamentaux était la plus grave lorsque des appareils techniquement perfectionnés étaient employés ; ainsi lorsque la vidéosurveillance était « doublée d'un traitement informatisé, permettant en particulier d'établir des profils de personnalité éventuellement en couplage avec des bases de données biométriques, de suivre automatiquement une scène, d'initier des alarmes en fonction de l'analyse de comportements types ou de caractéristiques prédéfinies »[10].

3.3 La surveillance par enregistrement vidéo simple

Dans l'hypothèse II, l'enregistrement vidéo et sonore des faits et gestes d'une personne dans son domaine privé constitue également un traitement de données personnelles, en partie sensibles[11], si bien qu'une base légale formelle claire ou un consentement explicite, libre et éclairé sont exigés en vertu de l'art. 35 al. 2 LIPAD. L'enregistrement dévoile en effet des informations sur l'origine raciale ou ethnique, voire la sphère intime ou même la santé, sans exclure des données sur les activités religieuses ou politiques (p. ex. un tabouret de prière dans la pièce, un poster du Che voire des images moralement ou pénalement répréhensibles). Dans la plupart des cas, une partie de l'atteinte peut être prévenue par la collaboration de la personne examinée qui soit ôtera les éléments problématiques, soit trouvera un environnement plus neutre. Si c'est de bonne foi impossible, une localisation alternative devrait être offerte par l'institution. Limiter les mouvements de la caméra permet aussi de restreindre l'atteinte.

Expressions d'un rapport de droit public spécial, les obligations ne portant pas une atteinte grave prises en relation avec le but même de l'Université destinées à assurer la bonne marche du service public n'ont toutefois pas besoin de base légale spéciale[12]. Il en va ainsi,

par exemple, de l'organisation des cours et des examens[13]. Cependant, contrairement à la vidéosurveillance du domaine public où la liberté de déplacement est présupposée, celle d'un examen, en salle ou à distance, repose sur le précepte inverse : une limitation des libertés par une surveillance délibérée et transparente. Lors des examens présentiels, une caméra avec micro n'enregistre toutefois pas chaque personne examinée individuellement. Si l'atteinte portée par un enregistrement vidéo simple n'est pas aussi importante que dans l'hypothèse précédente, elle reste cependant d'une certaine gravité ; d'autant plus si l'on admet que des données sensibles sont enregistrées. Une base légale formelle claire ou un consentement explicite sont dès lors exigés en vertu de l'art. 35 al. 2 LIPAD.

3.4 La surveillance vidéo sans enregistrement

Dans l'hypothèse III, l'atteinte est la plus faible. Il n'y en aurait même aucune si l'on appliquait par analogie une jurisprudence constante de la CourEDH relative à la vidéosurveillance du domaine public : « S'agissant de la surveillance des actions d'un individu au moyen de matériel photo ou vidéo, les organes de la Convention ont ainsi estimé que la surveillance des faits et gestes d'une personne dans un lieu public au moyen d'un dispositif photographique ne mémorisant pas les données visuelles ne constituait pas en elle-même une forme d'ingérence dans la vie privée. En revanche, des considérations tenant à la vie privée peuvent surgir dès lors que des données à caractère personnel, notamment les images d'une personne identifiée, sont recueillies et enregistrés de manière systématique ou permanente »[14].

Une application par analogie au domaine privé ne relève pourtant pas de l'évidence : surveiller à distance l'intérieur d'un domicile, même sans enregistrement, diffère du domaine public où quiconque est susceptible d'être vu. L'atteinte reste cependant légère compte tenu tant du contexte d'un examen, qui présuppose de toute manière une supervision en présentiel, que de l'absence de données enregistrées où l'on peut admettre que la caméra se substitue simplement aux yeux et oreilles du personnel de surveillance.

Étant donné l'existence d'un rapport de droit spécial, une base légale matérielle peut suffire lors d'une surveillance vidéo sans enregistrement, pour autant selon nous qu'elle émane des instances participatives de l'Université. Dans ce cas, la légitimité démocratique que vise le principe de légalité est assurée puisque les principales personnes concernées sont directement associées au processus de décision.

Concrètement, il faudrait disposer d'un fondement clair dans le Statut adopté par l'Assemblée de l'Université de Genève et approuvé par le Conseil d'État (art. 41 de la loi sur

l'Université[15]), et/ou dans les règlements d'études approuvés par les Conseils participatifs des Facultés (art. 29 al. 1 let. a du Statut) ; le tout devant être précisé par des directives rectorales et décanales.

À défaut d'une base claire dans le Statut, une base participative claire au niveau facultaire (règlement d'études) précisée par une directive décanale pourrait suffire ; mais pour autant que ces textes reposent sur une directive rectorale autorisant les Conseils participatifs à introduire une telle surveillance, sans toutefois les y contraindre. En effet, en cas de contrainte par le Rectorat sans base claire dans le Statut, la décision de surveillance ne pourrait pas être librement prise par l'instance participative facultaire.

4 La base légale et le consentement dans la pratique genevoise

En pratique, le Rectorat de l'Université de Genève a autorisé, par directive interne révisée le 24 novembre 2020, une surveillance numérique des examens de janvier-février 2021 en limitant le choix à une surveillance par visioconférence Zoom, avec ou sans enregistrement, et à « d'autres outils numériques »[16].

Au niveau facultaire par exemple, le décanat de la Faculté d'économie et management (GSEM) a prévu et réglementé la surveillance par TestWe[17]. Le Conseil participatif de Faculté de droit a autorisé quant à lui le corps enseignant à recourir à une « surveillance ponctuelle et aléatoire » « par des outils numériques », avec ou sans enregistrement[18], en pratique par Zoom.

On ne trouve cependant pas de base légale formelle claire au niveau du Grand Conseil, ni de base matérielle au niveau du Conseil d'État. La loi sur l'Université n'ayant pas été révisée, l'état de nécessité au sens de l'article 113 Cst. GE, proclamé le 1er novembre 2020[19], aurait pourtant permis au Conseil d'État d'adopter un arrêté urgent, valant base légale formelle à titre extraordinaire et provisoire[20], dans la mesure où cette surveillance découle de la crise sanitaire.

Si une base légale permet de se passer du consentement de la personne examinée, le consentement de celle-ci permet de suppléer au défaut de base légale pour autant qu'il soit explicite, libre et éclairé (art. 35 al. 2 LIPAD). Pourtant, à propos de l'utilisation du logiciel de surveillance biométrique et algorithmique TestWe, les préposés genevois « émettent de sérieux doutes sur le fait que les étudiants puissent, dans un tel cas, émettre un consentement explicite, libre et éclairé »[21] précisant que « le consentement des étudiants ne saurait suppléer au manque de base légale formelle »[22]. À ce stade du raisonnement, on pourrait

penser que les préposés condamnent le recours à ce logiciel. Pourtant, ils concluent leur recommandation en jugeant qu'« un étudiant ne souhaitant pas se voir imposer un traitement biométrique de ses données [devrait]se voi[r] offrir un choix alternatif (passation de l'examen en présentiel ou autre), quelles que soient les contraintes liées à la situation sanitaire. »[23]

Si cette conclusion est à saluer, elle recèle toutefois une injonction paradoxale si le droit sanitaire devait interdire l'organisation d'examens en présentiel, car on serait alors face à deux ordres contradictoires. En cas d'interdiction, il ne resterait d'autre solution que de passer l'examen sous une « autre » modalité, selon la recommandation des préposés.

À ce sujet, la GSEM offre, dans l'hypothèse où les examens présentiels seraient temporairement suspendus pour « force majeure en lien avec la situation sanitaire actuelle (COVID-19) », à titre alternatif « une évaluation à distance avec une version de TestWe sans traitement biométrique »[24], mais pas sans une surveillance automatisée de certains comportements. Outre son défaut de base légale formelle, cette solution n'offre pas une véritable alternative permettant de consentir librement, car n'étant plus automatiquement identifiables par reconnaissance faciale, les candidates et candidats devront subir, contrairement aux autres, des contrôles manuels susceptibles de les prétériter tant au niveau du temps disponible que de la perte de concentration potentielle.

Par chance, ce problème semble dorénavant être théorique (provisoirement du moins), car le Conseil fédéral vient d'apporter, par révision du 4 décembre 2020, une exception à l'interdiction des activités présentielles dans les établissements de formation en vigueur depuis le 2 novembre 2020[25], en permettant d'organiser des examens en présentiels, même au-delà de 50 personnes[26].

5 Conclusion

En conclusion, à défaut d'une base claire dans la loi sur l'Université ou dans une ordonnance de nécessité du Conseil d'État, la surveillance numérique des examens de janvier/février 2021 par biométrie et/ou intelligence artificielle (TestWe) ou par simple vidéosurveillance enregistrée (Zoom) n'est admissible que si les étudiants et étudiantes y consentent de manière explicite, libre et éclairée. Les personnes candidates doivent dès lors se voir offrir, à titre alternatif, la possibilité effective d'opter pour un examen présentiel classique sans crainte de discrimination.

Seule une surveillance par simple vidéo non enregistrée peut être imposée sans consente-

ment individuel, à condition d'avoir été clairement et librement décidée par une instance universitaire participative. Ainsi, à défaut de base claire dans le Statut de l'Université, un tel fondement dans les règlements d'études, approuvés par les Conseils participatifs des Facultés et précisés par directives décanales, peut suffire à condition de reposer sur une directive rectorale autorisant les Conseils participatifs à introduire une telle surveillance, sans toutefois les y contraindre.

On précisera que cette conclusion ne présume pas la constitutionnalité de tels procédés à défaut d'avoir procédé ici à une analyse de la proportionnalité : une surveillance numérisée, reposât-elle sur une base légale suffisante, pourra toujours échouer au test de proportionnalité, comme le droit comparé le démontre.

En droit français par exemple, « 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). »[27]

Les préposés genevois parviennent, dans leur recommandation, à la fois à la même conclusion (« l'utilisation d'un logiciel d'*eproctoring* tel que TestWe, faisant usage de technologie biométrique, n'est pas proportionnée dans le cadre de la passation d'examens académiques »[28]) et à la conclusion exactement inverse au paragraphe suivant où ils en recommandent néanmoins l'utilisation, qu'ils estiment « tolérable », après une « pondération des intérêts […] [prenant] en compte le caractère extraordinaire de la situation [épidémiologique] ». La pesée des intérêts étant partie intégrante du contrôle de proportionnalité, ils reconnaissent donc implicitement - même si le raisonnement est déroutant - que l'utilisation d'un tel logiciel de surveillance est proportionnée dans le contexte sanitaire particulier de la pandémie de covid-19.

Proposition de citation : Alexandre Flückiger, La légalité de la surveillance numérique des examens universitaires à distance, 10 décembre 2020 *in* www.swissprivacy.law/42