L’utilisation d’applications de surveillance d’examen à distance

David Dias Matos, le 14 février 2022

Dans sa délibération du 11 mai 2021, la Commission Nationale de protection des données portugaise a ordonné à l’Université do Minho la cessation de l’utilisation d’applications de surveillance d’examen à distance. Ces applications sont susceptibles de violer les principes de licéité, de finalité, de minimisation des données et de proportionnalité.

Délibération de la CNPD n° 2021/622 du 11 mai 2021

La Commission Nationale de protection des données portugaise (CNPD) a rendu une décision à la suite d’une plainte déposée contre l’Université do Minho (Portugal) concernant l’utilisation de deux applications imposées par l’institution pour passer des examens à distance. La CNPD a statué avant la tenue de la session d’examens en cause.

La plainte visait l’utilisation des applications « *Respondus Lockdown Browser* » et « *Respondus Monitor* ». L’Université, responsable du traitement, a passé un contrat de licence contenant un *Data Protection Agreement* avec le sous-traitant états-unien *Respondus Inc.*, pour utiliser ses deux applications lors de sessions d’examen.

Les deux applications s’intègrent aux divers systèmes d’apprentissage à distance existant dans l’institution. Le système d’évaluation informatique présente deux composantes :

1. un navigateur internet, *Respondus Lockdown Browser*, qui bloque l’ordinateur et empêche les étudiants d’utiliser d’autres applications et certaines fonctionnalités sur leur ordinateur pendant la durée de l’examen ;
2. *Respondus Monitor* qui est un système de surveillance de l’étudiant qui analyse les données chaque seconde selon trois vecteurs concurrents. Il recourt à la détection faciale, des mouvements et de la luminosité pour analyser l’étudiant et son environnement d’examen. Le système récolte des informations sur le dispositif de l’étudiant et en identifie les tendances (*pattern*). Enfin, il analyse l’interaction de l’étudiant avec l’examen et compare les réponses entre étudiants. Un compte-rendu est ensuite envoyé à l’enseignant détaillant l’évaluation de chaque étudiant en leur attribuant à chacun une valeur relative au risque de la survenance de fraude.

Dans sa décision, la CNPD constate que l’utilisation de ces applications par l’Université est

susceptible de violer divers principes du RGPD, à savoir les principes de finalité, de licéité, de minimisation des données et de proportionnalité.

Premièrement, la CNPD constate qu'en tant que responsable du traitement, l'Université ne respecte pas le principe de finalité de l'art. 5 par. 1 let. b RGPD, qui exige de déterminer de manière précise et explicite le(s) but(s) pour lequel des données sont récoltées. La CNPD observe que les cas où les applications sont susceptibles d'être utilisées sont peu clairs et donc peu prévisibles. Cette absence de critères précis et homogènes crée un risque de discrimination entre étudiants, car le choix d'utiliser ou non les applications dépend de la volonté de chaque enseignant.

Deuxièmement, l'autorité portugaise relève que le motif justificatif invoqué par l'Université pour l'utilisation de ces applications ne peut être l'intérêt légitime de l'art. 6 par. 1 let. f RGPD. En tant qu'institution ayant pour mission la poursuite d'intérêts publics, seuls des intérêts légalement inscrits sont invocables. La CNPD ajoute que, quand bien même l'Université invoquerait l'intérêt public à la réalisation des examens, les conditions ne seraient pas remplies.

Pour cela, l'Université aurait dû démontrer l'impossibilité de faire passer ses examens d'une autre manière (en présentiel ou d'autres moyens qui n'impliqueraient pas le traitement d'autant de données personnelles). Ensuite, il aurait fallu démontrer que les intérêts privés des personnes concernées ne prévalent pas. En l'espèce, aucune démonstration d'une quelconque pesée des intérêts n'a été opérée par le responsable du traitement (art. 5 par. 2 et 24 par. 1 et 2 RGPD). Elle en conclut donc à un traitement dénué de base légale.

Troisièmement, l'art. 5 par. 1 let. c RGPD énonce le principe de minimisation en ce sens que les données récoltées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées. Selon la CNPD, le responsable du traitement traite, en plus de la détection et de la reconnaissance faciale, des données biométriques sous forme de *pattern* par l'utilisation de la souris, du clavier ou encore des mouvements corporels de l'étudiant.

Cette récolte intensive de données vise à définir, par des moyens automatisés, un profil de l'étudiant et à lui attribuer une valeur. Elle relève aussi que malgré le fait que l'enseignant prenne une décision *a posteriori* sur la valeur qui lui est présentée, cette « intervention humaine » n'est pas suffisante pour faire perdre le caractère automatisé du traitement. C'est pourquoi il s'agit d'un traitement de données sensibles aux yeux de la CNPD. À défaut d'une justification de sa licéité, il se révèle non nécessaire, excessif et viole donc l'art. 5 par. 1 let. c RGPD.

Ensuite, la CNPD considère de manière différente la position de *Respondus Inc.* dans le cadre de l'utilisation des données récoltées à ses propres fins pour améliorer ses services. L'entreprise états-unienne agit alors comme responsable du traitement. Cependant, ce traitement est déployé sans consentement valable de l'étudiant et donc sans base juridique valable. Aux termes des art. 6 par. 1 let. a et art. 4 par. 11 RGPD, le consentement doit prendre la forme d'une manifestation de volonté, libre, spécifique, éclairée et univoque. Les conditions générales des deux applications prévoient que l'étudiant doit obligatoirement les accepter pour accéder à l'examen. Cela rend le consentement invalide, car il n'est ni libre ni spécifique. Par conséquent, *Respondus Inc.* traite ces données en violation du principe de licéité de l'art. 5 par. 1 let, a RGPD.

Finalement, concernant le transfert de données vers les États-Unis, la CNPD retient que ni le *Privacy Shield* ni les *SCCs* utilisés n'étaient valides. Se basant sur l'arrêt Schrems II (cf. swiss privacy.law/17), la CNPD constate qu'ils n'offrent pas un niveau adéquat de protection des données. Selon la CNPD, il aurait fallu mettre en place des mesures supplémentaires pour garantir un niveau plus élevé.

La CNPD conclut que l'utilisation des deux applications *Respondus* viole les dispositions du RGPD et ordonne à l'Université de demander la suppression de toutes les données personnelles qui auraient déjà été récoltées par *Respondus Inc.*

En Suisse, le préposé genevois à la protection des données et à la transparence a émis une recommandation validant le recours à un logiciel « anti-triche » associant données biométriques, intelligence artificielle et enregistrement vidéo et sonore afin de surveiller les examens et confirmer l'identité des étudiants à l'Université de Genève. Selon cette recommandation, le recours à un tel logiciel devait répondre à certaines conditions notamment liées à la typologie des examens (fraude facile à réaliser) et au nombre de candidats à l'examen concerné (plus de 200 personnes).

Dans sa contribution sur swissprivacy.law, le Prof. Alexandre Flückiger a conclu qu'à défaut d'une base légale formelle claire, une telle surveillance nécessite un consentement explicite, libre et éclairé des personnes examinées. Il a cependant noté que si le raisonnement du préposé genevois soulevait des interrogations, il s'inscrivait dans le cadre très particulier de la pandémie. La recommandation aurait selon lui été différente dans un autre contexte (cf. swissprivacy.law/42).

_swissprivacy.law

Proposition de citation : David Dias Matos, L'utilisation d'applications de surveillance d'examen à distance, 14 février 2022 *in* www.swissprivacy.law/124