ALEXIS FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris
5, rue Daunou - 75002 PARIS
Tél. 01.53.63.33.10 - Fax 01.45.48.90.09
afoc@afocavocat.eu

JUGE DES RÉFÉRÉS DU

TRIBUNAL ADMINISTRATIF DE MONTREUIL

NOTE EN DÉLIBÉRÉ

N° 2216570

POUR : **L'association « La Quadrature du Net » (LQDN).**

AU SOUTIEN DE : [redacted]

CONTRE : **L'Université Paris 8**

FAITS

1. Dans l'instance n° 2216570, l'audience publique s'est déroulée le mardi 6 décembre 2022 à 14 heures 30.

2. L'exposante a pu rappeler que le traitement litigieux mis en œuvre par les décisions attaquées par [redacted] constitue un traitement de données personnelles, dont des données sensibles, qui n'est fondé sur aucune base légale et qui est manifestement disproportionné.

3. En défense, l'Université de Paris 8 a tenté d'affirmer certains éléments contredits par les pièces du dossier et la jurisprudence.

4. La présente note en délibéré vise à réaffirmer par écrit les éléments apportés par l'exposante en réplique à l'oral lors de l'audience. Elle ne modifie en rien les moyens et conclusions précédemment articulés, que l'exposante réitère expressément.

DISCUSSION

5. **En premier lieu**, il ressort des pièces du dossier, notamment le guide de l'utilisateur du logiciel « TestWe » produit le 2 décembre 2022 (*cf.* pièce n° 4), que le dispositif litigieux consiste bien en un traitement de données personnelles, dont de données sensibles.

6. Premièrement, il ressort de cette pièce que l'identité du candidat est vérifiée de manière automatisée par le dispositif litigieux, par l'analyse du visage du candidat puis la comparaison de ce visage à la photo sur la carte d'identité (pp. 9–10), et ensuite tout au long de l'épreuve (*cf.* pièce n° 4, p. 14).

7. Or, un traitement de vérification de l'identité par analyse automatisée du visage constitue un traitement de reconnaissance faciale (*cf.* mémoire en intervention du 2 décembre 2022, §§ 27–28 ; CE, 4 novembre 2020, *La Quadrature du Net*,

n° 432656, pt. 2).

8. Deuxièmement, il ressort également de ce guide de l'utilisateur que le regard est analysé. En effet, la page 13 de ce guide (*cf.* pièce n° 4) enjoint au candidat de « *Concentre*[r] *votre regard sur votre écran pendant l'examen* ». Cette même page donne des exemples de comportements constitutifs d'une potentielle fraude par l'analyse automatisée du logiciel, incluant les personnes dont le regard serait dirigé ailleurs que sur l'écran ou dont les yeux ne seraient pas visibles par la caméra – et, donc, dont le regard ne pourrait être traité par le dispositif litigieux.

9. Troisièmement, ce même guide de l'utilisateur précise sur sa dernière page que « *TestWe monitore votre environnement pendant votre examen, tout comportement suspect sera reporté à votre administration.* » Cet avertissement montre bien que le comportement du candidat, au-delà du cas de la vérification d'identité et du suivi du regard, est analysé de manière continue par le dispositif litigieux.

10. Quatrièmement, la seule captation d'images vidéo constitue un traitement de données (*cf.* CJUE, 14 février 2019, *Buivids*, aff. C-345/17, pt. 31 ; CJUE, 11 décembre 2014, *Ryneš*, aff. C-212/13, pt. 22). Il en va de même, *a fortiori*, des traitements postérieurs sur ces images captées (*cf.* CE, 22 décembre 2020, *La Quadrature du Net*, n° 446155, Rec. T. p. 750, pt. 7).

11. **Il en résulte que**, le dispositif litigieux consiste bien en un traitement de données personnelles, dont des données sensibles, par la captation des images et du son des candidats, puis par leur analyse à des fins d'identification et de détection automatisée de fraude.

12. **En deuxième lieu**, à supposer que certaines fonctionnalités soient désactivées – ce qui n'est pas démontré, ni même sérieusement allégué en l'espèce par la défense –, cette circonstance resterait, en toute hypothèse, dépourvue de toute conséquence sur la qualification de traitement de données personnelles et sur l'illégalité de ce traitement.

13. **En droit**, le considérant 26 du règlement UE n° 2016/679 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 (ci-après « RGPD »)

vient préciser la méthodologie à utiliser pour déterminer la présence ou non d'un traitement de données personnelles et savoir quelles données personnelles sont traitées :

> « [...] *Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.* [...] »

14. Autrement dit, ces « *facteurs objectifs* » sont indépendants des choix du responsable de traitement, par nature subjectifs, de ne pas utiliser certaines fonctionnalités offertes par un traitement. Le juge des référés du Conseil d'État a ainsi estimé que la promesse d'un responsable de traitement de n'utiliser un dispositif de surveillance que dans des situations ne permettant pas d'identifier les personnes est sans incidence sur la qualification du dispositif en traitement de données personnelles, à partir du moment où il est techniquement possible de ne pas respecter cette doctrine d'usage (*cf.* CE, ord., 18 mai 2020, *La Quadrature du Net et autre*, n° 440442, 440445 ; CE, 22 décembre 2020, *La Quadrature du Net*, n° 446155, Rec. T. p. 750). C'est ainsi qu'il a jugé que :

> « [...] *Alors même qu'il est soutenu que les données collectées par les drones utilisés par la préfecture de police ne revêtent pas un caractère personnel dès lors, d'une part, que l'usage qui est fait de ces appareils, tel qu'il est prévu par la note du 14 mai 2020, ne conduit pas, en pratique, à l'identification des personnes filmées et, d'autre part, qu'en l'absence de toute conservation d'images, le visionnage en temps réel des personnes filmées fait en tout état de cause obstacle à ce qu'elles puissent être identifiées, il résulte de l'instruction que les appareils en cause qui sont dotés d'un zoom optique et qui peuvent voler à une distance inférieure à celle fixée par la note du 14 mai 2020 sont suscep-*

tibles de collecter des données identifiantes et ne comportent aucun dispositif technique de nature à éviter, dans tous les cas, que les informations collectées puissent conduire, au bénéfice d'un autre usage que celui actuellement pratiqué, à rendre les personnes auxquelles elles se rapportent identifiables. Dans ces conditions, les données susceptibles d'être collectées par le traitement litigieux doivent être regardées comme revêtant un caractère personnel.

[…]

[…] *Compte tenu des risques d'un usage contraire aux règles de protection des données personnelles qu'elle comporte, la mise en œuvre, pour le compte de l'Etat, de ce traitement de données à caractère personnel sans l'intervention préalable d'un texte réglementaire en autorisant la création et en fixant les modalités d'utilisation devant obligatoirement être respectées ainsi que les garanties dont il doit être entouré caractérise une atteinte grave et manifestement illégale au droit au respect de la vie privée.* ». (*cf.* CE, ord., 18 mai 2020, *La Quadrature du Net et autre*, n° 440442, 440445, pts. 16 et 18 *in medio*)

15. Cette interprétation est rendue au visa de la directive UE n° 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (ci-après directive « police-justice ») et de son considérant 21 mais est, *mutatis mutandis*, parfaitement applicable au RGPD, ces deux textes posant la même méthodologie pour déterminer un traitement de données personnelles.

16. Or, **en l'espèce**, à supposer, pour les seuls besoins de la discussion, que certaines fonctionnalités se trouveraient désactivées – ce qui n'est pas démontré, ni même sérieusement allégué, par la défense –, cela n'aurait en toute hypothèse aucune incidence sur la qualification du dispositif en traitement de données personnelles sensibles. Le responsable de traitement (l'institut d'études à distance (IED) et/ou l'Université) pourrait très bien activer ou désactiver à sa guise ces fonctionnalités sans que rien, dans le logiciel, ne vienne l'en empêcher. Il convient donc de déterminer les contours du traitement et les données personnelles traitées non pas en

prenant en compte les fonctionnalités activées lors des examens par le responsable du traitement, mais en prenant en compte les données personnelles qui, si toutes les fonctionnalités étaient activées, pourraient être traitées par le logiciel « TestWe ».

17. **Il en résulte que** le dispositif litigieux, indépendamment des fonctionnalités qui pourraient être activées ou désactivées, constitue un traitement de données personnelles, dont des données sensibles.

18. **En troisième lieu**, les décisions attaquées sont parfaitement contestables à l'occasion d'un recours en excès de pouvoir car altérant l'ordonnancement juridique et faisant grief aux étudiants concernés. Elles ne sont nullement des mesures d'ordre intérieur.

19. **En droit**, le tribunal administratif de Marseille a déjà jugé qu'une délibération d'un conseil régional autorisant l'expérimentation de portiques de reconnaissance faciale dans deux lycées (qui constituent des traitements de données personnelles, dont des données biométriques) était une décision attaquable en excès de pouvoir (*cf.* TA Marseille, 27 février 2020, *La Quadrature du Net et autres*, n° 1901249, pts. 8, 12, 13 et 14).

20. **En l'espèce**, les décisions attaquées mettent en œuvre ou, à tout le moins, révèlent la décision de mettre en œuvre le traitement de données « TestWe ». Elles peuvent donc parfaitement être attaquées par la voie d'un recours en excès de pouvoir, comme en l'espèce.

21. **Il en résulte que** la requête de [redacted] est recevable.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, persiste dans ses conclusions.

Fait à Paris, le 7 décembre 2022

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièces déjà communiquées :

Pièce n° 1 : Statuts de La Quadrature du Net ;

Pièce n° 2 : Pouvoir spécial ;

Pièce n° 3 : Courrier daté du 25 octobre 2019 adressé par la CNIL à la ville de Saint-Étienne concernant un dispositif de surveillance algorithmique des sons ;

Pièce n° 4 : Guide utilisateur de TestWe (URL : `https://cdn.testwe.eu/docs/fr/guide_utilisateur.pdf`) ;

Pièce n° 5 : CNIL, « Surveillance des examens en ligne : les rappels et conseils de la CNIL », 20 mai 2020 (URL : `https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil`) ;

Pièce n° 6 : Position de la CNIL sur les conditions de mise en œuvre de dispositifs d'analyse algorithmique des images de vidéosurveillance dans l'espace public ;

Pièce n° 7 : CNIL, « Conformité RGPD : comment recueillir le consentement des personnes ? », 3 août 2018 (URL : `https://www.cnil.fr/fr/les-bases-legales/consentement`) ;

Pièce n° 8 : Site Internet de l'IED, page « Examens », consulté le vendredi 2 novembre à 4 heures 15 (URL : `https://www.iedparis8.net/?-Examens-`)

Pièce n° 9 : Requête en intervention volontaire produite dans l'affaire n° 2216571.

Pièce produite le 6 décembre 2022 :

Pièce n° 10 : Communiqué daté du 5 décembre 2022 du département « programmation et informatique fondamentale » de l'Université Paris 8 (URL : `https://informatique.up8.edu/actu/2022-2023.html#2022-12-05_13-12`).