

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

REQUÊTE EN INTERVENTION VOLONTAIRE

N° 2216570

POUR : L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1^{er} juillet 1901 dont le siège social est situé au 115, rue de Ménilmontant à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par [REDACTED], membre du collège solidaire en exercice.

AU SOUTIEN DE : La requête enregistrée le 14 novembre 2022 sous le n° 2216570, par laquelle [REDACTED] a demandé au juge des référés du tribunal administratif de Montreuil de suspendre, sur le fondement de l'article L. 521-1 du code de justice administrative, premièrement, la décision du 25 octobre 2022 par laquelle l'institut d'études à distance de l'université de Paris 8 a modifié l'organisation des examens au titre de l'année 2022/2023, deuxièmement, la décision du 9 novembre 2022 par laquelle le même institut a soumis les étudiants à choisir avant le 18 novembre 2022 entre examens à distance et examens en présentiel et, troisièmement, la décision du 14 novembre 2022 par laquelle le même institut a soumis les étudiants sous condition suspensive à des examens en présentiel.

Table des matières

| | |
|---|-----------|
| Faits | 3 |
| Discussion | 5 |
| I Sur l'intérêt à intervenir de La Quadrature du Net | 5 |
| II Sur la qualification juridique des faits | 6 |
| A. En ce qui concerne la qualification de données personnelles, et notamment de données sensibles | 6 |
| B. En ce qui concerne l'existence d'un traitement | 10 |
| III Sur l'urgence | 12 |
| IV Sur les moyens propres à faire naître un doute sérieux quant à la légalité des décisions attaquées | 15 |
| A. En ce qui concerne le défaut de base légale du traitement litigieux | 15 |
| 1. S'agissant du consentement | 18 |
| 2. S'agissant du respect d'une obligation légale ou de la poursuite d'une mission de service public | 20 |
| B. En ce qui concerne la disproportion du traitement litigieux | 23 |
| C. En ce qui concerne le traitement de données sensibles | 26 |
| Bordereau des productions | 30 |

FAITS

1. L'association « La Quadrature du Net » (LQDN), exposante, est investie de longue date dans la défense des droits et des libertés, notamment le droit à la vie privée et à la protection des données personnelles.
2. Par plusieurs décisions, l'institut d'études à distance (IED) de Paris 8 a imposé aux étudiants suivant une formation en son sein de passer les examens de fin de semestre à distance. Pour cela, l'usage du logiciel dénommé « TestWe », édité par la société du même nom, a été exigé. Concrètement, cela signifie que les étudiants doivent installer le logiciel « TestWe » sur leur ordinateur, donner les droits administrateurs à ce logiciel et l'utiliser pendant toute la durée de l'épreuve.
3. Le logiciel « TestWe » accède aux images filmées par la caméra et aux sons captés par le micro de l'ordinateur du candidat qui passe l'examen. Il va analyser en permanence pendant toute la durée de l'épreuve ces données pour repérer de manière automatisée une éventuelle fraude.
4. Comme il sera démontré ci-dessous, ce dispositif litigieux – le logiciel « TestWe » – consiste en un traitement de données personnelles, dont des données sensibles, souffre d'un manque de base légale et est manifestement disproportionné.
5. Par une requête datée du 14 novembre 2022 et enregistrée sous le numéro 2216571, ██████████, étudiante à l'IED de l'université Paris 8 et concernée par l'usage obligatoire du dispositif litigieux dénommé « TestWe », a demandé au tribunal administratif de Montreuil d'annuler plusieurs décisions. Il s'agit de la décision du 25 octobre 2022 par laquelle l'IED a modifié l'organisation des examens au titre de l'année 2022/2023, la décision du 9 novembre 2022 par laquelle il a soumis les étudiants à choisir avant le 18 novembre 2022 entre examens à distance et examens en présentiel, et la décision du 14 novembre 2022 par laquelle il a soumis les étudiants sous condition suspensive à des examens en présentiel.
6. Parallèlement, par une requête datée du 14 novembre 2022 et enregistrée sous le numéro 2216570, ██████████ a demandé au juge des référés de ce tribunal de suspendre, sur le fondement de l'article L. 521-1 du code de justice

administrative, ces décisions.

7. Par un mémoire en défense daté du 25 novembre 2022, l'Université Paris 8 a conclu au rejet de la requête.

8. Par un courrier daté du même jour, le greffe du tribunal administratif de Montreuil a informé [REDACTED] que l'audience publique se tiendra le 6 décembre 2022 à 14 heures 30.

9. C'est l'instance à laquelle l'exposante souhaite intervenir, après avoir présenté une requête en intervention volontaire le 2 décembre 2022 dans l'instance n° 2216571 (*cf.* pièce n° 9).

DISCUSSION

I. Sur l'intérêt à intervenir de La Quadrature du Net

10. D'emblée, il convient de relever que l'association exposante est bien recevable à intervenir au soutien de la requête susmentionnée.

11. L'association « La Quadrature du Net » (LQDN) promeut et défend les libertés fondamentales dans l'environnement numérique. Elle lutte contre la surveillance généralisée, que celle-ci vienne des États ou des acteurs privés, et contre le fichage généralisé. Elle a notamment pour objet, aux termes de l'article 3 de ses statuts constitutifs, la promotion et la défense « *des réseaux – notamment Internet – libres, ouverts, distribués, neutres et éthiques* », « *du droit à l'intimité, à la vie privée, à la protection de la confidentialité des communications et du secret des correspondances et à la protection des données à caractère personnel* », ou encore « *de la liberté d'expression, la liberté d'accès à l'information et la lutte contre la censure* ». La poursuite de cet objet statutaire peut notamment se faire par « *la mise en œuvre d'actions juridiques et de contentieux* ».

12. L'exposante est régulièrement amenée à défendre les droits et libertés fondamentaux devant le Conseil d'État¹ et le Conseil constitutionnel français², ainsi que devant le juge de l'Union européenne³.

1. CE, 21 avril 2021, n^{os} 393099, 394922, 397844, 397851, 424717, 424718; CE, 13 avril 2021, n^o 439360, 440978, 441151, 442307, 442317, 442363, 443239; CE, ord., 4 janvier 2021, n^{os} 447970, 447972 et 447974 (trois affaires); CE, 16 octobre 2019, n^o 433069; CE, 18 octobre 2018, n^o 404996; CE, 26 juillet 2018, n^{os} 394924, 394922, et 393099 (trois affaires); CE, 21 juin 2018, n^o 411005; CE, 18 juin 2018, n^o 406083; CE, 25 octobre 2017, n^o 411005; CE, 17 mai 2017, n^o 405792; CE, 18 novembre 2016, n^o 393080; CE, 22 juillet 2016, n^o 394922; CE, 15 février 2016, n^o 389140; CE, 12 février 2016, n^o 388134; CE, ord., 27 janvier 2016, n^o 396220; CE, 9 septembre 2015, n^o 393079; CE, 5 juin 2015, n^o 388134.

2. Cons. const., 20 mai 2020, n^o 2020-841 QPC; Cons. const., 3 avril 2020, n^o 2020-834 QPC; Cons. const., 30 mars 2018, n^o 2018-696 QPC; Cons. const., 2 février 2018, n^o 2017-687 QPC; Cons. const., 15 décembre 2017, n^o 2017-692 QPC; Cons. const., 4 août 2017, n^o 2017-648 QPC; Cons. const., 21 juillet 2017, n^o 2017-646/647 QPC; Cons. const., 2 décembre 2016, n^o 2016-600 QPC; Cons. const., 21 octobre 2016, n^o 2016-590 QPC; Cons. const., 24 juillet 2015, n^o 2015-478 QPC.

3. TUE, ord., 14 décembre 2020, aff. T-738/16; CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18.

13. Elle a notamment été recevable à agir dans des recours dirigés contre des décisions locales, notamment de la préfecture de police de Paris consistant à utiliser des drones (*cf.* CE, ord., 18 mai 2020, n^{os} 440442, 440445 ; CE, 22 décembre 2020, n^o 446155, Rec. T. p. 750) ou contre une délibération de la région PACA autorisant l'utilisation de portiques de reconnaissance faciale (*cf.* TA Marseille, 27 février 2020, *La Quadrature du Net et autres*, n^o 1901249).

14. Or, les décisions attaquées dans l'instance n^o 2216570, en ce qu'elles mettent en œuvre de manière obligatoire un traitement de données personnelles, dont des données sensibles, participent à l'accentuation du fichage et de la surveillance de la population. Ces décisions affectent donc directement l'exercice des droits fondamentaux dans l'environnement numérique que l'association exposante entend défendre. En particulier, en imposant le logiciel de surveillance par analyse algorithmique des images et des sons dénommé « TestWe », sans base légale ni proportionnalité, les décisions litigieuses participent directement à une augmentation de la surveillance contre laquelle La Quadrature du Net s'est donnée pour mission de lutter.

15. **Partant**, l'objet statutaire de l'association exposante ainsi que les actions, notamment juridictionnelles, qu'elle a entreprise depuis plusieurs années en ce sens caractérisent manifestement son intérêt à intervenir au soutien du recours enregistré sous le numéro 2216570.

II. Sur la qualification juridique des faits

16. Les décisions attaquées mettent en œuvre un traitement (B) de données personnelles, et notamment de données sensibles et biométriques (A).

A. En ce qui concerne la qualification de données personnelles, et notamment de données sensibles

17. Les données concernées par le dispositif mis en œuvre par les décisions attaquées ont bien la qualité de données personnelles, et plus particulièrement de

données sensibles dont des données biométriques.

18. **En droit**, aux termes du 1) de l'article 4 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 »), une donnée personnelle est définie comme :

« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; »

19. Ainsi, une donnée personnelle doit pouvoir être rattachée à une personne physique identifiée ou identifiable. Le considérant 26 du RGPD précise que *« 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 [...] »*.

20. Le troisième alinéa de l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés ») renvoie directement aux définitions du RGPD.

21. Par ailleurs, l'article 9 du RGPD précise qu'il existe certaines catégories particulières de données personnelles, dites « données sensibles », qui *« révèle[nt] l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale »*, ainsi que celles concernant *« des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle »*. Cette définition est reprise à l'identique par l'article 6 de la loi Informatique et Libertés.

22. Parmi ces données sensibles se trouvent donc les données biométriques. Le 14) de l'article 4 du RGPD définit les données biométriques comme « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ».

23. Concernant l'analyse sonore automatisée, la présidente de la Commission nationale de l'informatique et des libertés (ci-après « la CNIL »), Mme Marie-Laure Denis, a considéré qu'un tel traitement vise des données sensibles lorsqu'elle a analysé un dispositif de captation et d'analyse de sons de l'espace public (cf. pièce n° 3). Ce dispositif permettait de capter de manière indifférenciée « *les sons émis sur la voie publique, y compris des sons de bombes aérosols bris de verre ou de crépitements* » (même pièce).

24. La présidente de la CNIL a également précisé que « *Les voix et conversations des personnes se situant dans la zone couverte sont ainsi susceptibles d'être captées par le dispositif envisagé* ». Elle a ainsi considéré que « *le traitement de captation et d'analyse des sons dont la mise en œuvre est envisagée est susceptible de porter sur des catégories de données personnelles relevant de l'article 9 du RGPD et de l'article 6 de la loi du 6 janvier 1978 modifiée (données dites « sensibles »), telles que les opinions politiques, les convictions religieuses et les données concernant la santé, la vie sexuelle ou l'orientation sexuelle de personnes physiques* » (même pièce).

25. Ces considérations concernant un dispositif de captation et d'analyse des sons dans l'espace public sont, bien entendu, parfaitement applicables au cas d'un dispositif de captation et d'analyse des sons dans l'environnement proche d'un candidat à un examen universitaire.

26. **En l'espèce**, les décisions attaquées mettent en œuvre un dispositif visant à surveiller le passage d'un examen universitaire par un candidat. Pour cela, cette surveillance consiste en l'analyse automatisée et la transmission à un tiers (une personne humaine supervisant la surveillance) des images et des sons.

27. **Premièrement**, le dispositif litigieux vérifie de manière automatisée l'iden-

tité du candidat. Cette vérification se fait sur deux temporalités : *d'une part*, en début d'épreuve par l'obligation de prendre en photo son visage puis sa carte d'identité pour que le dispositif vérifie l'authenticité de la carte d'identité, la concordance entre la photo de la carte d'identité et le visage du candidat, et si l'identité civile du candidat est bien celle attendue (cf. pièce n° 4, pp. 9–10); *d'autre part*, cette vérification automatisée se poursuit tout au long de l'épreuve, par une analyse continue du visage du candidat filmé.

28. Or, il ressort directement de la définition de donnée biométrique du 14) de l'article 4 du RGPD qu'une telle analyse automatisée de l'image à des fins d'authentification constitue un traitement biométrique, et plus particulièrement un traitement de reconnaissance faciale. La CNIL confirme cela en précisant sur son site Internet, dans un article rappelant les dispositions légales applicables aux établissements voulant surveiller les examens universitaires à distance, que « *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.*** »⁴ (cf. pièce n° 5, p. 2).

29. Deuxièmement, le dispositif litigieux analyse de manière continue pendant l'épreuve les images et les sons captés pour détecter des comportements suspects. En cela, il s'agit également d'un traitement biométrique, puisque les images du candidat seront en permanence analysées pour vérifier l'absence de tels comportements suspects.

30. En outre, l'analyse des sons et l'analyse vidéo de l'environnement du candidat, c'est-à-dire tout ce qui l'entoure à l'exclusion de son visage, constitue également un traitement de données sensibles. En effet, la captation de manière indifférenciée et permanente permet par exemple de capter les paroles d'une personne entrant par erreur dans la pièce où le candidat passe une épreuve. De même, l'analyse vidéo de l'environnement pourrait avoir comme conséquence la captation de signes religieux ou révélant l'opinion politique, syndicale ou philosophique du candidat, ou de signes révélant son orientation sexuelle, notamment si le candidat passe l'épreuve à son domicile.

31. Enfin, troisièmement, pour fonctionner, le dispositif litigieux requiert un

4. En gras dans le texte original.

accès administrateur à l'ordinateur du candidat, et la désactivation de l'antivirus (cf. pièce n° 4, p. 4). Or, cet accès administrateur sur l'ordinateur et la désactivation forcée de l'antivirus implique que le dispositif litigieux pourra avoir accès à l'ensemble des données stockées sur cet ordinateur et pourra potentiellement s'exécuter postérieurement à la session de l'examen. En cela, le dispositif litigieux peut donc accéder à des données extrêmement sensibles de l'utilisateur – n'importe quelle information stockée sur l'ordinateur exécutant le logiciel.

32. **Il en résulte que** les décisions attaquées mettent en place un dispositif susceptible de traiter des données personnelles, dont des données sensibles.

B. En ce qui concerne l'existence d'un traitement

33. Le dispositif autorisé par les décisions attaquées consiste bien en un traitement de données personnelles.

34. **En droit**, aux termes du 2) de l'article 3 du RGPD, un traitement est ainsi défini comme :

« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ; »

35. L'article 2 de la loi Informatique et Libertés renvoie explicitement à la définition du RGPD.

36. Il ressort de cette définition que la simple collecte d'une donnée personnelle constitue un traitement. De plus, il ressort de cette définition que l'analyse automatisée d'images est également un traitement.

37. Sur ce dernier point, le Conseil d'État a notamment précisé qu'un dispositif de floutage postérieur à la captation d'images, et ne renvoyant que des images floutées au responsable de traitement, doit s'analyser en un traitement de données personnelles soumis à la loi Informatique et Libertés (cf. CE, 22 décembre 2020, *La Quadrature du Net*, préc., pts. 6 et 7). M. le rapporteur public Laurent Domingo précisait dans cette affaire que « *Peu importe qu'une partie du flux d'informations, à l'une des étapes de la transmission de ce flux, subissent une altération technique. En réalité, en floutant les images captées par le drone lors de leur transmission au centre de commandement, la préfecture de police n'a fait qu'ajouter un traitement aux données captées.* »

38. De manière similaire, en matière de vidéosurveillance, il faut ainsi distinguer l'étape de captation des images – qui consiste en un traitement fondé sur les articles L. 251-1 et suivants du code de la sécurité intérieure – et les éventuelles analyses automatisées de ces mêmes images – qui ne peut avoir comme base légale les dispositions de ce code ne prévoyant que le déploiement de caméras. Dans sa « *Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics* » (cf. pièce n° 6), la CNIL a ainsi explicitement écarté la possibilité pour ces dispositifs d'« *analyse automatisée d'images à partir de caméras vidéo* » de se prévaloir du code de la sécurité intérieure comme base légale, parce que la captation et l'analyse automatisée sont deux traitements distincts qui doivent avoir chacun leur propre base légale.

39. **En l'espèce**, comme présenté ci-avant, le dispositif litigieux consiste en la captation (c'est-à-dire la collecte) de sons et d'images, puis en leur analyse postérieurement à la captation. En cela, il s'agit donc de deux traitements au sens du droit des données personnelles.

40. **Premièrement**, le dispositif litigieux capte et transmet à la personne chargée de surveiller l'examen l'image et le son de l'environnement de chaque candidat. Ce premier traitement est indépendant des analyses automatisées de ces données, la seule captation et transmission de données personnelles consistant en un traitement au sens du RGPD et de la loi Informatique et Libertés.

41. **Deuxièmement**, le dispositif litigieux analyse également des sons et des images pour détecter automatiquement des fraudes potentielles. Le guide utilisateur du dispositif litigieux précise ainsi, de manière explicite, que « *TestWe monitore*

vosre environnement pendant vosre examen, tout comportement suspect sera reporté à vosre administration » (cf. pièce n° 4, p. 14).

42. Il s'en déduit que l'objectif du dispositif litigieux est d'effectuer une analyse automatisée et systématique, à l'aide d'outils informatiques, des sons et images captés afin de détecter des comportements susceptibles de constituer une possible fraude. Le dispositif litigieux détermine si un son ou une image donnés à un instant *t* correspond à l'une des caractéristiques pré-établies par la société qui édite le logiciel « TestWe ». Ainsi, à partir d'un son ou d'une image, le dispositif pourra le classer automatiquement dans une catégorie de fraudes pour renvoyer une alerte à la personne chargée de surveiller les candidats.

43. Cette analyse automatisée, qu'elle soit pendant l'épreuve ou lors de la vérification d'identité au début, constitue donc un deuxième traitement qui, pour reprendre les mots de M. le rapporteur public Laurent Domingo, « [ne] fait qu'ajouter un traitement aux données captées » (cf. CE, 22 décembre 2020, préc.).

44. **En résumé**, le dispositif litigieux consiste donc bien dans un premier temps en la « captation » de données personnelles (les sons et les images), captation qui est faite de manière permanente, puis en leur « organisation » et en leur « structuration » afin de détecter d'éventuelles situations de fraude.

45. **Il en résulte que** le dispositif litigieux consiste bien en un traitement au sens du RGPD et de la loi Informatique et Libertés. En conséquence, le dispositif litigieux est bien un traitement de données personnelles.

III. Sur l'urgence

46. L'urgence, au sens de l'article L. 521-1 du code de justice administrative, est caractérisée.

47. **En droit**, aux termes du 1^{er} alinéa de l'article L. 521-1 du code de justice administrative :

« *Quand une décision administrative, même de rejet, fait l'objet d'une requête en annulation ou en réformation, le juge des référés, saisi d'une demande en ce sens, peut ordonner la suspension de l'exécution de cette décision, ou de certains de ses effets, lorsque l'urgence le justifie et qu'il est fait état d'un moyen propre à créer, en l'état de l'instruction, un doute sérieux quant à la légalité de la décision.* »

48. La condition d'urgence, à laquelle est subordonnée le prononcé d'une mesure de suspension, est regardée comme remplie lorsque la décision administrative contestée préjudicie de manière suffisamment grave et immédiate soit à un intérêt public, soit à la situation du requérant ou aux intérêts qu'il entend défendre (*cf.* not. CE sect. 19 janvier 2001, *Confédération nationale des radios libres*, n° 228815, Rec. p. 29).

49. Il appartient au juge des référés d'apprécier concrètement, compte tenu des justifications fournies par le requérant, si les effets de la décision administrative contestée sont de nature à caractériser une urgence justifiant que, sans attendre le jugement de la requête au fond, l'exécution de la décision soit suspendue (*cf.* not. CE sect. 28 février 2001, *Préfet des Alpes-Maritimes et société Sud-Est Assainissement*, n° 229562, Rec. p. 109).

50. Le juge national a le devoir d'écarter toute disposition nationale contraire au droit de l'Union européenne « *au moment même* » de l'application de celui-ci (*cf.* CJCE, 9 mars 1978, *Simmenthal*, n° C-106/77, pt. 22 : « *serait, dès lors, incompatible avec les exigences inhérentes à la nature même du droit communautaire toute disposition d'un ordre juridique national ou toute pratique, législative, administrative ou judiciaire, qui aurait pour effet de diminuer l'efficacité du droit communautaire par le fait de refuser au juge compétent pour appliquer ce droit, le pouvoir de faire, au moment même de cette application, tout ce qui est nécessaire pour écarter les dispositions législatives nationales formant éventuellement obstacle à la pleine efficacité des normes communautaires* » ; CJCE, 19 juin 1990, *Factortame*, n° C-213/89, pt. 20 ; Cons. const., 12 mai 2010, *Loi relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*, n° 2010-605 DC, pt. 14 ; CE, 14 mai 2010, *Rujovic*, n° 312305, Rec. p. 165 ; CE, ord., 14 février 2013, *Lallier*, n° 365459) et même si l'obstacle en question n'est que « *temporaire* » (*cf.* CJCE, 19 juin 1990, *Factortame*, préc.).

51. En sorte que le doute sérieux sur la compatibilité d'une norme française avec le droit de l'Union européenne caractérise, à lui seul, une situation d'urgence (cf. CE, ord., 14 février 2013, *Lallier*, n° 365459).

52. Le juge des référés du Conseil d'État, dans une ordonnance prise sur le fondement de l'article L. 521-2 du code de justice administrative (CE, ord., 18 mai 2020, *La Quadrature du Net et autre*, n°s 440442, 440445), a jugé qu'eu égard, d'une part, au nombre de personnes susceptibles d'en faire l'objet et, d'autre part, à leurs effets, la fréquence et le caractère répété des mesures de surveillance effectuées par une flotte de drones, ces dernières créent une situation d'urgence au sens de l'article L. 521-2 du code de justice administrative. La condition d'urgence au sens de l'article L. 521-1 du code de justice administrative étant moins exigeante, elle s'en trouve, *a fortiori*, remplie (cf. CE, 22 décembre 2020, *La Quadrature du Net*, préc.).

53. **En l'espèce, premièrement**, l'intérêt public qui commande que soient prises les mesures provisoires nécessaires pour faire cesser immédiatement l'atteinte aux droits conférés par l'ordre juridique de l'Union européenne caractérise l'urgence au sens de l'article L. 521-1 du code de justice administrative (cf. *mutatis mutandis*, CE, ord., 14 février 2013, *Lallier*, n° 365459).

54. **Deuxièmement**, eu égard, d'une part, au nombre de personnes susceptibles d'en faire l'objet – l'intégralité des 4 000 étudiants inscrits à l'IED de l'Université Paris 8 – et, d'autre part, à leurs effets et au caractère continue des mesures de surveillance litigieuses pendant les examens, ces dernières créent une situation d'urgence au sens de l'article L. 521-1 du code de justice administrative.

55. En effet, l'atteinte engendrée par les décisions attaquées, tant aux intérêts que l'exposante entend défendre qu'à l'intérêt public qui s'attache au droit fondamental à la protection des données personnelles et à la préservation de l'ordre juridique de l'Union européenne et qu'aux intérêts de la requérante directement concernée, est à la fois grave, dès lors qu'il s'agit de la méconnaissance tant de droits fondamentaux que du droit de l'Union européenne, et immédiate, dès lors que les décisions litigieuses sont déjà en vigueur et que leurs effets délétères vont se produire dans quelques semaines lors des examens de janvier 2023.

56. Il ne fait donc aucun doute que l'atteinte engendrée par cette décision est donc grave et immédiate.

57. Ainsi, une situation d'urgence, au sens de l'article L. 521-1 du code de justice administrative est constituée.

58. **En outre, il existe plusieurs moyens de nature à faire naître, à tout le moins, un doute sérieux quant à la légalité des décisions attaquées.**

IV. Sur les moyens propres à faire naître un doute sérieux quant à la légalité des décisions attaquées

A. En ce qui concerne le défaut de base légale du traitement litigieux

59. **En premier lieu**, les décisions attaquées sont illégales dès lors qu'elles sont contraires à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après « CESDH »), à la lecture combinée des articles 5, 6 et 9 du RGPD, et à la lecture combinée des articles 4 et 5 la loi Informatique et Libertés, en ce qu'elles prévoient une atteinte au droit à la vie privée qui n'est pas prévue par la loi.

60. **En droit**, aux termes de l'article 8 de la CESDH, intitulé « *Droit au respect de la vie privée et familiale* » :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

61. La Cour européenne des droits de l'homme (ci-après « CEDH ») a ainsi considéré que l'ingérence devait avoir « *une base en droit interne* », être par ailleurs « *suffisamment accessible* », la personne devant « *pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné* » et enfin que ne pouvait être considéré comme une loi au sens de la CESDH « *qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé* » (cf. CEDH, 25 mars 1983, *Silver et autres c. Royaume-Uni*, n° 5947/72, §§ 85–88).

62. De la même façon, il a été jugé que :

« *Les mots “prévue par la loi” veulent d’abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l’accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit [...]. Cette expression implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention* » (cf. CEDH, 12 juin 2014, *Fernandez Martinez c. Espagne*, n° 56030/07, § 117)

63. Il a ainsi suffi à la Cour européenne de constater que la mesure incriminée n'était pas prévue par la loi pour conclure à la violation de l'article 8 de la Convention (cf. CEDH, 8 avril 2003, *M. M. c. Pays-Bas*, n° 39339/98, §. 46 ; voir dans ce sens également : CEDH, *Guide sur l'article 8 de la Convention - Droit au respect de la vie privée et familiale*, § 14).

64. Il en résulte que toute ingérence dans la vie privée des personnes doit être fondée sur un cadre juridique clair et précis, suffisamment accessible, permettant au citoyen de disposer de renseignements suffisants sur les normes juridiques applicables à un cas donné.

65. Cette exigence de la CESDH est reprise en substance par l'article 5 du RGPD et 4 de la loi Informatique et Libertés. Aux termes du 1. de l'article 5 du RGPD, « *les données à caractère personnel doivent être : a) traitées de manière licite, loyale et transparente au regard de la personne concernée; [...]* ». La loi Informatique et Libertés reprend ce critère en exigeant à son article 4 que « *les données à caractère personnel doivent être : 1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée; [...]* ».

66. La définition de la licéité est donnée au 1. de l'article 6 du RGPD :

« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

[...]

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

[...]

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

[...] »

67. L'article 5 de la loi Informatique et Libertés reprend une définition similaire à celle du RGPD.

68. **En l'espèce**, les décisions attaquées mettent en œuvre un traitement de données personnelles sans prévoir de base légale explicite. L'illégalité de ce traitement de données ainsi mis en œuvre par les décisions attaquées est, de cette seule constatation, déjà acquise.

69. Au surplus, aucune des bases légales – et, en particulier, ni le consentement (1), ni le respect d'une obligation légale ou l'exécution d'une mission de service public (2) – prévues par le droit ne peut venir fonder le traitement litigieux.

1. S'agissant du consentement

70. **En droit**, le 11) de l'article 4 du RGPD définit ainsi le consentement :

« consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ; »

71. Il y a donc quatre conditions cumulatives au consentement : il doit être libre, spécifique, éclairé et univoque. L'article 7 du RGPD précise ces critères :

« 1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.

3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère

personnel qui n'est pas nécessaire à l'exécution dudit contrat.

72. La CNIL précise également l'interprétation de ces conditions sur son site Internet (cf. pièce n° 7). Concernant le caractère libre, elle rappelle que « *refuser de consentir à un traitement qui n'est pas nécessaire à l'exécution du contrat ne doit pas avoir de conséquence sur son exécution ou sur la prestation du service.* » Concernant le caractère spécifique, elle rappelle que « *un consentement doit correspondre à un seul traitement, pour une finalité déterminée.* » Enfin, concernant le caractère univoque du consentement, elle rejette la possibilité pour un responsable de traitement de déduire le consentement du silence gardé par la personne concernée : « *le consentement doit être donné par une déclaration ou tout autre acte positif clairs. Aucune ambiguïté quant à l'expression du consentement ne peut demeurer.* »

73. Concernant le cas particulier d'examens à distance, la CNIL rappelle que, pour que le traitement de données permettant la tenue dudit examen puisse se fonder sur le consentement, celui-ci ne doit être « *ni contraint ni influencé (par exemple par la position d'autorité du responsable de traitement). L'étudiant doit notamment se voir offrir un choix réel, sans avoir à subir de conséquences négatives en cas de refus.* » (cf. pièce n° 5, p. 1).

74. Elle conclut sans ambiguïté : « *Dans ces conditions, le consentement comme base légale peut difficilement être retenu pour les traitements de surveillance des examens organisés et surveillés en ligne* » (même pièce).

75. **En l'espèce**, l'Université tente – vainement – d'affirmer que le traitement litigieux reposerait sur la base légale du consentement. Le mémoire en défense précise ainsi que « *l'IED [...] a proposé, sur la base du volontariat, aux étudiants qui le souhaitent de passer les examens en présentiel* » (cf. mémoire en défense du 25 novembre 2022, p. 7)⁵.

76. Or, **premièrement**, un tel consentement n'est pas libre : les enseignements à distance s'adressent essentiellement à des étudiants ayant des contraintes spécifiques (domicile à l'étranger, contraintes professionnelles ou personnelles em-

5. On ne pourra que s'étonner de cette formulation de « *volontariat* » qui ne correspond à aucune base légale du RGPD ou de la loi Informatique et Libertés. Pour les besoins de la discussion, on considérera que l'Université entend ici faire référence au consentement.

pêchant la venue dans les locaux de l'université, etc.) et l'alternative consistant à passer les examens dans une salle de l'université est souvent incompatible ou très difficile pour les étudiants de l'institut d'études à distance.

77. Aujourd'hui encore, le site Internet de l'IED précise que « *Pour l'année 2021-2022, les examens se dérouleront en ligne* » (cf. pièce n° 8). Si cette seule phrase ne constitue bien évidemment pas un engagement de la part de l'IED, l'Université sait néanmoins qu'en précisant cette modalité d'examen en ligne et en laissant l'information sur son site, elle attirera des étudiants ne pouvant se déplacer dans les locaux de l'Université pour passer leurs examens.

78. **Deuxièmement**, un tel consentement n'est pas univoque : l'université déduit le consentement de l'absence de demande d'aménagement des épreuves. Un tel silence gardé par les étudiants n'est pas un « *acte positif clair* ».

79. **Troisièmement**, un tel consentement n'est pas spécifique : le traitement imposé ne consiste pas en la seule transmission des images et sons du candidat à une personne humaine qui serait chargée de surveiller l'épreuve, mais bien, en sus, de l'analyse automatisée de ces images et sons. L'université aurait donc dû demander un consentement spécifique pour, d'une part, le traitement consistant à capter et transmettre à un surveillance les images et sons et pour, d'autre part, le traitement consistant en l'analyse automatisée de ces images et sons, y compris pour la vérification d'identité. Pourtant, les étudiants ne pouvaient pas s'opposer à la seule analyse automatisée des images.

80. **Il en résulte que** le consentement ne peut fonder le traitement litigieux.

2. S'agissant du respect d'une obligation légale ou de la poursuite d'une mission de service public

81. **En droit**, les 2. et 3. de l'article 6 du RGPD précisent ce qu'il faut entendre par le respect d'une obligation légale ou la poursuite d'une mission de service public :

2. Les États membres peuvent maintenir ou introduire des dispositions

plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX.

3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :

- a) le droit de l'Union ; ou*
- b) le droit de l'État membre auquel le responsable du traitement est soumis.*

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. »

82. Autrement dit, le droit de l'UE ou le droit interne doivent suffisamment encadrer les traitements dont la base légale serait le respect d'une obligation légale ou la poursuite d'une mission de service public, notamment en prévoyant des finalités particulières pour cette base juridique ou en précisant les données ainsi traitées.

83. L'article D. 611-12 du code de l'éducation encadre ainsi de manière très

limitée le recours à un traitement de données personnelles pour les examens à distance :

« Les conditions de la validation des enseignements, dispensés en présence des usagers ou à distance, le cas échéant sous forme numérique, sont arrêtées dans chaque établissement d'enseignement supérieur au plus tard à la fin du premier mois de l'année d'enseignement et elles ne peuvent être modifiées en cours d'année.

La validation des enseignements contrôlée par des épreuves organisées à distance sous forme numérique, doit être garantie par :

- 1° La vérification que le candidat dispose des moyens techniques lui permettant le passage effectif des épreuves ;*
- 2° La vérification de l'identité du candidat ;*
- 3° La surveillance de l'épreuve et le respect des règles applicables aux examens. »*

84. Ainsi, l'article D. 611-12 du code de l'éducation, en ne prévoyant explicitement pas la possibilité de recourir à une analyse automatisée des images et sons, ne peut servir de base légale que pour un traitement limité à la transmission des images et sons à un surveillant, sans aucune analyse automatisée de ces données. La CNIL précise ainsi que, dans le cadre d'une surveillance à distance d'examens, *« le traitement des données biométriques étant par principe interdit par le RGPD, de tels dispositifs nécessiteraient une disposition légale particulière »*, disposition aujourd'hui inexistante.

85. Or, **en l'espèce**, le traitement litigieux ne peut être fondé sur le respect d'une obligation légale ou la poursuite d'une mission de service public.

86. S'agissant du respect d'une obligation légale, aucune disposition de niveau législatif ou réglementaire n'impose la réalisation d'un examen à distance par l'utilisation d'un traitement d'analyse automatisée des images et sons. Si l'article D. 611-12 du code de l'éducation encadre – de manière très limitée – le recours à un traitement de données, il n'en impose pas l'usage ni, *a fortiori*, l'usage d'un traitement d'analyse automatisée des images et sons comme en l'espèce.

87. S'agissant de la poursuite d'une mission de service public, seule la transmission des images et sons à un surveillant, sans analyse automatisée de ces données, pourrait se fonder sur la poursuite d'une mission de service public et l'article D. 611-12 du code de l'éducation. Or, force est de constater que le dispositif litigieux ne consiste pas qu'en la seule transmission de ces images et sons à un surveillant pour analyse humaine : il s'agit surtout de surveiller (donc de traiter ces données) de manière automatisée et de ne transmettre à une personne humaine que le résultat d'éventuelles alertes.

88. **Il en résulte que** le dispositif litigieux ne peut avoir comme base légale ni le respect d'une obligation légale, ni la poursuite d'une mission de service public.

* *

89. **En conclusion**, aucune base légale ne permettant de fonder le dispositif litigieux, les décisions attaquées sont illégales.

B. En ce qui concerne la disproportion du traitement litigieux

90. **En deuxième lieu**, les décisions attaquées sont illégales en ce qu'elles autorisent la mise en œuvre d'un traitement méconnaissant l'article 8 de la CESDH, l'article 5 du RGPD et l'article 4 de la loi Informatique et Libertés, dès lors que les données traitées ne sont ni adéquates, ni pertinentes et, en tout état de cause, ne sont manifestement pas limitées à ce qui est nécessaire.

91. **En droit**, le 2. de l'article 8 de la CESDH prévoit qu'« *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.* »

92. De même, le c) du 1. de l'article 5 du RGPD dispose que « *Les données à*

caractère personnel doivent être : [...] c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données); ».

93. À ce titre, le considérant 39 du RGPD énonce que « *Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens.* ».

94. L'article 4 de la loi Informatique et Libertés reprend ces dispositions en exigeant que « *les données à caractère personnel doivent être : [...] 3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives; [...] ».*

95. Il en résulte que pour déterminer le caractère adéquat, pertinent et limité d'un traitement de données, il convient notamment de vérifier si la finalité poursuivie pouvait être atteinte par d'autres moyens moins intrusifs et de prendre en compte le contexte de sa mise en œuvre, les risques qu'il représente pour les droits et libertés des personnes concernées, la possibilité de détournement ou de mauvais usage du dispositif, ou, enfin, la nature des données traitées.

96. Par ailleurs, il incombe au responsable du traitement de démontrer, par exemple dans le cadre d'une analyse d'impact sur la protection des données (AIPD), en quoi le traitement est proportionné et que la finalité poursuivie ne peut pas être atteinte autrement.

97. C'est notamment en application de ce principe que le Conseil d'État a pu reprocher au ministre de l'intérieur de ne pas avoir démontré la nécessité du recours à des drones aux fins de garantie de la sécurité publique : « *le ministre n'apporte pas d'élément de nature à établir que l'objectif de garantie de la sécurité publique lors de rassemblements de personnes sur la voie publique ne pourrait être atteint pleinement, dans les circonstances actuelles, en l'absence de recours à des drones* » (cf. CE, 22 décembre 2020, *La Quadrature du Net*, préc., pt. 11).

98. Enfin, la grande chambre de Cour de Justice de l'Union européenne (CJUE) a récemment précisé que :

« Il convient cependant de souligner que le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte. » (cf. CJUE, gr. ch., 1^{er} août 2022, *Vyriausioji tarnybinės etikos komisija*, aff. C-184/20, pt. 89)

99. Autrement dit, les moyens insuffisants alloués à un responsable de traitement ne peuvent être pris en compte pour la détermination de la proportionnalité du traitement. Cette proportionnalité doit être déterminée de manière objective, par la seule prise en compte de la finalité et des données traitées.

100. **En l'espèce**, le dispositif litigieux mis en œuvre par les décisions attaquées permet, à des fins de surveillance des examens, le traitement de données personnelles, dont des données sensibles.

101. Même si cette base légale n'est en l'espèce pas mobilisable en raison de la nature des données traitées, le dispositif litigieux poursuit la finalité de l'article D. 611-12 du code de l'éducation, à savoir la « *validation des enseignements contrôlée par des épreuves organisées à distance sous forme numérique* ». La finalité est donc de faire se dérouler à distance les examens universitaires, de s'assurer de l'identité des candidats et de surveiller les examens.

102. Or, cette finalité n'implique aucunement de surveiller les épreuves de manière automatisée ni de faire vérifier par un algorithme l'identité civile de chaque candidat.

103. L'Université échoue manifestement à apporter le moindre élément concernant la nécessité à analyser automatiquement les images et les sons des candidats. Il n'est à aucun moment défini dans les décisions attaquées en quoi ce traitement serait nécessaire aux fins de faire passer un examen à distance. Le mémoire en défense n'apporte pas le moindre commencement de preuve de la nécessité de recourir au dispositif litigieux pour les finalités exposées dans l'article D. 611-12 du code de l'éducation.

104. En particulier, le mémoire en défense se borne à invoquer « *des dysfonctionnements majeurs lors du déroulement des examens de l'année universitaire 2021-2022 sur la plateforme Moodle* » (cf. mémoire en défense du 25 novembre 2022, p. 6) et produit un rapport – au demeurant ni daté ni signé – pour étayer cette affirmation (cf. pièce adverse n° 2). Or, force est de constater que les dysfonctionnements invoqués sont exclusivement dus au manques de moyens alloués à l'infrastructure par l'Université, celle-ci ayant visiblement sous-dimensionnée sa précédente plateforme d'examens à distance et n'ayant pas réalisé les tests de montée en charge adéquats.

105. Le rapport produit en défense précise ainsi que « *Le diagnostic établi en coopération active entre la DSI et Idianet indiquait un goulot d'étranglement au niveau du CAS [le service d'authentification centralisée] de l'université* » et que « *les tests de charge sur le CAS n'avaient pas été réalisés par le responsable du pôle IPN, contrairement à ce qui lui avait été demandé* » (même pièce, p. 1). Ce rapport précise d'ailleurs que ces problèmes de sous-dimensionnement de l'infrastructure sont exceptionnels : « *L'IED organise des examens à distance via la plateforme Moodle IED depuis 2018, sans incident technique majeur, à l'exception d'une journée lors de la seconde session 2021 où l'annuaire LDAP avait été modifié sans que nous en ayons été informés par la DSI* » (même pièce, p. 2).

106. Autrement dit, en augmentant la taille de son infrastructure informatique et en modifiant ses procédures internes pour s'assurer du bon déroulement de tous les tests usuels, l'Université aurait pu poursuivre les mêmes finalités sans devoir recourir au dispositif litigieux.

107. **Il en résulte que** le dispositif n'est pas nécessaire aux finalités envisagées.

C. En ce qui concerne le traitement de données sensibles

108. **En troisième lieu**, les décisions attaquées sont illégales, en ce qu'elles autorisent la mise en œuvre d'un traitement de données contraire à l'article 8 de la CESDH, à l'article 9 du RGPD et à l'article 6 de la loi Informatique et Libertés, dès lors qu'elles entraînent notamment le traitement de données sensibles sans respecter les conditions de légalité d'un tel traitement.

109. **En droit**, comme rappelé ci-avant, l'article 8 de la CESDH proclame le droit à la vie privée.

110. De même, l'article 9 du RGPD relatif aux traitements de données dites « sensibles », pose le principe de leur interdiction. Selon ce même article, un tel traitement ne peut être licite que par exception :

« 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques [...];

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;

[...]

g) «le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;

[...] »

111. Concernant le cas particulier d'un dispositif de surveillance des examens à distance, la CNIL a énuméré une liste de traitements qui « *n'apparaissent à priori pas proportionnés au regard de la finalité poursuivie* ». Elle cite notamment « *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)* » et « *les dispositifs de surveillance reposant sur des traitements biométriques (exemple : reconnaissance faciale via une webcam)* » (cf. pièce n° 5, p. 2).

112. **En l'espèce**, comme rappelé *supra* (cf. § 26), le dispositif litigieux permet d'identifier de manière unique le candidat. Cette identification unique se fait une première fois lors de la vérification de la carte d'identité et du visage du candidat, puis tout au long de l'épreuve par l'analyse des images de la caméra du candidat.

113. Le dispositif litigieux s'exécutant avec les droits administrateurs et imposant que l'antivirus soit désactivé (cf. § 31), il a potentiellement accès à tous les documents stockés sur l'ordinateur du candidat. Il peut ainsi avoir accès à des données personnelles révélant des opinions politiques, syndicales, religieuses, philosophiques, ou l'orientation sexuelle du candidat. Pourtant, rien ne justifie un accès total à l'ordinateur.

114. Dès lors, si le dispositif litigieux consiste en un traitement de données sensibles, dont des données biométriques, il n'est pourtant justifié par aucune des exceptions du 2. de l'article 9 du RGPD.

115. En particulier, il est insusceptible de légalement se fonder sur le consentement des candidats (cf. 1), constatation qui s'applique *a fortiori*, pour un traitement de données biométriques, et ne peut davantage être regardé comme poursuivant un motif d'intérêt public important.

116. Sur ce dernier point de l'intérêt public important, une telle notion doit être définie par le droit. Or, ni l'article D. 611-12 du code de l'éducation, ni aucune disposition réglementaire ou législative ne vient préciser en quoi il y aurait un intérêt public important à traiter des données sensibles, y compris par de la reconnaissance

faciale, pour surveiller les examens. De plus, un tel intérêt public important nécessite également que la condition de nécessité soit remplie, qui implique donc que la même finalité puisse être remplie par une mesure moins attentatoire aux droits et libertés. Comme développé ci-avant (*cf.* 103), tel n'est pas le cas en l'espèce et l'absence de nécessité du dispositif est alors d'autant plus criante s'agissant de données sensibles.

117. **Il en résulte que** les décisions attaquées mettent en œuvre un traitement de données sensibles ne correspondant à aucune des exceptions autorisant de tels traitements.

* *

118. À tous égards, la suspension des décisions attaquées s'impose.

PAR CES MOTIFS, l'association La Quadrature du Net, exposante, conclut qu'il plaise au juge des référés du tribunal administratif de Montreuil de :

ADMETTRE l'intervention de La Quadrature du Net dans la présente instance ;

FAIRE DROIT à la requête de [REDACTED] et, **EN CONSÉQUENCE**, notamment de :

SUSPENDRE les décisions du 25 octobre 2022 et 9 et 14 novembre 2022, jusqu'à ce qu'il soit statué au fond sur la requête en annulation présentée à l'encontre de ces décisions ;

ENJOINDRE à l'autorité administrative d'organiser les examens de licence 2022/2023 au sein de l'IED, seulement à distance avec la plateforme Moodle dans l'attente du jugement au fond.

Fait à Paris, le 2 décembre 2022

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

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.