Délibération n° 2023-058 du 8 juin 2023 portant adoption d'une recommandation relative aux modalités de mise en œuvre des dispositifs de télésurveillance pour les examens en ligne

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I-2°-b ;

Vu le Code de l'éducation, notamment son article D. 611-12 ;

Après avoir entendu le rapport Mme Sylvie Robert, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement

Formule les observations suivantes :

1. La Commission nationale de l'informatique et des libertés a constaté, notamment depuis la crise sanitaire liée au COVID-19, l'augmentation du recours au passage d'examens à distance sous forme numérique dans les établissements d'enseignement supérieur publics et privés. Cette modalité d'examen s'accompagne du souhait par les établissements de recourir à des outils de télésurveillance afin d'organiser la validation des enseignements à distance, telle qu'autorisée et encadrée depuis 2017.
2. En effet, l'article D. 611-12 du code de l'éducation prévoit que les modalités d'examen (en présence ou à distance, sous forme numérique ou non) doivent être arrêtées dans chaque établissement d'enseignement supérieur au plus tard à la fin du premier mois de l'année d'enseignement et ne peuvent être modifiées en cours d'année. Ce même article prévoit que l'organisation d'examens 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* ».
3. Les établissements ayant recours à des outils de télésurveillance, par nature intrusifs, la CNIL rappelle les obligations qui découlent du RGPD et incite au respect de bonnes pratiques.

4. En préambule, la Commission remarque que la validation des enseignements à distance peut, dans une certaine mesure, porter atteinte au principe d'égalité des chances entre les candidats en introduisant des biais socio-économiques dans les conditions de leur évaluation. En effet, un système d'enseignement et d'évaluation à distance entraîne la disparition du nivellement des conditions matérielles assuré par la nécessité d'être présent physiquement dans les lieux de l'épreuve. Cela peut avoir pour conséquence de pénaliser les candidats résidant en zone blanche, ou ne

disposant pas d'une pièce au calme, d'un bureau, d'un ordinateur suffisamment performant, etc. Dès lors, de manière générale, et quel que soit le dispositif utilisé, la télésurveillance devrait être exempte de tout biais discriminatoire quant à l'origine des étudiants concernés. Il convient en particulier de prendre en compte la situation des personnes handicapées (par exemple avec un logiciel d'agrandissement et de lecture d'écran).

5. Par ailleurs, la mise en œuvre d'une télésurveillance qui se voudrait aussi performante que la surveillance habituellement réalisée dans les locaux d'examen impliquerait le recours à des moyens informatiques particulièrement intrusifs. Il faut souligner que l'organisation d'une épreuve à distance conduit généralement l'établissement à surveiller un terminal informatique privé, à l'intérieur d'un local privé. Par ailleurs, cette télésurveillance est nécessairement imparfaite, ne serait-ce que parce que le dispositif ne peut pas surveiller l'intégralité du local où se trouve le candidat (notamment les toilettes).
6. À l'inverse, l'organisation d'examens à distance peut avoir des conséquences bénéfiques, par exemple sur la diversité géographique et sociale des candidats. Il arrive en effet que des candidats renoncent à participer à des épreuves du fait de l'éloignement géographique du centre d'examen. L'organisation d'examen à distance peut favoriser l'accès à la formation continue et à la formation professionnelle. De même, l'organisation d'épreuves à distance peut permettre à un candidat d'obtenir certaines qualifications alors qu'il poursuit ses études ou effectue un stage dans une autre ville ou à l'étranger. Elle peut également faciliter le passage d'un examen pour un candidat en situation de handicap. Ainsi, l'organisation d'épreuves à distance peut s'avérer pertinente dans certains cas spécifiques, ou dans certains contextes particuliers (crise sanitaire notamment).
7. À ce titre, la Commission rappelle qu'il existe des modalités d'examen compatibles avec une validation à distance et permettant d'attester des compétences d'un étudiant sans recourir à de la télésurveillance (mémoire de fin d'études, soutenance de projet, etc.) ou permettant de limiter le caractère intrusif du dispositif employé (examen oral, examen à livre ouvert, passage de l'examen dans des locaux dédiés, *etc.*). Ces modalités devraient être privilégiées lorsque cela est possible.
8. Face à l'absence d'encadrement spécifique des dispositifs de télésurveillance utilisés dans le cadre du passage d'examens ou de concours à distance, qui relève en partie de l'autonomie des établissements d'enseignement, et dans l'objectif de garantir la conformité de ces dispositifs au règlement général sur la protection des données (RGPD) et à la loi « Informatique et Libertés », de maintenir la confiance entre les étudiants et les établissements d'enseignement supérieur et de favoriser les bonnes pratiques en matière d'inclusion numérique et de traitement de données à caractère personnel, la Commission émet les recommandations suivantes.

Recommande :

Article 1er
Principes généraux sur le recours à la télésurveillance d'examen

9. La présente recommandation concerne la mise en œuvre de dispositifs de télésurveillance pour les examens en ligne pour tout type d'examen ou certification, organisée par un établissement public ou un organisme privé.

10. Un établissement ou un organisme décidant de recourir à une solution de télésurveillance est responsable du traitement qui sera mis en œuvre. Il lui incombe de se montrer vigilant en utilisant des solutions éprouvées et réputées sûres, et en testant en amont des épreuves les dispositifs envisagés pour la télésurveillance dans les différents cas pouvant se présenter (faible bande passante entre le candidat et le serveur, perte temporaire de connexion à Internet du candidat, compatibilité avec les terminaux et systèmes d'exploitation utilisés par les candidats, *etc.*).

11. De plus, le recours à des outils de télésurveillance doit respecter les principes du RGPD et de la loi « Informatique et Libertés », quelles que soient les technologies utilisées. À cet égard, l'établissement doit se rapprocher de son délégué à la protection des données afin de s'assurer de la conformité du dispositif de télésurveillance à la règlementation relative à la protection des données à caractère personnel.

12. Les principes suivants devront notamment être pris en compte :
    - **l'obligation d'information** ;
    - le **respect des droits des personnes concernées**, en particulier le droit d'accès ;
    - la **limitation des traitements de données à caractère personnel à des fins précises et déterminées** ;
    - le **principe de minimisation des données** traitées ;
    - le **principe de sécurité et de confidentialité des données** ;
    - le **principe de proportionnalité et de pertinence** ;
    - la **limitation de la durée de conservation des données** ;
    - la **limitation des transferts de données en dehors du territoire de l'Union européenne** selon les conditions définies par le RGPD.

13. Concernant le devoir d'information, bien que l'article D. 611-12 du code de l'éducation dispose que les modalités d'examen doivent être arrêtées dans chaque établissement d'enseignement supérieur au plus tard à la fin du premier mois de l'année d'enseignement, la Commission encourage vivement les établissements à communiquer les modalités d'examen envisagées ainsi que les dispositifs susceptibles d'être employés pour la télésurveillance suffisamment à l'avance pour permettre aux étudiants de faire leur choix de formation en toute connaissance de cause.

14. Au surplus, au regard des difficultés que peut présenter le passage d'examens à distance (risque de dysfonctionnement du matériel, étudiant ne disposant pas du matériel nécessaire ou d'une connexion adaptée, modalités d'examen non compatibles avec un handicap de l'étudiant, étudiant ne disposant pas d'un environnement adapté au passage de l'examen, etc.), les établissements devraient informer leurs étudiants aussi tôt que possible et de façon précise sur les modalités organisationnelles et techniques de passage des examens. Ils devraient envisager des mesures permettant de pallier ces difficultés (prêt de matériel adapté par exemple) et prévoir aussi souvent que possible une possibilité de passage de l'examen en présentiel, étant précisé que l'organisation de deux modalités distinctes pour passer l'examen devra respecter l'égalité de traitement entre les candidats.

15. Il convient pour le responsable de traitement, avec l'appui du délégué à la protection des données, le cas échéant, de procéder à une analyse et à une réflexion préalables à toute décision d'organiser un examen à distance impliquant une télésurveillance, en tenant compte des risques réels de fraude et des conséquences de celle-ci, afin d'éviter de recourir à des outils excessivement intrusifs au regard de l'enjeu et des risques.

16. En tout état de cause, et comme rappelé ci-avant, l'accès de l'étudiant à ses données collectées dans le cadre de la télésurveillance doit toujours être garanti.

17. Par ailleurs, les responsables de traitement, ainsi que leurs éventuels sous-traitants, ne devraient pas utiliser les données pour une finalité autre que celle pour laquelle elles ont été collectées initialement.

18. Le recours à l'évaluation à distance nécessitant la mise en œuvre d'une télésurveillance ne doit pas constituer une alternative de confort destinée uniquement à rendre moins contraignante ou moins coûteuse pour l'établissement l'organisation de la validation des compétences des candidats. Le déroulement des épreuves dans un local soumis à une surveillance humaine demeure souvent la façon la plus appropriée de garantir l'absence de fraude lors d'un examen.

19. Lorsqu'il est pertinent, le passage de certaines épreuves à distance devrait être une faculté offerte aux étudiants et non une obligation. Ainsi, lorsqu'un établissement décide de recourir au passage d'un examen à distance avec télésurveillance, la Commission recommande qu'une alternative en présentiel soit systématiquement proposée aux candidats. L'organisation de deux modalités de passage de l'examen doit se faire en respectant l'égalité de traitement entre les candidats.

20. L'absence d'alternative en présentiel devrait être réservée à des cas spécifiques. Cela peut notamment être admis pendant une crise sanitaire. Par ailleurs, il existe des établissements ayant fait du distanciel l'essence même de leur organisation, qu'il s'agisse de l'enseignement des matières ou du passage d'examen. Dès lors, une même appréciation ne saurait s'appliquer uniformément à toutes les formations, et celles dont l'organisation est fondée exclusivement sur l'offre de cours et l'organisation d'examens à distance devraient pouvoir maintenir ce modèle de fonctionnement. Les modalités d'examen, et notamment de télésurveillance, devraient alors être connues des étudiants au moment de leur inscription à la formation. L'information sur les modalités d'examen pourra notamment être faite au moment où l'étudiant se renseigne sur la formation.

21. Enfin, la Commission estime que le recours à des outils de surveillance d'examens à distance n'a pas vocation à être plus efficace qu'une surveillance d'examens en présentiel, ni même à garantir un niveau de surveillance équivalent.

Article 2
Sur la base légale

22. Les bases légales appropriées permettant de fonder les traitements de données impliqués dans la télésurveillance d'examens à distance doivent être déterminées dans les conditions prévues à l'article 6 du RGPD.

23. Les établissements d'enseignement supérieur qui poursuivent une mission d'intérêt public, peuvent se fonder sur l'exécution d'une mission d'intérêt public au sens du e) du 1. d l'article 6 du RGPD.

24. Par ailleurs, en cas d'absence de dispositions légales permettant de recourir au e) du 1. de l'article 6 du RGPD, les établissements ont la possibilité de fonder les traitements de télésurveillance d'examen sur le contrat, au sens du b) du 1. de l'article 6 du RGPD, à condition que les modalités d'examen soient fixées dans celui-ci, et donc connues de l'étudiant avant son inscription.

25. Les autres bases légales apparaissent moins appropriées pour l'organisation d'examen. Le consentement nécessite qu'une alternative en présentiel soit proposée au candidat, sans conséquence négative pour lui s'il la choisit. En outre, le consentement doit pouvoir être retiré, ce qui implique que le candidat puisse modifier son choix. De même, l'intérêt légitime implique la possibilité de s'opposer au traitement, ce qui apparaît difficile à gérer dans le cadre de l'organisation d'un examen.

Article 3
Sur l'application de l'article 82 de la loi « Informatique et Libertés »

26. L'article 82 de la loi « Informatique et Libertés » impose, pour les opérations de lecture/écriture sur l'équipement terminal de l'utilisateur d'un service via un réseau de télécommunications ouvert au public, de recueillir le consentement de l'utilisateur, sauf « *si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :*
    - *soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;*
    - *soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* ».

27. Comme énoncé dans la FAQ « Cookies et autres traceurs », les dispositifs mis en œuvre sur des réseaux inaccessibles au public, comme des intranets ou des extranets reposant sur un réseau privé virtuel (VPN), ne sont a priori pas soumis à cet article.

28. Les responsables de traitement devront analyser si les solutions techniques envisagées pour l'organisation d'examens à distance relèvent de cet article.

29. En l'espèce, le recueil d'un consentement au sens du RGPD au début de l'examen semble difficilement compatible avec le passage de l'examen, qui ne peut se tenir sans surveillance. Dans le cas où l'article 82 est applicable, le candidat doit être informé de ce que la connexion à la plateforme d'examen en ligne peut nécessiter certaines formes de télésurveillance, conformément à l'article D. 611-12 du code de l'éducation. Les modalités de télésurveillance utilisées et la nature des données collectées devraient être rappelées avant la connexion à la plateforme.

30. Dans ces conditions, il pourra être considéré que les opérations de lecture et d'écriture dans le terminal du candidat qui demande à accéder au service de

communication en ligne permettant de passer l'épreuve à distance, sont strictement nécessaires à sa fourniture.

Article 4
Sur la proportionnalité des technologies utilisées pour prévenir les fraudes à l'examen

Observations générales applicables à tous les dispositifs

31. Les établissements d'enseignement supérieur doivent procéder à une analyse préalable de la proportionnalité des dispositifs envisagés, en associant si possible les responsables pédagogiques, les représentants des étudiants et, le cas échéant, le délégué à la protection des données. Cette analyse devrait tenir compte notamment compte de la nature, de la durée, et de l'importance des examens concernés. Un test des dispositifs envisagés devrait être effectué en amont de l'examen sur un panel représentatif du matériel utilisé par les candidats aux épreuves.

32. Au regard du caractère intrusif des dispositifs de télésurveillance, le responsable du traitement devra réaliser, conjointement avec son délégué à la protection des données, et avant la mise en œuvre du traitement, une analyse d'impact relative à la protection des données (AIPD), à moins que le dispositif utilisé n'engendre pas de risques élevés pour les droits et libertés des étudiants.

Sur l'analyse de la proportionnalité des dispositifs de télésurveillance

33. L'analyse de l'efficacité et de la proportionnalité d'un dispositif de télésurveillance d'examen doit se faire globalement et non mesure par mesure. À cet égard, un dispositif ne permettant pas de prévenir efficacement la fraude apparait par nature disproportionné. En outre, si un juste équilibre ne peut être trouvé entre efficacité de la télésurveillance et intrusivité du dispositif employé, il faudrait envisager d'organiser l'épreuve en présentiel ou de privilégier une autre forme d'examen. À cet égard, il faut souligner que le choix du type d'épreuve (composition ou QPC, questions identiques pour tous les candidats ou non, temps accordé pour répondre à chaque question, etc.) constitue l'un des éléments à mobiliser pour éviter les fraudes.

34. Par ailleurs, en vertu du principe de proportionnalité, le choix des outils de télésurveillance doit s'apprécier au regard du contexte et de l'enjeu de l'épreuve. À titre d'exemple, une surveillance renforcée parait appropriée pour le passage d'un concours d'entrée dans une école. En revanche, un examen présentant un enjeu faible, dans le processus de validation de la formation d'un étudiant, tel qu'un examen blanc, devrait être effectué sans télésurveillance.

35. Au regard de ce qui précède, les modalités suivantes semblent proportionnées pour des examens nécessitant une télésurveillance renforcée :
    - la télésurveillance vidéo et audio du candidat en temps réel pendant la durée de l'examen par les personnes chargées de la télésurveillance, sans conservation des données, sauf en cas de suspicion de fraude ;
    - la télésurveillance de l'activité du candidat en temps réel via un partage d'écran, sans conservation des données, sauf en cas de suspicion de fraude;

- le contrôle de l'activité du candidat via une plateforme en ligne permettant de détecter voire de bloquer l'accès à d'autres onglets ;
- la vérification ponctuelle en début d'épreuve de l'environnement de l'étudiant via sa caméra par une personne chargée de la télésurveillance sans conservation de données, sauf en cas de suspicion de fraude ;

Sur les dispositifs de télésurveillance procédant à des analyses automatiques

36. Certains dispositifs de télésurveillance proposent d'avoir recours à l'analyse automatique, soit de l'environnement du candidat (détection d'un niveau sonore anormal, de la présence d'une tierce personne dans la pièce, etc.), soit de son comportement (fréquence de frappe, direction du regard, émotions, etc.).

37. Ces dispositifs présentent un caractère particulièrement intrusif. Par ailleurs, il est ressorti des travaux menés par la CNIL et de la consultation qu'elle a effectuée que ceux de ces dispositifs qui cherchent à repérer des comportements du candidat s'apparentant à de la fraude présentent un risque élevé de faux positifs. Cela peut nuire au bon déroulement de l'examen et parfois troubler les étudiants, qui risquent de se focaliser sur l'adoption d'un comportement « normal » face à l'outil de télésurveillance plutôt que de se concentrer sur l'examen. Par conséquent, eu égard au principe de nécessité et de proportionnalité, la CNIL recommande de ne pas recourir à des dispositifs de télésurveillance procédant à des analyses automatiques du comportement des candidats.

38. En revanche, les dispositifs repérant certains événements dans l'environnement du candidat (comme l'entrée d'une tierce personne dans la pièce où il passe l'examen) apparaissent plus fiables et moins intrusifs. Au cas par cas, lorsque le nombre de candidats est important, il peut être envisagé de recourir à des dispositifs d'analyse automatique de l'environnement du candidat, à condition que ce dispositif soit suffisamment fiable. Ces dispositifs ne doivent jamais conduire à une décision automatique ayant un effet immédiat pour le candidat : leur seul rôle est d'attirer l'attention d'un surveillant sur une situation potentiellement anormale ; conformément à l'article 22 du RGPD, il est nécessaire qu'une vérification humaine ait lieu systématiquement avant toute décision ou modification des conditions d'examen du candidat afin de confirmer la suspicion de fraude.

39. Un établissement souhaitant recourir à ces dispositifs devrait réaliser des tests préalables afin d'en vérifier la fiabilité et documenter la nécessité de ce dispositif pour l'examen concerné.

40. Ainsi, à titre d'exemple, un examen ne devrait pas être interrompu, pour un candidat, en raison de la seule détection automatique d'un niveau sonore anormal. En revanche, il peut être proportionné d'alerter un surveillant qu'un niveau sonore anormal a été mesuré et de lui proposer de réécouter cet événement, notamment lorsque le nombre d'étudiants à surveiller en même temps est important.

Sur les dispositifs de télésurveillance procédant à une collecte incidente de données

41. Certains dispositifs présentent un risque de collecte incidente de données à caractère personnel concernant les candidats, leurs proches ou leur environnement. Les établissements doivent informer les étudiants sur ces risques et sur les moyens d'éviter une telle collecte, en leur conseillant notamment de s'isoler, dans la mesure du possible, dans une pièce calme et neutre, de façon à ne pas porter atteinte au droit à la vie privée des autres personnes qui pourraient se trouver dans la pièce.

Sur les dispositifs de vérification de l'identité du candidat comportant un traitement de données biométriques

42. Les établissements organisant des examens à distance ont l'obligation vérifier l'identité des candidats, conformément au cadre juridique portant sur l'organisation des épreuves.

43. La vérification de l'identité du candidat peut être opérée par un rapprochement documentaire effectué par un surveillant lors d'un entretien en visioconférence. Par ailleurs, le recours à un dispositif de vérification automatisé à distance, par comparaison d'un justificatif d'identité avec le visage du candidat peut parfois être justifié, notamment si le nombre d'étudiants est très important.

44. Ce dispositif conduit à traiter des données biométriques au sens de l'article 9 du RGPD et pourrait être mis en œuvre :
    - soit en demandant le consentement des personnes concernées ; une alternative doit alors être disponible (il peut être proposé aux candidats de se rendre sur la session d'examen en ligne en avance afin de laisser au surveillant le temps de procéder à un rapprochement documentaire, par exemple) ;
    - soit s'il est fondé sur un motif d'intérêt public important (g) du 2. de l'article 9 du RGPD). Il doit alors être strictement encadré par un texte et une intervention humaine doit être possible en cas de difficulté de l'étudiant à s'authentifier.

45. À cet égard, le recours à des traitements biométriques de vérification d'identité, dans le cadre de l'application des a) et g) du 2. de l'article 9 du RGPD, devrait répondre aux conditions cumulatives suivantes :
    - une seule vérification d'identité est effectuée avant ou pendant l'examen ;
    - l'examen concerne un nombre d'étudiants très important compte tenu de la nature de l'épreuve (par exemple, une certification obligatoire concernant tous les étudiants d'un établissement) rendant difficile la vérification individuelle par les surveillants ;
    - une alternative est toujours disponible (par exemple, un rapprochement documentaire effectué par un surveillant lors d'un entretien en ligne individuel) pour les candidats ne pouvant pas ou ne parvenant pas à obtenir un contrôle automatique de leur identité;
    - Dans la mesure où le consentement de l'étudiant serait recueilli au moment du déclenchement du dispositif, l'établissement devra informer en amont (par exemple, quelques semaines avant l'épreuve) des modalités précises du recueil du consentement de l'étudiant portant sur le recours à la reconnaissance faciale pour la vérification d'identité.

46. Ce type de dispositif ne doit, en aucun cas, conduire à la constitution de bases de données de gabarits biométriques au sein des établissements d'enseignement supérieur ou des prestataires de télésurveillance d'examens. Le recours à des prestataires spécialisés dans la vérification d'identité à distance, conformément aux recommandations de la CNIL, devrait être privilégié.

47. Les dispositifs comportant un traitement de données biométrique ne devraient être mis en œuvre pour d'autres fins que celles visant la vérification d'identité.

Sur la conservation des données collectées par les dispositifs de télésurveillance

48. Lorsque les dispositifs envisagés pour la télésurveillance d'examens à distance conduisent à une conservation de données à caractère personnel, le responsable de traitement, le cas échéant avec son délégué à la protection des données, doit fixer, avant sa mise en œuvre, les conditions d'accès à ces données et leur durée de conservation ou les critères permettant de la définir, en fonction du type d'information enregistrée et de la finalité du traitement.

49. En cas de suspicion de fraude, la durée de conservation des données ne devrait pas excéder les délais légaux des procédures disciplinaire ou contentieuse qui pourraient être engagées, et qui est en principe de deux mois.

Sur les dispositifs nécessitant l'installation de logiciels dédiés au passage d'examen à distance

50. Certains dispositifs de télésurveillance nécessitent l'installation sur le terminal des candidats d'un logiciel dédié ou d'une extension de navigateur. De tels dispositifs, par exemple un logiciel empêchant l'ouverture de toute application ou de toute page internet en dehors de ce qui est strictement nécessaire au passage de l'examen, peuvent avoir l'avantage de n'entraîner aucune collecte supplémentaire de données à caractère personnel (« *privacy by design* »). Cependant, le responsable de traitement devrait s'assurer que ces dispositifs n'engendrent pas un traitement inégal entre les étudiants (par exemple si le logiciel à installer n'est pas compatible avec certains ordinateurs, navigateurs ou systèmes d'exploitation). Il est également impératif que soit garantie l'absence de réutilisation des données par l'éditeur du logiciel.

Article 5
Sur le transfert de données en dehors du territoire de l'Union européenne

51. Le recours à des sous-traitants, en particulier étrangers, peut impliquer un transfert de données en dehors de l'Union européenne. La CNIL rappelle que le transfert de données hors de l'Union européenne (UE) et de l'Espace économique européen n'est possible qu'à condition de s'assurer d'un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant les outils juridiques prévus par la réglementation.

Article 6
Sur la sécurité des traitements de télésurveillance d'examen

52. Le responsable de traitement doit, conformément au principe de « *privacy by design* », se rapprocher de son délégué à la protection des données en amont de la décision de mettre en place tout dispositif de télésurveillance, afin d'identifier les mesures organisationnelles et techniques permettant de garantir un niveau de sécurité adapté au traitement, conformément à l'article 32 du RGPD.

53. À ce titre, les données à caractère personnel collectées doivent être chiffrées à l'aide d'algorithmes réputés forts, aussi bien durant leur transfert qu'au repos.

54. L'accès en lecture aux données collectées doit par ailleurs être restreint aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, les surveillants, les professeurs ou le conseil de discipline concernés). Cet accès devrait avoir lieu depuis des locaux dédiés et des terminaux spécifiques à la télésurveillance, afin de minimiser le risque de violation de données.

55. Les opérations de modification ou de suppression de données collectées dans le cadre de la télésurveillance d'examens devraient être proscrites si elles concernent des procédures disciplinaires ou contentieuses en cours. Elles devraient, par ailleurs, être réservées aux administrateurs du système d'information.

56. Une journalisation des accès aux données à caractère personnel doit également être mise en place, conformément aux recommandations de la CNIL à ce sujet (délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation). En effet, la journalisation participe, par sa capacité dissuasive, à la sécurité du traitement et au maintien de l'intégrité des données collectées. Les journaux d'accès aux données doivent disposer d'une durée de conservation propre, généralement comprise entre six mois et un an.

57. Dans le cas où le passage d'examen à distance nécessite l'installation d'un logiciel spécifique sur le terminal personnel des candidats, cette installation ne devrait pas engendrer de risques de sécurité. Les logiciels nécessitant des privilèges élevés lors de leur utilisation ou la désactivation des mesures de protection des terminaux (antivirus, par exemple) doivent ainsi être évités. Le responsable de traitement doit également s'assurer que les terminaux peuvent être facilement remis dans leur état initial après le passage de l'examen ou à la fin de l'année universitaire (désinstallation du logiciel et suppression de toutes les traces et configurations laissées par son installation). Les solutions dont le code source est librement accessible (*open-source*) devraient être privilégiées et l'intégrité du logiciel vérifiée avant toute collecte de données à caractère personnel.

La présente délibération sera publiée au Journal officiel de la République française.

La Présidente

Marie-Laure DENIS