PROJET DE RECOMMANDATION

MODALITÉS DE MISE EN ŒUVRE DES DISPOSITIFS DE TÉLÉSURVEILLANCE POUR LES EXAMENS EN LIGNE

La CNIL lance une consultation publique sur la télésurveillance des examens en ligne

Version soumise à consultation publique jusqu'1er janvier 2023

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1. La Commission nationale de l'informatique et des libertés a constaté, en raison notamment de 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 de recourir à des outils de télésurveillance afin d'organiser la validation des enseignements à distance, telle qu'autorisée et encadrée depuis 2017[1].

2. L'article D. 611-12 du code de l'éducation, notamment, 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 s'assortir de certaines garanties : « *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* ». Si le cadre juridique autorise le recours au passage d'examens à distance, il ne l'oblige ni ne l'encourage.

3. Des établissements d'enseignement supérieur ayant recours à des outils de télésurveillance, par nature intrusifs, voire parfois particulièrement intrusifs, (reconnaissance vocale ou analyse de frappe, par exemple), la CNIL souhaite rappeler les obligations qui découlent du RGPD et inciter au respect de certaines bonnes pratiques.

4. L'organisation des examens et concours dans un local dédié, en présence des étudiants et sous surveillance humaine, constitue une modalité de passage d'examen présentant un risque moins élevé pour la protection des données qu'un passage d'examen à distance recourant à la télésurveillance.

5. L'obtention d'un grade universitaire ou l'entrée dans une école ou dans la fonction publique nécessite de garantir une stricte égalité entre les candidats et l'absence de fraude. L'organisation d'un examen à distance pose des difficultés au regard de ces deux exigences.

6. D'une part, la validation des enseignements à distance pourrait, dans une certaine mesure, porter atteinte au principe d'égalité des chances en introduisant des biais socioéconomiques dans les conditions d'évaluation des élèves. En effet, un système d'enseignement et d'évaluation à distance entraine 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 élèves qui ne disposent pas d'une pièce au calme, d'un bureau, d'un ordinateur suffisamment performant, *etc.*

7. D'autre part, la mise en œuvre d'une télésurveillance qui se voudrait aussi performante que celle réalisée dans les locaux d'examen ou de concours 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 observer 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 l'étudiant (notamment les toilettes). En tout état de cause, le recours à des outils de télésurveillance est susceptible d'entraîner une atteinte à la protection des données, de manière parfois particulièrement importante (reconnaissance vocale ou analyse de frappe, par exemple).

8. A l'inverse, l'organisation d'examens à distance peut avoir des conséquences positives, par exemple sur la diversité géographique et sociale des candidats. Il arrive en effet que des candidats renoncent à participer à des examens ou concours du fait de l'éloignement géographique du lieu de passage. De même, l'organisation d'épreuves à distance peut permettre à un étudiant d'obtenir certaines qualifications alors qu'il poursuit ses études ou un stage dans une autre ville ou à l'étranger. L'organisation d'épreuves à distance peut donc s'avérer pertinentes dans certains cas spécifiques, ou certains contextes particuliers (crise sanitaire notamment).

9. Un établissement 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 n'utilisant que 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 systèmes d'exploitation utilisés par les candidats, compatibilité

[1] Voir le Décret n°2017-619 du 24 avril 2017 et le Décret n° 2017-1748 du 22 décembre 2017 fixant les conditions de recours à la visioconférence pour l'organisation des voies d'accès à la fonction publique de l'Etat

avec les antivirus les plus courants, etc.). Cela permet, entre autres, de prévenir la détection de faux positifs par le dispositif de télésurveillance durant l'examen.

10. 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 la recommandation suivante. Si les enjeux ne sont pas les mêmes selon que l'étudiant est dans son domicile privé ou lorsqu'il se trouve dans un local professionnel, certaines des recommandations qui suivent ont vocation à s'appliquer dans les deux cas de figure.

I – Principes généraux sur le recours à ces outils.

11. Si le cadre juridique autorise le recours au passage d'examens à distance, il ne l'oblige ni ne l'encourage. Comme tout traitement de données à caractère personnel, le recours à des outils de télésurveillance doit respecter les principes du RGPD et de la loi informatique et libertés, quelle que soit la technologie utilisée.

12. Les responsables de traitement et leurs éventuels sous-traitants doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les droits et libertés des personnes (article 32 du RGPD).

Ainsi, doivent notamment être respectés les principes suivants :

- Le respect du droit à l'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. Le recours à l'évaluation à distance et aux outils de télésurveillance associés ne devrait pas être motivé par le seul objectif de rendre moins contraignant pour l'établissement l'organisation de la vérification des connaissances des étudiants. Le passage de l'épreuve dans un local dédié et soumis à une surveillance humaine devrait rester la modalité normale d'organisation. Lorsqu'il est pertinent, le passage de certaines épreuves à distance plutôt que dans l'établissement devrait, en principe, être une faculté offerte aux étudiants et non une obligation.

14. Le recours à des épreuves à distance, notamment s'il est obligatoire, devrait être réservé à des cas particuliers pour lesquels cela est pertinent au regard de la nature de l'épreuve, de l'intérêt des étudiants, d'un contexte particulier (par exemple en cas de crise sanitaire) ou de contraintes spécifiques. En particulier, l'ouverture d'une possibilité de passage de l'épreuve à distance est plus pertinente si les modalités d'interrogation de l'étudiant rendent plus difficiles les fraudes dans son domicile (par exemple, dissertations, compositions diverses etc.), permettant ainsi de limiter l'intrusivité des dispositifs de télésurveillance utilisés.

15. 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.

16. Il convient de procéder à une analyse et une réflexion préalable à toute décision d'organiser un examen à distance, en tenant compte des risques réels et des conséquences de ces fraudes, afin d'éviter de recourir à des outils excessivement intrusifs au regard de l'enjeu et des risques. En tout état de cause, comme rappelé plus haut, **l'accès de l'étudiant à ses données collectées dans le cadre de la télésurveillance doit toujours être garanti**.

17. Au surplus, au regard des difficultés que peut poser le passage des examens à distance (stress généré par le 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 et prévoir des solutions alternatives tenant compte des difficultés des étudiants (passage en présentiel ou dans un centre d'examen durant la même session universitaire, prêt de matériel adapté, *etc.*). En aucun cas, le recours aux examens à distance ne doit affecter la réussite des étudiants. Il convient donc de garantir des conditions d'examen aussi équitables qu'en présentiel.

18. En outre, le recours aux examens en ligne et à leur télésurveillance ne doit pas générer de rupture d'égalité entre les étudiants, notamment au regard de leurs moyens matériels. Dès lors, il incombe aux établissements d'enseignement supérieur de tout mettre en œuvre pour éviter toute rupture d'égalité, en choisissant des dispositifs de passage d'examen universels - compatibles notamment avec l'ensemble des systèmes d'exploitation.

II- Sur la base légale

19. La ou les **base(s) légale(s) appropriée(s)** permettant de fonder les traitements de données impliqués dans l'organisation d'examens à distance doivent être déterminées, au cas par cas, dans les conditions prévues à l'article 6 du RGPD.

20. Il ne semble pas possible de retenir **le consentement comme base légale de ces traitements lorsque l'épreuve ne peut être passée qu'à distance dans la mesure où le consentement doit être libre - c'est-à-dire ni contraint ni influencé - et doit pouvoir être retiré à tout moment.** Les étudiants ne peuvent en effet refuser les traitements de données liés à leur passage d'examen sans subir de conséquences négatives.

21. **Les établissements d'enseignement supérieur peuvent s'appuyer sur une autre base légale.** Ainsi, les universités et les établissements privés d'enseignement supérieur, qui poursuivent une mission d'intérêt public, tels que les établissements d'enseignement supérieur privés d'intérêt général par exemple, peuvent se fonder sur l'exécution d'une mission d'intérêt public au sens de l'article 6 du RGPD.

22. **Les établissements d'enseignement supérieur privés** ont la possibilité de fonder les traitements de télésurveillance d'examen sur un contrat, au sens du b du 1. de l'article 6 du RGPD, dès lors que les modalités d'examen sont fixées dans celui-ci en début d'année scolaire.

23. L'intérêt légitime ne devrait pas être retenu en tant que base légale, dans la mesure où cette dernière implique la possibilité de s'opposer au traitement, ce qui ne paraît pas envisageable dans le cadre d'un passage d'examen.

III - Sur l'application de l'article 82 de la loi « Informatique et Libertés ».

24. Certaines opérations de lecture et d'écriture sur l'équipement terminal de l'utilisateur d'un service de communication électronique sont régies par l'article 82 de la loi « Informatique et Libertés ». 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.

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

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. En l'espèce, pour les raisons indiquées ci-dessous, le recueil d'un consentement au sens du RGPD n'est pas envisageable. Dans le cas où l'article 82 est applicable, l'étudiant doit être informé de ce que la connexion à la plateforme d'examen en ligne implique nécessairement certaines formes de télésurveillance impliquant un accès à des informations stockées dans son terminal, l'épreuve ne pouvant pas être passée sans surveillance, ainsi que le rappelle l'article D. 611-12 du code de l'éducation. Les modalités de télésurveillance utilisées doivent être rappelées avant la connexion à la plateforme.

28. 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 qui permet de passer l'épreuve à distance, sont strictement nécessaires à sa fourniture.

IV – Sur la proportionnalité des technologies utilisées pour prévenir les fraudes à l'examen

Observations générales applicables à tous les dispositifs

29. Les établissements d'enseignement supérieur doivent procèdent à une analyse préalable de la proportionnalité des dispositifs envisagés, en associant si possible les responsables pédagogiques et les représentants des étudiants. Cette analyse tiendra 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.

30. Au regard du risque pour les droits et libertés des personnes concernées induits par les dispositifs **de télésurveillance,** le responsable du traitement devra réaliser, au préalable, **une** analyse d'impact relative à la protection des données (AIPD), à moins que le dispositif utilisé n'engendre pas de risques élevés.

31. Dans un souci de transparence, les rapports de ces analyses devraient être rendus disponibles à la consultation pour le personnel éducatif de l'établissement ainsi que pour les étudiants concernés.

Sur la conservation des données collectées par les dispositifs de télésurveillance lors du passage de l'examen à distance

32. Lorsque les dispositifs envisagés pour la télésurveillance d'examens à distance impliquent la conservation de données à caractère personnel, le responsable de traitement doit identifier, 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. Par exemple, les photographies ou captures d'écran prises aléatoirement pendant un examen dans le but de permettre un visionnage différé par des surveillants devraient être supprimées à l'issue de celui-ci, sauf déclenchement d'une procédure disciplinaire.

Sur les dispositifs de télésurveillance en principe proportionnés

33. Le recours aux modalités suivantes de télésurveillance est en principe toujours proportionné :

- La télésurveillance vidéo et audio du candidat en temps réel pendant la durée de l'examen par les personnes chargées de cette télésurveillance ;
- La télésurveillance de l'activité du candidat en temps réel via un partage d'écran ;
- La prise de photographies, de captures d'écran, de flux vidéo et/ou de sons de manière ponctuelle (régulièrement, aléatoirement ou suite à une action de la part d'un surveillant).

34. L'analyse de l'efficacité et de la proportionnalité du dispositif de télésurveillance d'examen doit se faire globalement et non mesure par mesure. Un dispositif, même peu intrusif, peut s'avérer porter une atteinte injustifiée à la vie privée lorsqu'il se révèle inefficace, par exemple si la fraude pour le contourner est trop aisée. Si un juste équilibre ne peut être trouvé entre efficacité de la télésurveillance et intrusivité des dispositifs employés, il faut envisager d'organiser l'épreuve en présentiel.

Sur les dispositifs de télésurveillance procédant à des analyses automatiques et sur les décisions automatisées

35. Certains dispositifs proposent d'**analyser automatiquement des informations collectées pendant l'examen en ligne pour détecter des suspicions de fraude.**

36. Ces dispositifs peuvent, par exemple, **écouter l'environnement sonore des candidats** en temps réel, afin d'alerter lorsque le niveau sonore augmente (suspicion que le candidat parle à une tierce personne). Ce type d'alerte est ensuite traité par un surveillant humain, ou déclenche une action automatique (par exemple l'enregistrement du flux audio du candidat pendant quelques secondes pour analyse *a posteriori*, ou la suspension de la session d'examen du candidat). D'autres dispositifs peuvent également proposer **la détection d'objets ou de tiers non autorisés dans le champ de la caméra**, ou **des analyses du comportement du candidat** (analyse de frappe, de la direction du regard, *etc.*). La décision de déclencher une alerte se fait généralement à l'aide d'algorithmes d'intelligence artificielle, entrainés sur des bases de données d'événements et de comportements suspects.

37. Dans la mesure où de tels dispositifs peuvent générer de nombreux faux positifs pouvant léser l'étudiant et compliquer la surveillance pour le personnel qui en a la charge, l'établissement qui a recours à ces dispositifs devraient réaliser des tests préalables afin de prévenir ces fausses alertes et déterminer la proportionnalité du dispositif. **Ces dispositifs ne devraient jamais conduire à une décision automatique ayant un effet sur le candidat** : il est nécessaire qu'une vérification humaine ait lieu systématiquement avant toute décision pédagogique ou modification des conditions d'examens du candidat afin de constater s'il y a ou non une fraude en cours.

38. Le caractère intrusif de ces dispositifs doit être souligné, en particulier ceux procédant à l'analyse des émotions, qui sont déconseillés. En tout état de cause, une analyse au cas par cas de ces dispositifs doit être effectuée.

39. Ainsi, il peut être proportionné de générer une alerte sur un niveau sonore anormal lorsqu'il y a un grand nombre d'étudiants à surveiller en même temps à distance et qu'il n'est pas possible de visionner simultanément toutes les caméras des ordinateurs ; de même, lorsque la plateforme le permet, il semble possible d'alerter en temps réel un surveillant si un étudiant affiche une page internet ou une fenêtre autre que celles autorisées dans le cadre de l'examen.

Sur les dispositifs de télésurveillance procédant à des traitements de données incidentes

40. Certains dispositifs peuvent entrainer la collecte incidente de données personnelles concernant les candidats, leurs proches ou leur environnement : techniques d'analyse ou d'enregistrement de l'historique de navigation, recours à la caméra à 360°, par exemple ; ces techniques peuvent révéler des informations sur la personne concernée ou son entourage.

41. Bien que le recours à la prise de photographies ou de vidéos lors d'un traitement de télésurveillance présente une probabilité élevée de collecte de données incidentes, la collecte fortuite de tels éléments dans le cadre de la télésurveillance d'examens ne constitue pas nécessairement, en soi, un manquement aux règles applicables en matière de protection des données.

42. Les établissements ont cependant l'interdiction de prendre en compte ces informations ou d'utiliser ces images pour en tirer des informations pouvant relever de la catégorie des données sensibles au sens de l'article 9 du RGPD. Les établissements devraient informer les étudiants sur ces risques et les moyens d'éviter une telle

collecte, notamment de s'isoler, dans la mesure du possible, dans une pièce neutre, de façon à ne pas porter atteinte au droit à l'image des autres personnes qui pourraient se trouver dans la pièce.

Sur les dispositifs procédant à des traitements de données biométriques

43. **Les établissements** organisant des examens à distance **ont l'obligation de procéder à une vérification de l'identité du candidat et à une surveillance de l'épreuve**, conformément au cadre juridique portant sur l'organisation des épreuves.
44. Pour ces deux finalités de vérification d'identité et de surveillance, des traitements de données biométriques au sens de l'article 9 du RGPD (reconnaissance faciale ou vocale) sont parfois mis en œuvre.

45. **S'agissant de la vérification de l'identité du candidat en début d'examen,** le recours à des traitements de données biométriques au sens de l'article 9 du RGPD peut être justifié. Il devra être fondé soit sur le consentement de la personne, soit sur un motif d'intérêt public important (9.2.g du RGPD), s'il est strictement encadré par un texte et sous réserve que l'intervention humaine soit possible en cas de difficulté de l'étudiant à s'authentifier.

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, certifiés selon le référentiel d'exigences PVID publié par l'ANSSI, devrait être privilégié. Il peut également être envisagé d'automatiser la comparaison entre un titre d'identité et le visage filmé du candidat, en excluant toute conservation de données.

47. **Par ailleurs, le recours à des traitements biométriques de vérification d'identité devrait répondre aux conditions cumulatives suivantes :**

- La vérification d'identité est effectuée et en début d'examen uniquement ;
- L'examen visé concerne un nombre d'étudiants important rendant difficile la vérification par un entretien en ligne individuel ;
- Une alternative est toujours disponible lorsque l'étudiant ne parvient ou ne peut pas procéder au contrôle d'identité automatique (rapprochement documentaire effectué par un surveillant lors d'un entretien en ligne individuel) ;
- Lorsque le recours à la biométrie repose sur le consentement des personnes concernées, une alternative devrait être disponible en ligne (il peut être proposé aux candidats de se rendre sur la session d'examen en ligne en avance afin de laisser du temps au surveillant pour procéder à un rapprochement documentaire, par exemple).

48. **D'autre part, s'agissant de la surveillance au cours de l'épreuve**, l'utilisation de dispositifs mettant en œuvre des traitements de données biométriques à des fins de télésurveillance des examens paraît disproportionnée, dans la mesure où il existe des alternatives moins intrusives permettant d'atteindre le résultat visé.

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

49. 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 du strict nécessaire au passage de l'examen, peuvent avoir l'avantage de n'entrainer aucune collecte supplémentaire de données à caractère personnel (« *privacy by design* »). Cependant, il ne devrait être recouru à ces dispositifs qu'après que les responsables de traitement se soient assurés qu'ils n'engendrent pas de risques de sécurité importants (voir section suivante), ni 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).

V – Sur la sécurité des traitements de télésurveillance d'examen

50. 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 les plus appropriées, conformément à l'article 32 du RGPD.

51. Les données à caractère personnel collectées devraient être chiffrées à l'aide d'algorithmes réputés forts, aussi bien durant leur transfert qu'au repos.

52. L'accès en lecture aux données stockées doit par ailleurs être restreint aux seules personnes ayant un intérêt à en connaître en raison de leurs fonctions (par exemple, les surveillants ou le conseil de discipline de l'établissement). Toute opération de modification ou de suppression de données stockées dans le cadre de la télésurveillance d'examens devrait être réservée aux administrateurs du système d'information.

53. 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 6 mois et un an.

54. Dans le cas où le passage d'examen à distance nécessite l'installation d'un logiciel spécifique sur le terminal personnel des candidats, le responsable de traitement devrait s'assurer que ces terminaux puissent 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.

Lien : www.cnil.fr