

Télétravail : Comment assurer la conformité au RGPD ?

13/07/2021



Chaque mois, AvoSial (*) publie une chronique pour actuEL-RH. Ce mois-ci, Sandrine Henrion, avocate associée au sein du cabinet AGIL'IT Avocats rappelle les règles que doivent respecter les employeurs en matière de télétravail afin d'être en conformité avec le Règlement général de protection des données.



AVOCATS D'ENTREPRISE EN DROIT SOCIAL

Le contexte actuel de la crise sanitaire due au Covid-19 entraîne un recours accru au télétravail par les entreprises. Le télétravail est une modalité d'organisation du travail qui implique de la part de l'employeur une vigilance particulière quant au respect des recommandations de la Cnil au regard du RGPD. C'est l'occasion de faire le point sur quelques questions pratiques.

L'activation de la caméra lors des visioconférences

Il est interdit d'enregistrer ou transmettre l'image d'une personne se trouvant dans un lieu privé. Toute personne a droit au respect de sa vie privée (*article 8 de la CEDH ; article 9 du code civil ; article 226-1 du code pénal*). C'est le cas également du salarié en télétravail.

Il s'agira de concilier le droit au respect de la vie privée du salarié et le pouvoir de direction de l'employeur (*article L.1121-1 du code du travail*).

La Commission nationale de l'informatique et des libertés (Cnil), dans ses [questions-réponses sur le télétravail](#), cherche à concilier, d'une part, la volonté du salarié de ne pas donner une vue même partielle de son domicile et, d'autre part, la volonté de l'employeur d'interagir visuellement avec son salarié en télétravail pour se rapprocher le plus possible des conditions de travail en présentiel.

Selon le principe dit de "minimisation" des données, les données à caractère personnel traitées doivent être "adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées" (*article 5.1 du Règlement général de l'Union européenne 2016/679 sur la protection des données*).

L'image du salarié est une donnée personnelle qui doit être traitée de façon adéquate, pertinente et limitée à ce qui est nécessaire au regard des finalités pour lesquelles elle est traitée.

En application de ce principe, la Cnil recommande aux employeurs de ne pas imposer l'activation de leur caméra aux salariés qui participent à des visioconférences. Elle considère qu'une participation via le micro est suffisante. Exiger du salarié qu'il active sa caméra pour rendre visible son image est susceptible de constituer une atteinte au

droit au respect de sa vie privée, tout particulièrement si le salarié travaille depuis son domicile.

Selon la Cnil, seules des "circonstances très particulières" pourraient justifier de rendre nécessaire l'activation de la caméra si aucun autre moyen n'est à disposition de l'employeur pour permettre son identification.

Le contrôle de l'activité des télétravailleurs

Le télétravail n'étant qu'une modalité d'organisation du travail, l'employeur continue d'exercer son pouvoir de contrôle de l'activité de ses salariés, en veillant toutefois à ce que les restrictions au droit au respect de la vie privée du télétravailleur soient justifiées par la nature de la tâche à accomplir et proportionnée au but recherché.

Il doit, en vertu de son obligation de loyauté, informer les salariés, préalablement à leur mise en œuvre, des éventuels dispositifs de contrôle de leur activité (*article L.1222-4 du code du travail*). Dans les entreprises d'au moins 50 salariés, le CSE doit être informé et consulté (*article L.2312-38 du code du travail*).

De plus, pour les télétravailleurs, les modalités de contrôle du temps de travail doivent être précisées par l'accord collectif relatif au télétravail ou par la charte élaborée par l'employeur (*article L.1222-9 du code du travail*).

Par ailleurs, depuis le 25 mai 2018, a priori, aucune déclaration préalable des traitements de surveillance n'est à effectuer auprès de la Cnil mais une inscription au registre des traitements de l'entreprise est nécessaire.

En revanche, en présence d'une surveillance systématique des salariés, les règles sont plus strictes.

En effet, pour certains systèmes de surveillance systématique, l'employeur devra procéder à une analyse d'impact relative à la protection des données (AIPD). C'est le cas notamment des "dispositifs de cybersurveillance tels que ceux procédant à une analyse des flux de courriels sortants afin de détecter d'éventuelles fuites d'information", étant entendu que le recours à ce mode de surveillance ne sera admis que dans certains secteurs d'activité très spécifiques. L'AIPD contiendra en outre une description du système de surveillance, ses finalités, une évaluation de la nécessité et de la proportionnalité du dispositif ainsi qu'une évaluation des risques.

D'autres systèmes de surveillance systématique ne sont quant à eux pas admis car trop excessifs ou intrusifs.

C'est le cas de la surveillance constante au moyen de dispositifs vidéo (par exemple, par webcam) ou audio, tout au long du temps de travail, pour s'assurer de la présence du salarié derrière son écran. C'est le cas également du partage permanent de l'écran et/ou de l'utilisation de "keyloggers" (logiciels qui permettent d'enregistrer l'ensemble des frappes sur le clavier effectuées par une personne sur un ordinateur), qui, sauf

circonstance exceptionnelle liée à un fort impératif de sécurité, est illicite. Enfin, il en est de même pour l'obligation qui incomberait au salarié d'effectuer très régulièrement des actions pour démontrer sa présence derrière son écran (obligation à intervalles réguliers de cliquer sur une application ou de prendre des photos).

La sécurisation de l'utilisation par le salarié d'équipements personnels

Il est possible pour le salarié d'utiliser son équipement personnel mais ce n'est pas une obligation. Si l'employeur met en place le télétravail, il doit fournir un ordinateur si le salarié n'en a pas ou ne veut pas utiliser son ordinateur personnel (*questions/réponses du ministère du travail sur le télétravail*).

La crise sanitaire a pu contraindre certaines entreprises à demander aux salariés qui avaient un équipement personnel (ordinateur portable, tablette, smartphone) de l'utiliser, dans la mesure du possible, le temps d'équiper l'ensemble des salariés. Cette décision emporte des conséquences importantes.

En effet, dès lors que l'utilisation des équipements personnels a été autorisée par l'employeur, celui-ci doit se montrer vigilant car il reste responsable de la sécurité des données personnelles de son entreprise, quand bien même les données seraient stockées sur des équipements personnels des salariés.

Or, les risques en matière de sécurité peuvent s'avérer plus importants avec l'équipement personnel, qui bénéficie parfois d'une protection moindre comparée à celle l'équipement professionnel.

Si l'employeur ne peut pas fournir l'accès aux mails et données professionnelles (accès VPN), le salarié est en droit de refuser de télétravailler. Il revient à l'employeur d'évaluer si le poste de travail est compatible ou non avec le télétravail. Si aucune solution technique ne permet au salarié d'exercer son activité en télétravail, l'activité pourra alors se poursuivre sur le lieu de travail (*questions/réponses du ministère du travail sur le télétravail*).

(*) AvoSial est une association d'avocats en droit du travail et de la sécurité sociale qui conseillent et représentent les employeurs en justice.



Sandrine Henrion

Source URL: <https://www.actuel-rh.fr/content/teletravail-comment-assurer-la-conformite-au-rgpd>