RISQUE CYBER ET DROIT DU TRAVAIL : QUELS IMPACTS ?

Une entreprise victime d'une cyberattaque peut voir son activité gravement perturbée. En réaction au risque cyber, l'employeur peut mettre en place une organisation du travail particulière notamment en matière de durée du travail. Quelles sont ces modifications et quels impacts sur les salariés fautifs ?

Risque cyber : comment réagir ?

Lorsqu'une entreprise est victime d'une cyber attaque, **c'est toute son activité qui peut être impactée**. Pour y faire face, la CNIL préconise de prévoir en amont un plan de maintien de l'activité. S'agissant du droit du travail, des aménagements peuvent également être réalisés pour adapter l'activité en cas de risque cyber ou de violation de données.

S'agissant de la durée du travail, des ajustements peuvent être rendus nécessaires : **certains salariés peuvent devoir travailler plus pour résoudre la cyber attaque,** d'autres au contraire peuvent voir leur activité impossible à maintenir.

Le recours à des heures supplémentaires est possible sous réserve de respecter les dispositions relatives aux durées maximales de travail et de repos. Un salarié ne peut travailler qu'au maximum 10h par jour et 48h sur une semaine, 44h en moyenne pendant 12 semaines. **Il doit bénéficier de 11h de repos quotidien et 35h de repos hebdomadaire. Il existe toutefois des dérogations à ces durées notamment en cas d'urgence.**

Gestion des risques informatiques : le recours aux astreintes

Si un accord collectif le prévoit, il est également possible de mettre en place des astreintes pour permettre des interventions en dehors des horaires d'ouverture si nécessaire. Le temps d'intervention pour réduire le risque cyber sera du temps de travail effectif. L'employeur devra s'assurer que le salarié bénéficie bien de son temps de repos quotidien à compter de la fin de son intervention.

En raison de ces circonstances exceptionnelles, **l'employeur peut demander (et non imposer) à des salariés en congés payés de mettre fin à leurs congés payés et de reprendre leur poste pour résoudre la crise**. Certaines conventions collectives prévoient des contreparties à ce rappel pendant les congés payés.

Par ailleurs, si la cyberattaque rend impossible le maintien de toute ou partie de l'activité, **l'employeur peut proposer (et non imposer) aux salariés concernés, l**a prise de congés payés. Le recours à l'activité partielle en raison de ces circonstances exceptionnelles telles que le cyber risques semble également possible.

Cyber attaque : comportement fautif du salarié et formation aux risques cyber

Cybersécurité : comportement à risque, quels recours ?

Les actions des salariés peuvent être à l'origine de failles de **cybersécurité en entreprise** voire être la porte d'entrée de cyberattaque. La question des agissements à risque et le fait de sanctionner un salarié peut se poser.

D'un point de vue juridique, **la présence d'une charte informatique ayant la valeur d'un règlement intérieur prend toute son importance car le salarié qui ne la respecte pas peut être passible d'une sanction**. Il convient avant toute chose d'établir que le salarié a commis une faute, qui est définie par le Code du travail comme tout " agissement du salarié considéré par l'employeur comme fautif - Article L1331-1" Pour déterminer la nature de la sanction, le Code du travail dispose que **toute sanction doit être proportionnée à la faute commise.** Les sanctions pécuniaires sont interdites. De nombreux éléments sont donc à prendre en compte pour déterminer la sanction adéquate, et notamment les suivants :

- L'agissement du salarié a-t-il agit à l'encontre d'une consigne dont il avait été informé ?

- A-t-il récemment suivi une action de sensibilisation aux cyberattaques, voire de formation qui avait abordé le comportement qui lui est reproché ?

- A-t-il de l'ancienneté ?

- Quel est son poste ? Nécessite-t-il d'utiliser des outils informatiques ? à quelle fréquence ?

Un employeur pourra sanctionner différemment deux salariés ayant commis une même faute, en fonction de la différence de leurs situation. En cas de contestation il reviendra au juge d'apprécier le caractère proportionné ou non de la sanction.

Prévention des risques cyber : quelle utilité ?

Ainsi, s'il peut être possible de sanctionner un agissement fautif d'un salarié c'est à la condition d'avoir préalablement mis en place des actions de gestion des risques :

- **de prévention des risques cyber**

- Sensibilisation

- Formation des salariés aux bonnes pratiques de cybersécurité

L'accent est à mettre sur des actions plus efficaces pour éviter une cyberattaque qu'une sanction qui pourrait avoir, par ailleurs, des effets néfastes sur le climat de travail, notamment pour les salariés ayant des difficultés sur l'outil informatique.

https://www.svp.com/actualite/risque-cyber-droit-du-travail-20241003?utm_source=thematic_newsletter&utm_medium=email&utm_campaign=thematic_newsletter_20241022