Covid-19 : télétravail et protection des données personnelles

Le 5 mai 2020, le Conseil National a adopté le projet de Loi n°1.014, qui favorise entre autres le recours au télétravail.

Ce vote a donné lieu à la publication en date du 15 mai 2020 de la Loi n° 1.488 du 11 mai 2020 interdisant les licenciements abusifs, rendant le télétravail obligatoire sur les postes le permettant et portant d'autres mesures pour faire face à l'épidémie de COVID-19.

Toutefois si l'intitulé de cette Loi mentionne que le télétravail est rendu obligatoire, les articles 10 et 11 de ce texte soumettent la mise en place du télétravail à deux conditions cumulatives :

- l'accord du salarié,
- la mise à disposition par l'employeur des moyens techniques et matériels nécessaires à un tel exercice.

Aussi, face à la généralisation récente du télétravail, en Principauté, la CCIN a jugé nécessaire de rappeler les bonnes pratiques à adopter tant côté employeurs que coté salariés afin d'assurer la sécurité des systèmes d'information, la protection des données personnelles et le respect de la vie privée des salariés.

Travailler depuis son domicile n'est en effet souvent pas aussi sécurisé qu'au sein de son entreprise, ce qui est une aubaine pour les pirates informatiques, toujours prêts à profiter de la moindre faille de sécurité.

Le travail à distance effectué le plus souvent de son domicile ne doit pas conduire à une surveillance constante et inopportune du travail ou du temps de travail des salariés, ni à enfreindre le nécessaire respect de leur vie privée et de celle de leur entourage.

Recommandations pour les employeurs

Il est important de prendre à la fois des mesures pour assurer l'information et la sensibilisation des salariés et des mesures techniques pour sécuriser le système d'information.

Les mesures pour assurer l'information et la sensibilisation des employés

Sensibilisez vos employés. Quelles que soient les solutions technologiques adoptées, vous devez sensibiliser dès le départ vos employés aux enjeux de sécurité liés au télétravail en les formant aux meilleurs usages et en leur faisant prendre conscience des risques que leurs actions (ou manque d'actions) peuvent avoir sur la sécurité du système d'information (par exemple l'absence de mise à jour d'un antivirus ou l'utilisation d'un Wifi non sécurisé).

Encadrez les usages, par exemple par le biais d'une charte informatique ou de tout autre document détaillant de manière claire les bonnes pratiques à adopter, les restrictions apportées et les procédures à respecter.

Apportez un soutien réactif à vos employés en télétravail en donnant au service technique (ou tout autre service dédié) les moyens de répondre rapidement et efficacement aux questions posées et/ou

aux problèmes techniques rencontrés par lesdits employés. Cela permettra d'éviter que ceux-ci n'essaient de résoudre les problèmes par eux-mêmes, souvent au détriment de la sécurité informatique de la société.

Les mesures techniques pour sécuriser le système d'information

Catégorisez les données et analyser les risques pour une plus grande sécurité informatique. Pour cela, il convient d'identifier clairement les risques que votre société peut encourir, en classant notamment les données selon leur sensibilité afin d'envisager pour certaines d'entre elles d'en interdire l'accès à distance, ou pour d'autres de mettre en place des mécanismes de sécurité renforcés.

Vous devez fournir à vos employés les équipements nécessaires (PC, téléphone, tablette…) à leur travail. Ces équipements seront ainsi sécurisés et maîtrisés par l'entreprise.

Mettez en place un système d'authentification à double niveau afin de limiter les risques d'intrusion. Il est en effet indispensable d'identifier avec certitude chaque employé. Aussi, lorsqu'un employé se connecte au réseau de l'entreprise, il convient de lui demander, par exemple, de renseigner au préalable un identifiant et mot de passe, puis un code à usage unique généré par une application ou un « *porte-clef* ».

Equipez tous les postes de travail des employés au minimum d'un pare-feu, d'un antivirus et d'un outil de blocage de l'accès aux sites malveillants. Les solutions antivirales utilisées doivent être des versions professionnelles afin de protéger l'entreprise de la plupart des attaques virales connues. Par ailleurs, les mises à jour de sécurité doivent être déployées dès qu'elles sont disponibles, les cybercriminels mettant peu de temps à exploiter les failles lorsqu'ils en ont connaissance.

Sécurisez vos accès extérieurs en mettant en place un VPN (*Virtual Private Network* ou « *réseau privé virtuel* ») pour éviter l'exposition directe de vos accès sur internet. Optez pour l'authentification du VPN, de préférence à deux facteurs pour vous prémunir de toute usurpation. Outre le chiffrement de vos connexions extérieures, ce dispositif permet également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements et seules personnes authentifiés.

Renforcez votre politique de gestion des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, en vous assurant que lesdits mots de passe sont suffisamment longs, complexes et uniques (combinaison de majuscules, minuscules, chiffres et caractères spéciaux) sur chaque équipement ou service utilisé. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

Utilisez des protocoles garantissant la confidentialité et l'authentification du serveur destinataire en vous assurant que vous disposez bien des versions les plus récentes de ces protocoles.

Mettez en place une journalisation systématique de l'activité de tous vos équipements d'infrastructure (serveurs, pare-feu, proxy…) et consultez régulièrement les journaux d'accès aux services accessibles à distance pour détecter tout comportement suspect. Prévoyez également une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure, voire des postes de travail. Cette journalisation et cette consultation des accès vous permettront de détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations. Elles vous permettront également de comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier.

Mais attention : si cette vérification des accès et de l'activité sur vos équipements conduit à la surveillance du travail ou du temps de travail de vos employés l'article 11-1 de la Loi n° 1.165 relative à la protection des informations nominatives s'applique et ces mesures de surveillance sont soumises à l'autorisation préalable de la CCIN.

De plus vos salariés doivent être préalablement informés de l'existence de telles mesures de surveillance de leur activité.

Nous vous invitons à vous reporter à la recommandation de la CCIN sur la gestion des habilitations et des accès informatiques :

https://www.ccin.mc/images/documents/26c89ba0fc0c084c6473cc533e7fb67b-b04f83a5503b1cc27a5a5d2bc7bcd1f6-Delib-2017-206-Recom-habilitations.pdf

Ne rendez pas directement accessibles les interfaces de serveurs non sécurisées. De manière générale, limitez le nombre de services mis à disposition au strict minimum pour réduire les risques d'attaques.

Durcissez les sauvegardes de vos données et activités. Celles-ci doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent. De même, il est important de vous assurer du niveau de sauvegarde de vos hébergements externes (cloud, site Internet d'entreprise, service de messagerie…) pour vous assurer que le service souscrit est bien en adéquation avec les risques encourus par l'entreprise.

Mettez en place des dispositifs de mise en veille automatique. Les équipements fournis à vos salariés doivent se mettre en veille automatiquement après un bref laps de temps sans activité, et ce afin d'éviter que toute personne non autorisée puisse accéder aux informations accessibles depuis votre système d'information.

Si vous avez fourni des *« webcams »* à vos salariés : afin de préserver la vie privée des salariés et de leur entourage *les caméras ne doivent pas être activées de manière permanente, mais uniquement pour des circonstances spécifiques (participation à certaines réunions de travail par visioconférence par exemple). Cependant vos salariés doivent pourvoir refuser d'utiliser la caméra, sauf justification étayée le nécessitant. Dans le cas contraire le recours à la conférence téléphonique constitue une modalité adéquate de participation aux réunions de travail.*

Les visioconférences ou les conférences téléphoniques ne doivent pas donner lieu à enregistrements, sauf justification particulière à des fins probatoires par exemple. Si tel est le cas les participants doivent en être préalablement informés.

Recommandations pour les employés

Suivez scrupuleusement les consignes de votre employeur en matière de sécurité, en respectant notamment la charte de l'entreprise si un tel document a effectivement été mis en place. En cas de difficultés à appliquer les mesures prescrites, il convient d'en informer immédiatement l'entreprise qui seule sera en mesure d'y remédier.

Utilisez les équipements et outils fournis par votre entreprise (ordinateur, téléphone, VPN…) pour le télétravail.

Sécurisez votre connexion internet. Le Wi-Fi peut être un point d'accès très fragile à votre ordinateur pour les hackers. Or, beaucoup de gens ont installé leur box Internet sans nécessairement changer les mots de passe par défaut ou bloquer certains accès. Vous devez donc vous assurer que vous avez bien activé les protections de votre box internet notamment en matière de Wi-Fi (chiffrement WPA2 ou WPA3) et de pare-feu intégré. Pensez également à mettre à jour régulièrement ladite box soit en la redémarrant, soit depuis son interface d'administration.

Renforcez vos mots de passe. La majorité des attaques informatiques étant due à des mots de passe trop simples, il est important d'utiliser des mots de passe suffisamment longs, complexes et différents, en mélangeant majuscules, minuscules, chiffres et caractères spéciaux, sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

Séparez votre usage professionnel de votre usage personnel. L'activité professionnelle doit se faire sur vos moyens professionnels et seulement sur vos moyens professionnels et l'activité personnelle doit se faire uniquement sur vos équipements personnels. Il convient ainsi de créer des comptes différents sur les sites ou les logiciels que vous utilisez. De même, le VPN fourni par l'entreprise doit être utilisé uniquement pour télétravailler et non pour surfer sur les sites de streaming vidéo !

Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablettes, téléphones…) dès qu'elles vous sont proposées afin de corriger les failles de sécurité qui pourraient être utilisées par des pirates pour s'y introduire et les utiliser pour attaquer le réseau de votre entreprise au travers de vos accès.

Ne faites pas chez vous ce que vous ne feriez pas au travail. Cela implique notamment de ne pas vous rendre sur des sites suspects et de n'installer des applications sur vos équipements professionnels qu'après l'accord du service informatique de votre entreprise. Par ailleurs, il convient de limiter au maximum les usages récréatifs (réseaux sociaux par exemple) sur vos équipements professionnels.

Méfiez-vous des messages (email, SMS,…) comprenant une demande douteuse ou un contenu inattendu. Il peut en effet s'agir d'une attaque par hameçonnage destinée à vous dérober des informations confidentielles (identifiant, mots de passe), de l'envoi d'un virus par pièce-jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque aux faux ordres de virement. Ne cliquez jamais sur les pièces jointes/liens dans les messages, demandez toujours confirmation à l'émetteur par un autre moyen, et en cas de doute, contactez le service informatique de votre société.

Communiquez en toute sécurité en privilégiant les canaux de communication interne de votre entreprise.

Sauvegardez régulièrement votre travail, si possible sur le réseau de l'entreprise, ou par le biais des moyens qu'elle met à disposition à cet effet (support externe chiffré que vous débranchez une fois la sauvegarde effectuée.)