



LABRUYÈRE & CO
A V O C A T S
D R O I T D U N U M É R I Q U E



Le Télétravail au cœur d'une transformation sociétale

Edition septembre 2020

SOMMAIRE

INTRODUCTION	3
CHAPITRE 1. L'EMERGENCE D'UNE NOUVELLE ORGANISATION DE TRAVAIL	6
CHAPITRE 2. LES AVANTAGES ET LES RISQUES LIÉS AU TÉLÉTRAVAIL	11
CHAPITRE 3. LA COMPATIBILITÉ DU TÉLÉTRAVAIL AVEC LE RGPD	15
<i>1) Les obligations de l'entreprise pour télétravailler dans les meilleures conditions</i>	
<i>2) Les devoirs du salarié, de nouvelles habitudes à adopter</i>	
<i>3) L'utilisation des outils personnels – Bring Your Own Device .. ou Disaster (BYOD)</i>	
<i>4) L'adéquation entre télétravail et vie privée</i>	
CHAPITRE 4. LE TÉLÉTRAVAIL, UN ÉCOGESTE POUR LA PLANÈTE ?	30
CONCLUSIONS	33
SOURCES	35
AUTEURS	36

INTRODUCTION

Ces dernières années, la révolution du numérique a permis l'émergence de nombreuses innovations qui ont changées le quotidien des travailleurs et leur comportement face au travail. La transition numérique a ainsi intensifié et facilité les échanges grâce aux emails, au cloud, à une gestion RH simplifiée via des plateformes, à une généralisation des intranets ou encore via une nouvelle façon de travailler avec la démocratisation du télétravail.

En effet la transformation numérique est aujourd'hui au centre de nos vies quotidiennes, personnelles et professionnelles, notamment via la mise en place du télétravail.

Et à son tour, le télétravail transforme les modes d'organisation, de gestion, de productivité, d'interaction entre les membres d'une même entreprise.

L'HISTOIRE DU TELETRAVAIL

LES PREMICES DU TELETRAVAIL

- 1950** Norbert Wiener, père de la cybernétique supervise la construction d'un immeuble aux Etats-Unis depuis l'Europe, grâce aux moyens de transmissions de données.
- 1972** Alvin Toffler dans son ouvrage « Le choc du futur », prédit la migration du bureau vers le domicile par ce qu'il appelle le « Téléwork ».

LE DEVELOPPEMENT DES NTIC

- 90's** Les innovations en matière de communication à distance (minitel, Macintosh d'Apple, World Wide Web de Tim Berners Lee), ont permis de faciliter le développement du télétravail.

L'AIDE DES POLITIQUES

Certaines politiques sociales ont aussi été d'une grande aide afin que le télétravail s'impose dans le monde professionnel.

- 2002** Accord-cadre européen en date du 16 juillet 2002 : le télétravailleur dispose des mêmes droits que le salarié qui travaille dans l'entreprise.
- 2005** Accord national interprofessionnel du 19 juillet 2005 : le texte européen est transposé par la Loi relative à la simplification du droit et des allègements des démarches administratives. Puis il est codifié dans le Code du Travail aux articles L.1222-9 à L.1222-11.
- 2017** Ordonnance Macron relative à la prévisibilité et à la sécurisation des relations de travail en date du 22 Septembre 2017 : le télétravail est reconnu comme une méthode de travail.



L'HISTOIRE DU TELETRAVAIL



L'ACCELERATION DU RECOURS AU TELETRAVAIL

Ce qui fait la popularité du télétravail est la simplicité de sa mise en œuvre car il ne nécessite qu'une connexion internet et un équipement informatique (ordinateur, smartphone, tablette).

Alors que le télétravail n'était pas une pratique, très répandue en France (en 2017 la France comptabilisait seulement 25% de télétravailleurs), cette tendance s'est accrue fin 2019. Les différents mouvements de grève mais surtout la pandémie du Covid-19 a obligé une bonne partie des salariés français à travailler de chez soi. Dans un contexte de confinement imposé par l'Etat pour limiter la propagation du virus, tout en maintenant une activité économique, ce mode de travail s'est très vite imposé en quelques mois.

Aujourd'hui le télétravail est devenu plus qu'une réalité économique, il contribue à l'accroissement de la productivité et de la compétitivité des entreprises, mais aussi au bien-être des salariés et au respect de notre environnement. Cependant, le télétravail en tant que prolongement de la transition numérique, doit obligatoirement être encadré afin de garantir son utilité à l'entreprise.

Le recours au télétravail peut être source de risques pour l'entreprise mais aussi générer des atteintes à la sécurité et à la santé du télétravailleur. Cette méthode de travail nécessite une particulière vigilance afin de limiter le risque de failles de sécurité pouvant faciliter la cyber malveillance, les atteintes en matière de protection des données personnelles, la possibilité de fraude interne ou le développement de risques de santé pour les salariés (risques psychosociaux).

La mise en place du télétravail se doit d'être préparée et accompagnée par les dirigeants et les salariés (accessibilité des outils informatiques, mise en œuvre d'un minimum de sécurité) afin de tirer uniquement les avantages de cette forme d'organisation.

QUELQUES CHIFFRES



Selon une **étude de Malakoff Humanis**, en 2019 :

30 %

*Des télétravailleurs
étaient issus du
secteur privé*

47 %

*Des télétravailleurs
pratiquent le télétravail
moins d'un jour par semaine*

Selon **l'étude Télétravail de Malakoff Humanis**, en 2020 :

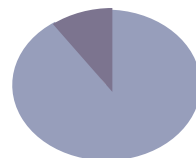
36%

*des salariés révèlent que leur entreprise les
incite à télétravailler pendant la crise du
Covid-19*

41%

*pendant la période du confinement, le
télétravail s'est surtout développé en Ile de
France avec un total de 41% de
télétravailleurs*

Autres 10 %



Télétravail au domicile

90 %



CHAPITRE 1
L'ÉMERGENCE D'UNE NOUVELLE
ORGANISATION DU TRAVAIL

1) Présentation du télétravail

Le télétravail est une méthode d'organisation du travail, qui s'appuie sur les nouvelles technologies.

Il est défini comme « *toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication (article L1222-9 du Code du Travail)* . »

Cette modalité d'organisation du travail permet au salarié de façon volontaire, d'effectuer son travail hors des locaux de l'entreprise.

Soit :

- Chez lui
- Dans un télécentre ou espace de coworking

1.1) Sous quelles conditions ?

Les conditions de mise en place du télétravail sont fixées par l'Ordonnance du 22 Septembre 2017 relative à la prévisibilité et à la sécurisation des relations de travail. Ces règles sont assez souples, car elles n'imposent aucune modification du contrat de travail, lorsqu'un salarié souhaite y recourir. En effet, le télétravail est mis en place par :

- Simple accord mutuel entre l'employeur et le salarié (notamment par oral, email, avenant au contrat)
- Accord collectif
- Charte élaborée par l'employeur après avis du Comité social et économique

Le télétravail peut tout de même être imposé par l'employeur en cas de force majeure ou de circonstances exceptionnelles, comme nous l'avons vécu avec la crise épidémique du Covid-19.

Certaines modalités sont alors à définir (**article L.1222-9 du Code du travail**) :

- Les conditions de passage au télétravail ;
- La durée du travail ;
- Les plages horaires dans lesquelles le télétravailleur pourra être contacté ;
- Les modalités d'acceptation par le salarié des conditions de mise en œuvre du télétravail ;
- Le mode de contrôle de temps de travail du salarié ou de régulation de la charge de travail ;
- Les modalités d'utilisation des outils et matériels mis à sa disposition ;
- Les sanctions encourues en cas de non-respect ;
- Les modalités de la période d'adaptation et du préavis ;
- La prise en charge de divers frais par l'employeur ;
- Les modalités d'accès des travailleurs handicapés à une organisation en télétravail.

1.2) Qui est concerné par le télétravail ?

Un accord collectif ou une charte peut prévoir des conditions d'éligibilité et dès lors fixer des critères objectifs et justifiés comme par exemple l'ancienneté.



2) Les devoirs de l'employeur

D'après l'**article L1222-9 du Code du Travail**, le télétravail est un droit.

En effet, l'employeur qui le refuse au salarié qui peut en bénéficier, selon les conditions prévues, doit impérativement motiver sa décision.

L'employeur doit informer le salarié sur toute restriction à l'usage d'équipements ou d'outils informatiques ou de services de communications électroniques, et des sanctions passibles en cas de non-respect des restrictions.

Tous les ans, il doit organiser un entretien portant sur les conditions d'activité du salarié et sur sa charge de travail.

Il doit aussi prévoir une protection des données ainsi que de la sécurité du système informatique de l'entreprise.

L'employeur n'a pas d'obligation de fixer une charte pour le télétravail mais il lui est fortement encouragé de le faire, afin de fixer les droits et devoirs de chacun au sein de l'entreprise.

Il est possible pour l'employeur ainsi que les représentants du personnel et les autorités administratives compétentes d'accéder au lieu du télétravail. Si le travailleur exerce son activité à son domicile, la demande devra impérativement être notifiée au salarié qui devra en amont donner son accord.



3) Droits du télétravailleur


En tant que salarié de l'entreprise, le télétravailleur bénéficie des mêmes droits individuels et collectifs que sur son lieu de travail et notamment :

- Du droit au respect de sa vie privée (*Arrêt Nikon 2001*) ;
- L'accès à toute formation ;
- La santé et la sécurité sociale (un télétravailleur ayant un accident est considéré comme ayant un accident de travail au sens de **l'article L.411-1 du Code de la sécurité sociale**) ;
- L'accès aux activités sociales de l'entreprise (participation aux élections professionnelles), aux informations syndicales ainsi qu'à tous les avantages sociaux (titres-restaurant, chèques vacances).



- Le salarié peut refuser de recourir au télétravail sans que cela ne soit un motif de rupture du contrat de travail (**article L1222-9 du Code du Travail**).
- Le salarié peut demander à l'employeur de prendre en charge le matériel informatique ou la connexion internet, si ce dernier ne dispose d'aucun matériel pour télétravailler (**article 7 de l'accord national interprofessionnel du 19 juillet 2005**). Cependant l'employeur n'a aucune obligation d'accepter.
- Le salarié qui utilise son domicile à des fins professionnelles, peut demander une indemnité d'occupation à son employeur lorsqu'un local professionnel n'est pas mis à sa disposition, et qu'il ne dispose pas du matériel nécessaire pour travailler. En effet cela peut constituer une immixtion dans la vie privée du salarié (**Cour de cassation, chambre sociale, 27 mars 2019 n°17-21.014**).

Cependant, dans le cas de circonstances exceptionnelles et afin de permettre la continuité de l'activité de l'entreprise et de garantir la protection des salariés, cette indemnité n'est pas obligatoire car le télétravail est considéré comme un aménagement du poste de travail nécessaire.



CHAPITRE 2
LES AVANTAGES ET LES
RISQUES LIÉS AU
TÉLÉTRAVAIL

Le télétravail présente un certain nombre de **bénéfices**. D'après **l'étude Télétravail 2020 Malakoff Humanis**, le télétravail entraîne :



Des **effets positifs sur la santé et le bien-être** (90 % des télétravailleurs constatent une diminution de la fatigue, du stress, mais aussi de la pollution sonore, ainsi qu'un cadre de travail plus confortable et une meilleure conciliation en présence d'un handicap ou d'une maladie chronique)



Une **réduction de la pollution**, 87 % des salariés perçoivent le télétravail comme un éco geste car les salariés utilisent moins les transports, ce qui permet de réduire l'empreinte carbone



L'accroissement de l'autonomie et de la productivité au travail

L'augmentation de l'engagement des salariés



Des **économies financières** ainsi qu'une **réduction de l'absentéisme**



Un **meilleur équilibre entre vie professionnelle et personnelle** (pour 46 % des salariés interrogés dans l'enquête, cela permet de réduire le temps de trajet ainsi que pour 39% cela leur donne la possibilité d'adapter leurs horaires)

Par exemple, un temps de trajet réduit donne au salarié d'autres opportunités pour organiser sa journée : cela lui permet d'emmener ses enfants à l'école, de faire des courses, de commencer plutôt la journée pour ensuite faire du sport ou une activité le soir.

Cependant, le télétravail n'a pas que des avantages, et peut entraîner des **inconconvénients**, d'autant plus lorsque le télétravail n'est pas organisé. Le risque est :

L'empiètement de la vie professionnelle sur la vie personnelle : *c'est un poids pour 57 % salariés, 51 % d'entre eux parlent même d'un risque d'addiction au travail.* En effet, la sollicitation perpétuelle par emails, la création de groupe d'échanges ou encore les conférences à distance peuvent conduire le salarié à développer une certaine hyper-connexion au travail dans le but de se rendre continuellement utile



La **rupture des liens sociaux, l'isolement des salariés**

La **diminution du sentiment d'appartenance** à l'entreprise et un **désintérêt professionnel**



Des échanges plus compliqués avec les collaborateurs et des **difficultés techniques** dues aux outils utilisés (*manque de connaissance, mauvaise connexion*)



Des **difficultés liées à l'organisation** de l'employeur ainsi qu'à la **sécurisation des données et des outils**



Des coûts supplémentaires pour la fourniture d'équipements informatiques ainsi que pour les formations des salariés (*par exemple faire appel à des services externes afin de donner des formations sur les usages informatiques, les procédures de sécurité*)



Un accroissement des inégalités (*entre les salariés disposant ou non de matériel informatique/ d'un lieu dédié au télétravail/ ayant des enfants à charge*)



Un **risque sur la santé** (*détresse psychologique, surcharge de travail, droit à la déconnexion quasi-inexistant*)

Ainsi même si certains inconvénients existent, les salariés et leurs dirigeants s'accordent sur les bénéfices du télétravail.

C'est ce qui ressort de l'Enquête Obergo de 2019, qui souligne que cette forme de travail est un « **facteur d'amélioration des conditions de vie** » à la fois sur son lieu de travail mais aussi en dehors.

Pendant le télétravail doit être utilisé avec parcimonie et de manière organisée pour que les inconvénients ne surplombent pas les avantages, comme notamment l'affaiblissement du lien social, l'empiètement entre vie privée et professionnelle ou encore les risques sur la santé.

C'est pourquoi, selon les experts, il est conseillé de recourir au télétravail **seulement deux (2) jours par semaine**, pour profiter des bénéfices, de ce dernier.





CHAPITRE 3
LA COMPATIBILITÉ DU
TÉLÉTRAVAIL AVEC LE
RGPD

Le Règlement Général sur la Protection des Données (n°2016/679) dénommé **RGPD**, est un règlement applicable à tous les pays de l'Union Européenne et qui ne nécessite aucune transposition dans les pays membres. **Il encadre le traitement des données à caractère personnel dans l'espace européen.**

Les **données à caractère personnel** se définissent comme toutes informations se rapportant à une personne physique identifiée ou identifiable notamment par référence à un identifiant, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (article 4 du RGPD).



Au-delà des bénéfices mais aussi de certains inconvénients, le télétravail impose certaines mesures en faveur de la protection des données personnelles des salariés.

Dans la mesure où le travail s'effectue à distance, de nombreuses données sont échangées, et l'employeur détient également des informations présentant un risque pour le respect de la vie privée de son salarié comme par exemple sa géolocalisation.

Ces mêmes préoccupations se posent du côté de l'employeur car ce dernier doit s'assurer que les mesures de sécurité imposées au salarié dans les locaux de l'entreprise, s'appliquent aussi lors du télétravail. Diverses mesures sont donc à prendre afin d'éviter tout risque de cyberattaques et de garantir la protection des données personnelles de chaque salarié.

1) Les obligations de l'entreprise pour télétravailler dans les meilleures conditions

Afin que la mise en place du télétravail se fasse dans les meilleures conditions, des points de vigilance particuliers sont à observer. Il semble impératif que les principes de confidentialité et d'intégrité des données mais aussi une authentification claire des utilisateurs, soient respectés.

C'est ainsi que la CNIL préconise certaines bonnes pratiques à prendre par l'employeur :

- **Obligation de sensibilisation**

L'employeur doit formaliser des mesures internes afin de protéger les données personnelles mais aussi dans le but de prévenir toutes failles de sécurité. Ainsi son obligation de sensibilisation des salariés est primordiale pour mettre en place une organisation optimale et sans risque.

Il lui est donc conseillé de rédiger une **Charte de sécurité du télétravail ou bien une Charte informatique** comportant des règles d'utilisation des outils numériques, les moyens de les sécuriser ainsi que les droits et devoirs à respecter. En effet, pour beaucoup d'entreprises la maîtrise des outils numériques et leur sécurité est assez faible. La sensibilisation doit nécessairement être réalisée afin de protéger les données personnelles mais aussi le secret des affaires des entreprises. La Charte informatique doit alors être régulièrement communiquée aux salariés.

Il est également important pour l'employeur de sensibiliser sur la question de la frontière entre vie personnelle et vie professionnelle dans les outils numériques.

L'ANSSI et la DGCRRF alertent sur les risques de cyber-malveillance et sur l'importance d'informer les salariés sur les dangers existants. En effet, dans la plupart des cas, les risques de cyber-attaques ont pour origine la négligence, l'erreur de manipulation ou bien de configuration de poste. Ainsi il est important d'avoir des recommandations sur « quoi faire en cas de cyber-attaques » afin d'y être préparé pour pouvoir réduire les conséquences négatives.



Voici une liste de quelques cybermenaces liées au télétravail :



Le Hameçonnage/Phishing : technique qui consiste à voler les données personnelles d'un organisme/entreprise dans le but d'usurper son identité par le biais de SMS, appel téléphonique, e-mail alarmiste demandant de communiquer en urgence des renseignements privés.



- **Le Rançongiciel/Ransomware** : technique qui consiste à chiffrer ou empêcher l'accès des informations professionnelles aux entreprises afin d'obtenir une rançon ou dans le seul but de détruire les données. Cette détention de données se fait via l'envoi d'e-mails contenant un lien vers un logiciel malveillant, une pièce jointe infectée ou une intrusion dans le système informatique.

- **Le Vol de données**



- **La Fraude au Président** : le dirigeant d'une entreprise se fait pirater ses appareils électroniques par un escroc qui se fait passer pour lui et qui demande le virement d'une somme importante ou le changement des coordonnées bancaires.



Afin que les mesures de sécurité soient suivies par les salariés, l'employeur se doit de montrer l'exemple et donc d'adopter un comportement sécuritaire. Il peut également proposer à ses employés de suivre les modules de formations (en ligne et gratuits) sur la sécurité de la **CNIL ou de l'ANSSI**.

- **Principe de responsabilité**

La protection des données personnelles détenues par l'entreprise est de la **responsabilité du dirigeant**. Il doit donc identifier les risques possibles et en estimer la gravité. Le dirigeant devra ensuite déterminer les mesures à mettre en place.

En terme de contrôle de l'activité des salariés, l'employeur peut être amené à **traiter des données personnelles**. Les données personnelles en jeu sont alors celles du télétravailleur notamment les données concernant son mode de vie, comme le type d'équipements informatiques utilisés par le salarié, la nature de son réseau internet ou encore l'espace de coworking utilisé. Pendant le confinement, de nombreux managers ont voulu effectuer des sondages afin de recenser les conditions dans lesquelles leurs employés télétravaillaient. Cependant ces sondages relèvent de la collecte de données personnelles car ils pouvaient interroger les salariés sur leur lieu de vie, le matériel à disposition, le nombre d'enfants à charge. **Ces traitements de données doivent être en accord avec le RGPD.**

Un équilibre doit donc être trouvé **entre la protection des données personnelles, le respect de la vie privée et l'exercice du pouvoir de direction de l'employeur**. *Par exemple : le dirigeant doit informer le salarié du contrôle qu'il exercera sur le traitement de ses données. Il doit donc lui garantir que ces informations seront protégées et qu'il pourra exercer ses droits sur ces dernières, tels que le droit d'accès aux informations recueillies, le droit d'opposition, le droit à l'effacement.*

En vertu du **RGPD**, une **analyse d'impact** sur la protection des données personnelles doit être effectuée lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes* ».

La **CNIL** établie une liste dans laquelle elle indique dans quels cas une analyse d'impact doit être effectuée. Elle estime que les traitements ayant pour finalité de « *surveiller de manière constante l'activité des employés concernés* » impose automatiquement l'établissement d'une analyse d'impact.

En tant **que responsable de traitement des données de ses salariés**, l'employeur est responsable de tout manquement susceptible de leur porter atteinte. Il doit notamment **alerter la CNIL** en cas de violation de données à caractère personnel susceptible d'entraîner un risque pour les droits et libertés des personnes concernées, sous peine d'une sanction financière (**article 33 du RGPD**).

Il est recommandé au dirigeant de mettre en place une **politique d'alerte interne** afin d'avoir connaissance le plus tôt possible de toute violation et de donc de notifier la **CNIL**. Le dirigeant doit prendre connaissance des recommandations édictées par la **CNIL**, aidant les entreprises à la sécurisation des données personnelles. (<https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mettre-en-place-du-teletravail>).





- **Principe de sécurité et de confidentialité**

L'employeur se doit de prendre toutes les mesures nécessaires afin **d'assurer la protection et l'intégrité des données** collectées ou traitées par l'entreprise (données des salariés, clients, fournisseurs), que ce soit sur le matériel fourni ou sur l'équipement personnel du salarié.

Le dirigeant doit mettre en place un **système de sécurité** sur tous les outils informatiques des télétravailleurs tels qu'un pare-feu, antivirus, un logiciel permettant de bloquer les sites malveillants ou encore l'utilisation de VPN.

Un VPN (Virtual Private Network) permet au télétravailleur de connecter son ordinateur portable à distance sur le réseau de l'entreprise via une simple connexion internet. L'emploi d'un VPN permet le chiffrement des connexions et garantit une protection en autorisant seulement un accès à distance aux outils informatiques déjà authentifiés. Cela permet de diminuer les risques de compromission et de fuite de données pouvant provenir de la connexion internet publique ou privée utilisée par le télétravailleur, qui ne présente pas le même niveau de sécurité que le réseau informatique de l'entreprise.

Cependant l'utilisation d'un VPN n'est pas conseillée lorsque le salarié utilise son ordinateur personnel car en se connectant au réseau de l'organisme, il peut mettre en danger la sécurité informatique de sa structure en y introduisant un **virus ou un malware**.

La **CNIL** recommande d'utiliser des outils de communication et de travail collaboratif assurant un niveau de sécurité assez satisfaisant. Ainsi certaines précautions doivent être prises comme la vérification des conditions générales d'utilisation, la garantie de la confidentialité des échanges/données partagés ainsi que leur authenticité, la possibilité de chiffrer les communications, l'interdiction de l'utilisation postérieure des données par le prestataire et l'interdiction du transfert des données vers un pays non européen.

Il est donc conseillé de bien se renseigner avant de télécharger un logiciel sur son ordinateur professionnel et de ne pas seulement s'arrêter au critère de gratuité. En effet comme l'adage le dit si bien, « *si c'est gratuit, c'est que c'est vous le produit* ».

De plus, il est recommandé de ne télécharger que des logiciels nécessaires à l'accomplissement des missions professionnelles et approuvés par la direction.

De ce fait, la **CNIL** recommande de bannir l'utilisation de certains logiciels publics tels que **Zoom**.

Zoom est une application gratuite de visioconférence, qui a connu un boum de téléchargement pendant la crise du Covid-19 (passant de 10 millions à 200 millions d'utilisateurs de Décembre 2019 à Mars 2020). Le succès de ce logiciel américain s'explique du fait, qu'il permet aux utilisateurs, de façon simple et accessible, d'effectuer leurs réunions et conférences professionnelles à distance.

Cependant, ce dernier se retrouve à la Une de nombreux scandales, accusé de ne pas respecter les principes de collecte transparente et de licéité du traitement des données personnelles, mettant en danger la vie privée de ses utilisateurs.

C'est ainsi qu'un article de Motherboard révèle que certains utilisateurs voient leurs données personnelles vendues par Zoom à Facebook, sans leur consentement. Et cela, même si ces derniers ne sont pas membre du réseau social, dans le seul but de leur établir un profil publicitaire.

Un article du journal Le Monde pointe du doigt lui aussi, les pratiques illicites utilisées par Zoom telles que la collecte des données personnelles de l'utilisateur sans son consentement, l'accès par l'application des vidéos échangées car ces dernières ne sont pas chiffrées et les failles de sécurité permettant à des pirates d'accéder aux webcams des internautes.

Malgré l'annonce de mesures prises afin de renforcer la sécurité de l'application comme *le cryptage de bout en bout des communications-vidéos*, ce logiciel présente un danger pour la sécurité de l'entreprise ainsi que pour la vie privée des salariés. Il est donc préférable d'utiliser des logiciels français voir européen qui garantissent la sécurité des données personnelles en accord avec le RGPD. L'ANSSI liste d'ailleurs les logiciels ayant une « certification de sécurité

L'entreprise doit également vérifier le niveau de sécurité des outils de stockage utilisés par le salarié comme le cloud, la clé USB ou bien le disque dur externe.

Il semble impératif pour que le télétravail soit exercé dans les meilleures conditions, que **les principes de confidentialité, d'intégrité des données traités mais aussi d'authentification claire des utilisateurs, soient en amont établis.**



2) Les devoirs du salarié, de nouvelles habitudes à adopter

Le salarié doit lui aussi répondre à certains principes pour une mise en œuvre efficace et sécuritaire du télétravail.

- **Principe de vigilance**

Obligation d'alerte : le salarié se doit d'appliquer les mesures de sécurité prévues par son employeur. En cas d'impossibilité d'application de ces mesures, il est impératif d'alerter immédiatement son supérieur afin de ne pas étendre les risques.

La **coopération et la communication** semble être les piliers d'un télétravail bénéfique. Ainsi le retour d'expérience est très important afin d'informer ses supérieurs sur les points positifs et/ou négatifs, afin que ces derniers améliorent les conditions de travail et le niveau de sécurité.

Obligation de responsabilité : malgré le fait qu'il soit chez lui, le salarié doit respecter la même ligne de conduite qu'en temps normal. Il ne doit pas faire en télétravail ce qu'il ne ferait pas au bureau.

On lui recommande donc d'avoir une utilisation responsable et vigilante des usages et outils informatiques. De plus, avoir une certaine culture cyber est un réel avantage car il permet d'être beaucoup plus vigilant envers toutes tentatives de cyber attaques.

Il faut donc prêter une attention particulière aux e-mails, appels téléphoniques suspects pour éviter d'être victime d'un hameçonnage ou d'un rançongiciel. Il faut surtout avoir le réflexe de demander automatiquement confirmation de la part de l'émetteur en cas de doute.

Exemple : en cas d'e-mail suspect d'un dirigeant demandant au service de comptabilité d'effectuer un virement bancaire d'une somme importante, il est recommandé de demander confirmation au dirigeant en question par téléphone.

Des sauvegardes régulières et externes des données (hébergement externe, cloud, disque dur externe) sont fortement recommandées afin d'éviter de perdre toutes les données en cas de cyberattaques. De même qu'une journalisation des outils informatiques (les serveurs, pare-feu, poste de travail, proxy), dans le but de comprendre l'origine d'une cyberattaque, l'étendue de cette dernière et ainsi pouvoir résoudre le problème afin d'en limiter les impacts et que cela ne se reproduise plus.

Il est conseillé au salarié lorsqu'il imprime des documents chez lui et dans un souci de confidentialité, de les déchirer en plusieurs morceaux avant de les jeter.

En effet il peut y avoir un risque de vol des informations de l'entreprise (un concurrent, dans le but de nuire à l'entreprise, pourrait chercher des informations sur cette dernière dans les poubelles des télétravailleurs).

Il est également important que **le salarié se sente responsable** de l'usage des outils numériques.

*Par exemple, lorsqu'un employé a un comportement déviant envers l'entreprise, il faut que celle-ci ait prévu, dans sa **Charte informatique**, des modalités de contrôles et des sanctions applicables au non-respect de celle-ci.*



- **Principe de sécurité**

Le Groupement d'Intérêt Public luttant contre la cyber-malveillance recommande aux télétravailleurs :

- De s'assurer de **l'utilisation d'un antivirus** : il doit être professionnel pour garantir une protection plus importante car il prévient des principales malveillances professionnelles.
- **D'utiliser des mots de passes forts et complexes** (la plupart des cas de cyberattaques sont dues à l'utilisation de mots de passe trop faibles). Pour chaque site, il est conseillé d'utiliser un mot de passe différent et avec si possible une double identification. De plus, aucune information personnelle susceptible d'être trouvée sur les réseaux sociaux ne doit composer le mot de passe. Le mot de passe ne doit pas non plus être une suite logique et en cas de soupçon il devra être immédiatement changé. L'ANSSI met en place un Guide afin d'obtenir un mot de passe solide. Il est aussi recommandé d'utiliser un gestionnaire de mots de passe et de ne surtout pas tous les noter sur un papier ou sur une note enregistrée dans votre ordinateur/smartphone/tablette. La CNIL propose un outil pour créer rapidement des mots de passe robustes et recommande certains gestionnaires de mots de passe tel que ZenyPass ou Keepass.
- De **sécuriser la connexion WiFi** pour éviter toute faille, de **vérifier sa box internet personnelle** et de s'assurer qu'elle ne soit pas victime d'une cyberattaque avant de se connecter avec son matériel professionnel. Il est ainsi conseillé de **chiffrer le WiFi par une clé WPA2/WPA3** avec un mot de passe long et complexe (Guide de l'ANSSI sur les mots de passe).
- D'utiliser des **protocoles qui garantissent la confidentialité et l'authentification des serveurs destinataires (HTTPS/SFTP)**, d'effectuer des **mise à jour de sécurité régulièrement** et de télécharger uniquement des **logiciels sur des sites officiels**. **L'ANSSI** informe même sur les dernières vulnérabilités des logiciels et des moyens de s'en prémunir à travers son bulletin d'actualité CERT-FR.

Avec le télétravail, l'échange d'informations est beaucoup **plus important** qu'en temps normal, également dans le but de garder ce lien social avec ses collègues. Que ce soit pour le partage de simples documents, de présentations, de tableurs ou bien d'e-mails, le **chiffage des documents est une mesure de sécurité primordiale** mais il est préférable d'utiliser une plateforme sécurisée d'échange de fichiers. Ce cloud d'échange de données, permet au personnel de l'entreprise de s'échanger des informations en toute sécurité, grâce à un processus d'identification rigoureux qui garantit l'authentification de son auteur. Ainsi que grâce au cryptage des données transférées, proposé par les solutions de cloud afin d'éviter tout vol de données. En effet, l'employeur peut décider du niveau de sécurité de la plateforme.

Par exemple, il pourrait imposer l'obligation d'avoir un mot de passe pour ouvrir un dossier envoyé par e-mail, qui aura été préalablement communiqué par SMS ou appel téléphonique.



3) L'utilisation des outils personnels – *Bring Your Own Device .. ou Disaster (BYOD)*

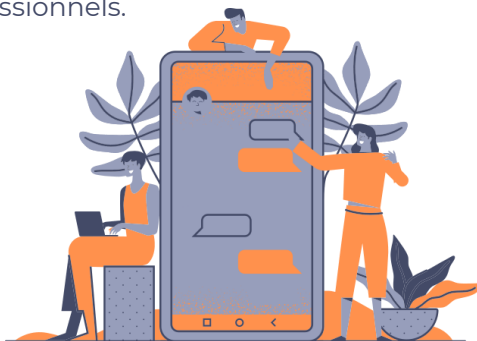
Le principe du ***Bring Your Own Device***, consiste pour le salarié à utiliser son **outil informatique ou téléphonique personnel pour effectuer ses missions professionnelles**. Cette pratique s'est beaucoup développée pendant le confinement, car prises de court, les entreprises n'ont pas pu fournir de matériel informatique adéquat à leurs salariés pour faire du télétravail. Néanmoins des précautions sont à prendre lors de l'utilisation d'un équipement personnel en télétravail.

En effet, les risques sont beaucoup plus importants en matière de cyber malveillance : *une moins bonne maîtrise sur les outils informatiques et le contrôle du respect à la vie privée du salarié qui est plus compliqué (il est essentiel de bien délimiter les deux).*

La **CNIL** édicte des recommandations pour prévenir les risques liés au **BYOD** et conseille notamment une connexion WiFi avec une clé de chiffrement WPA2 WPA3.

Il revient à l'employeur de décider s'il autorise son salarié à utiliser son propre ordinateur ou sa tablette pour travailler (il peut l'interdire).

Ainsi pour que le BYOD ne se transforme pas en *Bring your Own Disaster*, le télétravailleur doit prendre certaines mesures de sécurité en effectuant des mises à jour régulières de son système d'exploitation, des logiciels et des extensions web utilisées. Il lui est conseillé de créer un compte spécialement dédié aux usages professionnels et avec des services limités au strict nécessaire, d'utiliser des mots de passe longs et complexes ayant une double authentification afin de garantir la sécurité des dossiers professionnels.





4) L'adéquation entre télétravail et vie privée

Lorsque le salarié se connecte au réseau de l'entreprise, celui-ci transmet à son employeur diverses données privées telles que sa géolocalisation ou encore ses horaires de connexion. Si l'on croise ces données, elles peuvent permettre d'identifier le salarié en tant que personne physique, retracer son emploi du temps et ses déplacements. Ces données sont donc, même individuellement, des données personnelles.

Par exemple, le dirigeant peut utiliser ces informations dans le seul but d'exercer son pouvoir disciplinaire et dans certains cas, exclure le salarié de potentiels bénéfices.

Le salarié dispose d'un **droit à la déconnexion** qui lui permet de ne pas se connecter aux outils informatiques en dehors du temps de travail :

- Ce droit garantit **le temps de repos du salarié**
- Ce droit régle **la charge de travail du salarié**
- Ce droit **réduit le risque d'épuisement professionnel du salarié**
- Ce droit permet **d'assurer le respect des durées maximales de travail**

Cependant, selon une étude **Eléas** de septembre 2016, *37 % des actifs utilisent leurs outils numériques professionnels en dehors des heures de travail.*

Le **droit à la déconnexion** a été institué par la loi Travail du 8 août 2016, codifié à l'**article L2242-17 du Code du Travail**. Depuis le 1^{er} janvier 2017, ce droit doit être formalisé via un accord collectif ou une charte, après avis du comité social et économique.

L'employeur s'engage également à ne pas contacter le salarié en dehors de la plage horaire établie. Ainsi, le dirigeant a un devoir d'exemplarité et de sensibilisation des différentes strates managériales pour assurer le respect de ce droit.



CHAPITRE 4
LE TÉLÉTRAVAIL, UN ÉCOGESTE POUR
LA PLANÈTE ?



Selon l'étude de l'ADEME *Ecoresponsable au bureau* de Juin 2020, le télétravail permet une réduction des déplacements domicile-travail et de surcroît permet de **diminuer de 30 % les impacts environnementaux de ces déplacements.**

Mettre en place le télétravail s'avère être un point positif pour l'environnement. Il exempte les salariés d'effectuer leurs trajets domicile/entreprise tous les jours, permettant ainsi de réduire notre impact énergétique et d'améliorer la qualité de notre air.

D'après une enquête réalisée par l'**ADEME** (Agence de la transition écologique), **70% des français** vont au travail en voiture. Ainsi **télétravailler 3 jours par semaine permettrait de réduire de 58 % des particules fines** liées au trajet domicile/entreprise.

Notre empreinte carbone réduite est bénéfique à la fois pour la planète mais aussi pour notre portefeuille car la diminution des déplacements en transports (individuels ou collectifs) entraîne une diminution des dépenses en essence ou en ticket de transport.

Le recours au télétravail est aussi un gage pour les entreprises de leur implication dans la préservation de la planète, leur permettant d'obtenir différents labels.



Néanmoins il faut garder à l'esprit que le numérique a des impacts importants sur l'environnement, et selon les experts il serait même **à l'origine d'environ 4 % d'émissions mondiales de gaz à effets de serre**. En effet, les nombreuses recherches internet, appels téléphoniques et connexions pour les visioconférences consomment une grande quantité d'énergie, ce qui crée un risque de saturation des réseaux. Il faut faire donc attention **aux effets rebonds**.

Qui dit télétravail, dit réorganisation de sa vie professionnelle et personnelle, ainsi cela permet à beaucoup de personnes d'effectuer d'autres tâches qu'elles ne pourraient pas faire en étant dans l'entreprise et donc d'effectuer d'autres déplacements. On peut citer par exemple, aller faire des courses ou emmener ses enfants à leurs activités sportives en voiture. Le trajet du travail et l'impact énergétique est ainsi remplacé par les déplacements annexes.

De plus, alors que certains experts considèrent que la consommation individuelle de climatisation ou bien de chauffage contribueraient à l'augmentation de l'empreinte carbone, d'autres plaident plus pour un déplacement de cette même consommation qui auraient lieu dans les locaux de l'entreprise.



Selon une étude réalisée au Royaume-Uni, l'impact énergétique serait beaucoup plus important en hiver du fait de l'augmentation des chauffages utilisés dans les maisons des télétravailleurs, qui consommeraient beaucoup plus que ceux des bureaux anglais. L'augmentation des échanges numériques conduit à une hausse de la pollution numérique.

Il existe néanmoins des solutions afin de réduire les impacts du numérique sur l'environnement notamment *en préférant les partages de données via une plateforme d'échanges de données plutôt que par e-mail, en limitant l'utilisation des vidéos lors de réunions à distance, en privilégiant la connexion Wifi à une connexion 4G, effectuer un ménage dans ses e-mails, dans ses dossiers numériques ou sur son cloud de façon régulière.*

Comme le souligne **WWF** (Fonds mondial pour la nature) dans son livre blanc « numérique et environnement », « *le numérique n'est pas intrinsèquement bon ou mauvais pour l'environnement* ». Ainsi **c'est la façon dont les outils informatiques sont conçus et par la suite utilisés qui va déterminer l'impact positif ou bien négatif sur la planète ainsi que sur notre vie privée.**

La conciliation entre protection éthique des données personnelles et croissance économique plus verte est tout à fait possible et cela mène à une transition à la fois numérique et écologique.

Vous pouvez retrouver l'article d'Oriana Labruyère qui fait le lien entre transition numérique et écologique dans les Décideurs Magazine (Groupe Leaders League): <https://www.magazine-decideurs.com/news/transition-numerique-et-ecologique-naissance-d-une-ecologie-by-design-et-by-default>

Notre mission est donc de mettre en place un télétravail respectueux de l'environnement.





CONCLUSION

Le Télétravail permet d'assurer une plus grande flexibilité de l'emploi et un gain de productivité pour les salariés. Le salarié s'avère être beaucoup plus autonome et responsable. Le télétravail remodèle la relation de travail entre manager et salarié, la notion de hiérarchie physique et de subordination, qui est moins présente. La relation est donc fondée sur le principe de la confiance et de l'autonomie et non plus sur le contrôle. Un contrôle sera certes nécessaire par le biais d'évaluation de performance ou de reporting mais les télétravailleurs développeront par eux même cet auto-contrôle.

Il est sûr qu'à la suite de la crise sanitaire liée au virus Covid-19, le télétravail s'est révélé salvateur que ce soit pour les dirigeants ou pour les salariés. Les avantages ne se sont pas fait attendre comme une meilleure communication permettant une rapidité dans la prise de décisions, une meilleure conciliation entre la vie professionnelle et la vie privée. Cependant certains inconvénients notables sont à prendre en compte tels qu'une pression psychologique plus importante ou une inégalité entre les salariés, concernant l'accès aux outils informatiques ou l'installation du télétravailleur chez lui.

En effet, certaines règles nécessitent d'être définies afin d'encadrer le télétravail pour assurer la protection des salariés et des entreprises.

Les risques de sécurité en termes informatique mais aussi juridique, comme par exemple ceux liés à la protection des données personnelles sont importants. Leurs gestions reposent sur le dirigeant notamment en matière de protection de la vie privée des salariés. Ainsi un cadre légal ou a minima un accord d'entreprise est plus que nécessaire pour que le télétravail se déroule dans les meilleures conditions.

La démocratisation du télétravail est un véritable changement d'habitude que ce soit pour les dirigeants ou les salariés qui doivent s'approprier une nouvelle culture d'hygiène informatique. Tout changement doit être accompagné d'actions de sensibilisation afin que celui-ci soit bénéfique à l'organisation. Cette sensibilisation peut prendre plusieurs formes comme la rédaction de fiches pratiques, la définition de dix règles d'or, la création de podcast de quelques minutes ou encore par la mise en place de jeux à but de formation. A la suite de ces actions de formation, des tests peuvent être réalisés comme par exemple des envois de spams afin de voir le taux de clic sur cet e-mail frauduleux et ajuster le plan de formation en fonction des résultats.

SOURCES

<https://www.service-public.fr/particuliers/vosdroits/F13851>

https://www.entreprises.gouv.fr/files/files/directions_services/cns/ressources/Teletravail_Rapport_du_ministere_de_Mai2012.pdf

<http://www.odoxa.fr/sondage/covid-19-bouleverse-deja-modifiera-durablement-rapport-francais-travail/>

https://dares.travail-emploi.gouv.fr/IMG/pdf/dares_analyses_salaries_teletravail.pdf

http://tnova.fr/system/contents/files/000/002/005/original/Terra-Nova_La-r_volution-du-travail-a-distance_300420.pdf?1588269514

<https://zevillage.net/wp-content/uploads/2019/02/Etude-Teletravail-Malakoff-Mederic-comptoir-Nelle-entreprise-2019.pdf>

<https://zevillage.net/wp-content/uploads/2018/01/Malakoff-Mederic-Ifop-Etude-Teletravail.pdf>

<https://lecomptoirdelanouvelleentreprise.com/le-teletravail-en-2020-et-impact-des-greves-et-des-epidemies/>

<https://empreintehumaine.com/sondage-empreinte-humaine-et-opinion-way-sur-letat-psychologique-des-salaries-francais-apres-5-a-6-semaines-de-confinement-infographie-barometre-t2/>

<http://www.teletravailler.fr/>

<https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques>

<https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mettre-en-place-du-teletravail>

<https://www.cnil.fr/fr/salaries-en-teletravail-quelles-sont-les-bonnes-pratiques-suivre>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf>

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail>

<https://www.institutreindus.fr/wp-content/uploads/2017/11/23-Ouvrage-Chap-15-compress%C3%A9.pdf>

<http://www.inrs.fr/publications/juridique/focus-juridiques/focus-teletravail.html>

<https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/>

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

LES AUTEURS

Le cabinet LABRUYÈRE&CO assiste ses clients face aux enjeux du droit du numérique et notamment de la mise en conformité au RGPD.

Sa fondatrice, **Oriana Labruyère** et son équipe s'attachent à fournir des réponses concrètes aux contraintes opérationnelles et juridiques propres à chaque client.

L'équipe est guidée par cette volonté au quotidien d'avoir une approche concrète, réaliste et opérationnelle.

Maître Oriana Labruyère est titulaire d'un Master de droit international obtenu à l'Université Aix Marseille et est inscrite au barreau de Paris.

Passionnée par les nouvelles technologies, elle se concentre sur toutes les problématiques du droit de l'internet et de la protection des données personnelles.

Avocate de terrain, Oriana Labruyère exerce notamment en tant que DPO externalisé depuis l'entrée en application du RGPD en 2018 et tient le rôle d'interlocuteur privilégié de la CNIL pour plusieurs entreprises françaises et internationales.



LABRUYÈRE & CO
A V O C A T S
D R O I T D U N U M É R I Q U E

Le cabinet RH Progress a été fondé par **Fabien MILLION-BRODAZ**.

Son objectif : accompagner le développement des entreprises en sécurisant leur gestion des ressources humaines.

Les dirigeants d'entreprise savent que de multiples obligations naissent du Code du travail et des conventions collectives. Pourtant peu connaissent les nombreux outils mis à leur disposition afin de surmonter d'éventuelles difficultés.

Fabien MILLION-BRODAZ a exercé des fonctions opérationnelles de direction RH au sein de PME d'au moins 500 salariés.

Proche du terrain, il est l'interlocuteur privilégié des dirigeants d'entreprise face à leurs problématique RH. Il leur apporte 20 ans d'expérience RH en entreprise dont 9 ans de conseil auprès des TPE/PME.



Merci pour votre lecture !
Vous pouvez nous
retrouver sur :

in LABRUYERE&CO

@ www.labruyere.law

in Fabien MILLION-BRODAZ

@ rh-progress.fr