NUMERIQUE

Protection des données personnelles :

Quels droits pour les salariés vis-à-vis de l'employeur ?

Janvier 2020

A retenir :

- Le Règlement général de la protection des données (RGPD) entré en application en mai 2018 vient compléter le code du travail sur ce sujet. Les règles du code du travail continuent à s'appliquer.

- Le RGPD actualise les droits de toute personne à une information sur le traitement de ses données personnelles et à la compréhension de ces traitements. En ce qui concerne les salariés, le RDPD fait porter la responsabilité de ces droits sur l'employeur. Ainsi une non-réponse de l'employeur à l'exercice de droits du salarié quant à la protection de ses données personnelles l'expose à une amende **«** effective, proportionnée et dissuasive » pouvant aller jusqu'à 4% de son chiffre d'affaires.

- Les droits génériques à l'information et à la compréhension sont complétés d'autres droits que nous recensons dans cette fiche, en complément de la Charte CFE-CGC Ethique et Numérique RH. Ils sont au nombre de 8 :
  - Le droit au respect de sa vie privée au travail ;
  - Le droit d'accès au traitement de ses données personnelles ;
  - Le droit à la rectification et à l'effacement de ses données ;
  - Le droit d'opposition à un traitement de ses données ;
  - Le droit à la portabilité de ses données ;
  - Le droit, sous condition, d'être informé d'une violation de ses données
  - Le droit de réclamation auprès de la Commission Nationale Informatique et Liberté (CNIL) ;
  - Le droit à réparation.

- Cette fiche vient compléter la Charte Ethique et Numérique RH réalisée par la CFE-CGC et le Lab RH, présentée en janvier 2018, actualisée en novembre 2018 suite à la relecture par la CNIL. Elle est également le pendant de la fiche « Protection des données personnelles : quelles obligations pour l'employeur vis-à-vis des salariés ? ».

INTRODUCTION

Avec l'entrée en application du depuis mai 2018, le cadre français de la protection des données personnelles au travail a été renforcé. La loi Informatique et Liberté du 6 janvier 1978 ainsi que **le Code du travail** prescrivaient déjà des règles de protection dans l'utilisation des données personnelles des salariés sur leur lieu de travail ou dans le cadre de leur contrat de travail. Le RGPD vient compléter ce cadre. Ainsi, en matière de RH et de contrôle du travail, la protection des données est à la fois prévue par le code du travail et le RGPD.

Le grand changement apporté par le RGPD au regard de loi Informatique et Liberté de 1978 est la **responsabilisation** de l'employeur dans le traitement des données personnelles des salariés et donc son implication dans le respect des droits à l'information et à la compréhension des traitements des données personnelles des salariés. Ainsi, sa non réponse à une demande d'exercice des droits d'un salarié selon les modalités prévues par le RGPD, expose l'employeur à une amende **« effective, proportionnée et dissuasive »** pouvant aller jusqu'à 4% de son chiffre d'affaires.
Les différents droits décrits ci-après découlent directement **du droit fondamental que détient chaque individu quant à la protection de ses données personnelles**.

Ces principaux droits sont au nombre de 8 :

- Le droit au respect de sa vie privée au travail ;
- Le droit d'accès au traitement de ses données personnelles ;
- Le droit à la rectification et à l'effacement de ses données ;
- Le droit d'opposition à un traitement de ses données ;
- Le droit à la portabilité de ses données ;
- Le droit, sous condition, d'être informé en cas de violation de ses données ;
- Le droit de réclamation auprès de la Commission Nationale Informatique et Liberté (CNIL) ;
- Le droit à réparation.

Comme pour le droit du travail, les représentants du personnel et syndicaux doivent veiller à sa bonne application.

LE DROIT AU RESPECT DE SA VIE PRIVEE AU TRAVAIL

Les outils numériques permettent une traçabilité de plus en plus fine. Ils peuvent permettre à l'employeur de renforcer son contrôle, sa surveillance à l'égard des salariés.

Parallèlement, apparaît une porosité de plus en plus grande entre la vie personnelle et la vie professionnelles liée aux outils du numérique. Ex : télétravail. Dans ce contexte, il est de plus en plus difficile de circonscrire des contrôles sur le temps de travail des salariés.

Cependant, la vie privée doit être préservée le plus possible. Elle ne doit pas être sacrifiée sur l'autel de la technologie ou de la pratique !

Il s'agit de concilier deux droits fondamentaux : le droit au respect de la vie privée[1] et le pouvoir de direction de l'employeur qui découle du droit de propriété et du lien de subordination[2].

Le droit du travail et le droit de la protection des données personnelles permettent la cet équilibre entre le respect de la vie privée et le pouvoir de l'employeur. Et les différents droits apportés par le RGPD au salarié dans l'entreprise doivent être lus au regard des dispositions du code du travail.

Le secret des correspondances

Le principe de la protection

Ce principe pour les salariés a été posée par les juges de la Cour de cassation :

Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée. Ce respect implique en particulier le secret des correspondances. L'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur[3].

Ainsi, les courriers personnels et la correspondance privée du salarié reçus ou émis dans le cadre du travail sont protégés. Cela signifie :

- Que l'employeur ne peut être en copie automatique des messages reçus par le salarié ;
- Que l'employeur ne peut pas librement consulter les courriels personnels de ses salariés employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles ;

[1] Article 9 du code civil ; article 8 de la CEDH

[2] Article L.1121-1 du code du travail : nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

[3] cass.soc 2 octobre 2001 Arrêt Nikon

- qu'il ne peut se servir de ces messages privés pour exercer son pouvoir de direction (demande de justification, sanction, preuve…).

La protection s'étend au cas où la messagerie personnelle serait ouverte sur un ordinateur professionnel : l'employeur ne peut y accéder sans atteinte à vie privée et atteinte au secret de la correspondance.

Les conditions de la protection : mention « personnel » ou « privé »

Pour qu'ils soient protégés, les messages personnels doivent être identifiés expressément comme tels. Ils doivent mentionner dans leur objet « Personnel » ou « Privé » par exemple, et être stockés dans un répertoire intitulé « Personnel » ou « Privé ».

Si cette mention n'apparaît pas, les messages reçus et émis dans le cadre de l'exécution du contrat de travail (sur le temps de travail, avec un outil professionnel, en lien avec le travail) sont présumés professionnels !

Autrement dit, tout message reçu et émis d'un outil professionnel est présumé professionnel, sauf s'il mentionne expressément dans on objet qu'il est personnel ou privé.

Ainsi, est qualifié de message professionnel, les messages envoyés à partir d'un ordinateur personnel avec une adresse électronique personnelle vers un ordi professionnel, sauf s'il est signalé comme un message personnel !

Cela signifie que l'employeur :

- peut consulter, en dehors de la présence du salarié et sans l'avertir préalablement, tous les messages reçus et émis dans une boîte électronique professionnelle ;
- utiliser l'existence et le contenu des messages dans le cadre de son pouvoir de direction.

L'application concrète aux messages électroniques et téléphoniques

Cas de suivi des communications électroniques personnelles d'un salarié au travail : la mise en place, par l'employeur, d'une surveillance des correspondances et des communications des salariés dans le cadre du travail doit s'accompagner de garanties suffisantes contre les abus : information claire et préalable des salariés sur la nature de la surveillance, distinction entre suivi du flux des messages et contenu des communications, proportionnalité dans le suivi au but recherché (preuve de recherche de moyens moins intrusifs)[4].

Cas des sms lus par l'employeur sur téléphone professionnel : les sms envoyés et reçus depuis un portable professionnel sont présumés professionnels sauf s'ils sont signalés comme personnels[5].

[4] arrêt CEDH 5 septembre 2017
[5] cass.soc. 10 février 2015

Cas de la messagerie instantanée au travail : le message est présumé professionnel mais le contenu peut exiger respect de la correspondance. En l'espèce, la messagerie instantanée a été considérée comme relevant du domaine privé et donc bénéficiant du secret des correspondances sur un seul motif : l'adresse mail associée au compte de messagerie instantanée était une adresse personnelle. De ce seul fait, les échanges relevaient du domaine privé[6].

Cas de l'accès à la messagerie professionnelle pendant une absence pour arrêt maladie : l'employeur peut accéder aux courriels provenant de la messagerie électronique professionnelle du salarié pendant son arrêt maladie et les utiliser à des fins de sanction à la condition que ces derniers aient bien un caractère professionnel et que leur contenu ne relève pas de la vie privée du salarié[7].

La protection de la vie privée dans le cadre de la géolocalisation

La géolocalisation est jugée comme atteinte disproportionnée aux droits des salariés, lorsque ces derniers ne peuvent désactiver le boitier de suivi[8].

L'utilisation d'un tel moyen de contrôle de la durée du travail n'est licite que si ce contrôle ne peut être opéré par un autre moyen, fût-il moins efficace[9].

La protection de la vie privée dans le cadre de la vidéo-surveillance

La caméra, parfois accompagné d'un enregistrement de son, sur le lieu de travail est un enjeu pour la protection des données personnelles (image, voix) car tout lieu de travail comporte dans la pratique des caméras de surveillance pour sécuriser les locaux.

Le placement sous surveillance permanente des salariés à des fins de localisation est attentatoire à leur vie privée et viole les prescriptions du RGPD. C'est ce que rappelle la CNIL au sujet d'un dispositif qui filme en permanence un poste de travail avec un accès aux données ouvert à tout le personnel sans chiffrement permettant d'en assurer la sécurité[10].

La CEDH a également dû se prononcer sur le cas d'un filmage des cours en amphithéâtre de professeurs d'université. Au regard des conditions d'installation et d'utilisation de la vidéo-surveillance, il y a une atteinte à la vie privée quand bien même on est sur un lieu de travail[11].

---

[6] cass.soc. 23 octobre 2019
[7] cass.soc. 3 avril 2019
[8] cass.soc. 25 janvier 2016
[9] cass.soc. 19 décembre 2018
[10] Communiqué CNIL 10 décembre 2019
[11] Arrêt CEDH 28 novembre 2017

LE DROIT D'ACCES AUX DONNEES COLLECTEES ET TRAITEES[12]

Tout salarié est en droit de demander à son employeur la liste de l'ensemble des données le concernant qui ont été collectées. Le droit d'accès comprend 2 aspects :

- un droit à interrogation : toute personne peut interroger le responsable de traitement en vue d'obtenir une confirmation que des données personnelles la concernant font ou ne font l'objet de traitement ;
- un droit à la communication de ses données personnelles traitées.

Quels sont les éléments concernés par le droit d'accès du salarié ?

Symétrie de l'obligation faite à l'employeur d'informer le salarié[13], outre les données personnelles concernant le salarié, l'employeur devra lui communiquer les éléments suivants :

- La source des données personnelles lorsque celles-ci n'ont pas été recueillies directement ;
- La finalité des traitements pour lesquelles il utilise les données personnelles ;
- Les destinataires qui ont pu accéder aux données ;
- Les catégories de données collectées ;
- La base juridique du traitement, sans laquelle un traitement ne peut être licite (recueil du consentement, intérêt légitime du responsable de traitement, exécution du contrat de travail, obligation légale). Dans le cas où le fondement du traitement repose sur un intérêt légitime, l'employeur doit le faire connaître ;
- La durée de conservation des données personnelles (à défaut les critères utilisés pour la déterminer) ;
- L'existence d'une prise de décision automatisée, y compris en cas de profilage, et la logique sous-jacente, l'importance et les conséquences pour le candidat à un poste ou le salarié d'une telle décision,
- L'éventuel transfert des données vers un pays tiers (non-membre de l'UE) ou vers une organisation internationale.

Concernant plus spécifiquement les données RH, la CNIL recense notamment les thématiques suivantes :

- Le recrutement ;
- L'historique de carrière ;
- L'évaluation des compétences professionnelles (entretiens annuels d'évaluation, notation) ;
- Les demandes de formation et les éventuelles évaluations de celles-ci ;
- Le dossier disciplinaire ;
- L'utilisation du badge de contrôle d'accès aux locaux ou d'utilisation d'outils d'impression ;
- Les données issues d'un dispositif de géolocalisation ;

[12] Article 15 du RGPD

[13] Cf. la Fiche « Protection des données : les obligations de l'employeur vis-à-vis des salariés »

- Tout élément ayant servi à prendre une décision à l'égard du salarié (une promotion, une augmentation, un changement d'affectation, etc.). Il peut s'agir des valeurs de classement annuel, parfois appelées « *ranking* », ou de potentiel de carrière.

Quelles sont les modalités d'accès aux données ?

La demande du salarié

Le droit d'accès est un droit discrétionnaire : le salarié n'a pas à justifier d'un motif. Pour exercer son droit d'accès, il convient de prouver son identité (photocopie de la CNI), et d'exprimer sa demande soit sur place (contre remise d'un avis daté et signé si celui-ci ne peut être satisfait immédiatement), ou sinon par écrit, y compris voie électronique.

La CNIL propose sur son site des modèles de courrier personnalisables et prêt à être envoyé à son employeur.

La transmission des données par l'employeur

Il doit faciliter l'exercice des droits des salariés. Il doit communiquer les données à caractère personnel et les informations associées « sous une forme accessible » (les codes, sigles et abréviations figurant dans les documents communiqués doivent être explicités, si nécessaire à l'aide d'un lexique ou d'icônes normalisées), et ce gratuitement (sauf cas de « demandes infondées ou excessives », telles des demandes répétitives, où le paiement ne pouvant excéder le coût de reproduction pourra être exigé).

L'employeur est tenu de répondre dans un délai d'un mois à compter de la réception de la demande. Ce délai peut être rallonger de deux mois supplémentaires, à condition d'avoir dans le premier délai d'un mois, informé le salarié de cette prorogation. En cas de non réponse ou de non-respect de la procédure, le salarié pourra exercer son droit de réclamation auprès de la CNIL.

LE DROIT A LA RECTIFICATION ET A L'EFFACEMENT[14]

Le droit à la rectification permet au salarié de pouvoir rectifier, compléter, actualiser des informations le concernant. Ce droit s'exerce pour corriger des erreurs, des inexactitudes. Dans cette hypothèse, il appartiendra l'employeur de veiller à ce que ce que l'ensemble des systèmes de traitement contenant la donnée obsolète ou erronée soit corrigée ou supprimée.

[14] Article 16 et 17 du RGPD

La CNIL propose un modèle de courrier personnalisable permettant d'exercer ce droit à la rectification.

Lorsque le salarié constate l'utilisation, la communication ou la conservation de données le concernant qui sont interdites, il peut exercer son droit à l'effacement. Celui-ci permet à la personne concernée, sous certaines conditions, d'obtenir l'effacement de données personnelles la concernant, la cessation de la diffusion de ces données ainsi que l'effacement par des tiers des liens vers ces données ou de toute copie ou reproduction de celles-ci. C'est par exemple le cas de données liées à une sanction conservées au-delà des délais requis ou des données utilisées à d'autres finalités que ce que la loi autorise.

Attention

Le RGPD prévoit un droit à l'effacement qui n'est pas un droit total et général à l'oubli. Le droit à l'effacement permet de rendre les données concernées inaccessibles. Mais elles ne disparaissent pas totalement en tant que telles. Le droit à une « amnésié générale » n'existe pas encore.

LE DROIT D'OPPOSITION A UN TRAITEMENT DE SES DONNEES[15]

Le droit d'opposition permet au salarié de s'opposer, pour des motifs légitimes, à ce que ses données à caractère personnel fassent l'objet d'un traitement, y compris lorsqu'il s'agit d'un profilage, qui lui serait désavantageux.

Cette demande est recevable sauf si l'employeur démontre que le traitement qu'il effectue répond à un des critères de licéité de traitement prévu dans le cadre du RGPD :

- il existe des motifs légitimes et impérieux à traiter les données, ou celles-ci sont nécessaires à la constatation, l'exercice ou la défense de droits en justice ;
- Il répond à une clause contractuelle ;
- Il répond à une obligation légale ;
- Il a reçu initialement le consentement du salarié ;
- Il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

A titre d'exemple, un salarié peut s'opposer à l'installation d'un dispositif de géolocalisation dans son véhicule professionnel, dès lors que ce dispositif ne respecte pas les conditions légales posées par la CNIL ou d'autres textes : information préalable des salariés de la mise en place du dispositif et du fonctionnement du dispositif, accès aux données les concernant enregistrées par l'outil (dates et heures de circulation, trajets effectués, etc.), possibilité de désactivation de la collecte ou la transmission de la localisation géographique en dehors du temps de travail.

[15] Article 21 du RGPD

Pour exercer son droit d'opposition, le salarié doit demander la suppression de la donnée personnelle et l'employeur dispose alors d'un mois pour répondre. En cas de non-réponse ou de réponse non satisfaisante, le salarié peut saisir la CNIL (voir la partie « droit d'introduire une réclamation devant la CNIL »).

LE DROIT A LA PORTABILITE DE SES DONNEES[16]

Les salariés peuvent demander à recevoir leurs données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine. Ils peuvent ainsi les stocker ou les transmettre en vue de leur réutilisation à des fins personnelles.

Dans le cadre des données personnelles au travail, seules celles dont le traitement est fondé sur le consentement du salarié (les données fournies volontairement par le salarié), ou les données traitées par procédé automatisé basé sur le consentement du salarié ou l'exécution du contrat de travail, sont concernées par le droit à la portabilité. Les données des salariés traitées sur la base d'un intérêt légitime ou d'obligations légales, ne sont pas concernées par le droit à la portabilité.

Le droit à la portabilité ne doit pas porter atteinte aux droits et libertés de tiers.

Ce droit s'exerce auprès de l'employeur qui dispose d'un délai d'un mois pour répondre à compter de la réception de la demande. En cas de demandes complexes, ce délai pourra être allongé à trois mois.

Attention

Ce droit à la portabilité est plus restrictif (cf. périmètre ci-dessus) que le droit d'accès qui concerne toutes les données du salarié.

LE DROIT SOUS CONDITION D'ETRE INFORME EN CAS VIOLATION DES DONNEES A CARACTERE PERSONNEL DES SALARIES[17]

En cas de constatation de violation des données à caractère personnel des salariés susceptible d'engendrer un risque élevé pour leurs droits et libertés, ils doivent être prévenus à moins que l'employeur ait pris des mesures permettant l'impossibilité d'exploitation des données (par un chiffrement par exemple) ou permettant la non-réalisation du risque élevé d'atteinte aux droits et libertés.

[16] Article 20 du RGPD
[17] Articles 33 et 34 du RGPD

Le plus syndical

Comme nous l'indiquons dans la charte Ethique et Numérique RH, la formation des salariés permet d'acquérir une « culture de la donnée » mais également d'être sensibilisés aux enjeux de sécurité, à l'heure où les cyberattaques touchent de plus en plus d'entreprises. Cette formation peut être mise en place au titre de l'adaptation des salariés à l'évolution du poste de travail et à la veille au maintien de leurs capacités à occuper un emploi au regard des évolutions des technologies et des organisations, au regard des compétences numériques requises[18].

LE DROIT D'INTRODUIRE UNE RECLAMATION AUPRES DE LA CNIL[19]

Un salarié qui ne parvient pas à exercer ses droits « Informatiques et Liberté », ou qui souhaite signaler une violation aux règles de protection des données personnelles (exemple : un système de vidéosurveillance installée sans information préalable des salariés) peut introduire une réclamation auprès de la CNIL.

Cette réclamation s'effectue en ligne sur l'espace dédié aux plaintes concernant le travail. La CNIL a classé par grands thèmes les différents motifs de plaintes :

- Le dossier professionnel,
- La vidéosurveillance,
- La géolocalisation (Téléphone et GPS Voiture),
- L'accès aux locaux,
- Les autres cas (les outils informatiques par exemple).

Le plus syndical

L'ensemble de ces sujets, sont traités en détail dans la fiche Travail et données personnelles de la CNIL, qui précise pour chacun des cas, la doctrine de la CNIL sur ces sujets de recrutement et de gestion du personnel, de géolocalisation, d'utilisation d'outils informatiques au travail, d'accès aux locaux et de contrôle des horaires, de vidéosurveillance au travail, d'écoute et d'enregistrement téléphonique.

Avant tout dépôt d'une plainte, nous conseillons de :

- bien lire les documents CFE-CGC (Charte Ethique Numérique RH, fiches complémentaires sur le RGPD) et la fiche de la CNIL dédiée aux données RH,

- de rencontrer le délégué à la protection des données (DPD/DPO) désigné par l'entreprise pour se faire expliquer les différents traitements possibles et pratiqués dans l'entreprise et

[18] Article L. 6321-1 du code du travail
[19] Article 77 du RGPD

reboucler ces informations avec les éléments d'information communiqués par l'employeur aux salariés et aux représentants du personnel,

- réunir les éléments du dossier montrant un non-respect des droits du salariés, comme par exemple, la copie de la lettre adressée à l'employeur et restée sans réponse depuis plus d'un mois. Ces éléments attestent d'un problème et vont aider la CNIL à bien évaluer la situation.

Ne pas oublier l'existence du droit d'alerte de la délégation des membres du CSE : si un délégué constate, notamment par l'intermédiaire d'un salarié, qu'il existe une atteinte aux droits des personnes ou aux libertés individuelles dans l'entreprise qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché, il en saisit immédiatement l'employeur[20].

LE DROIT A REPARATION[21]

Un salarié qui aurait subi un dommage matériel ou moral du fait d'une violation du RGPD a le droit d'obtenir de son employeur ou du sous-traitant réparation du préjudice subi.

Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant la CNIL (reconnue par le Conseil d'Etat comme une autorité administrative indépendante). Par ailleurs, la loi ajoute que : « tout citoyen peut également porter plainte directement auprès du procureur de la République ou par un service de police ou de gendarmerie en vue de faire condamner pénalement le non-respect par les responsables de fichiers de ses droits »[22].

[20] Articles L.2312-5 et L.2312-59 du code du travail
[21] Article 82 du RGPD
[22] Récapitulatif CNIL des sanctions pénales