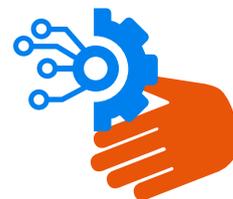




# TRAVAIL & NUMÉRIQUE



AGISSONS POUR DES TECHNOLOGIES

AU SERVICE DE L'HUMAIN

S'ENGAGER POUR CHACUN  
AGIR POUR TOUS

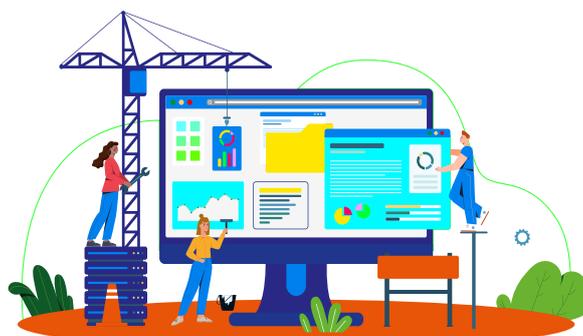
## TABLEAU DE BORD DES LEVIERS RÉGLEMENTAIRES ET DES OUTILS JURIDIQUES À MOBILISER SUR LE NUMÉRIQUE ET LES SIA\* DANS LE SECTEUR PRIVÉ

Le déploiement des outils numériques et des systèmes d'intelligence artificielle (SIA) sur les lieux de travail est trop rarement discuté dans les différents espaces de dialogue social malgré l'existence de nombreux leviers réglementaires et outils juridiques.

Ce tableau de bord à destination des militants du privé cartographie les différentes « portes d'entrée » mobilisables qui se complètent pour agir sur le déploiement des outils numériques dans le travail.

Il est organisé en 5 parties :

1. DIALOGUE SOCIAL ET DROITS EN TANT QU'ÉLUS DU CSE .....	2
2. PROTECTION DES DONNÉES PERSONNELLES .....	8
3. SANTÉ ET SÉCURITÉ .....	13
4. DISPOSITIFS DE SURVEILLANCE DES TRAVAILLEURS .....	14
5. RÈGLES EN COURS DE CONSTRUCTION OU PAS ENCORE APPLICABLES .....	15
Ressources complémentaires .....	16



\* SIA: systèmes d'intelligence artificielle.





# 1. DIALOGUE SOCIAL ET DROITS EN TANT QU'ÉLUS DU CSE

## Consultations récurrentes (article L. 2312-17 Code du travail) :

Le comité social et économique est obligatoirement consulté sur :

- les orientations stratégiques de l'entreprise;
- la situation économique et financière de l'entreprise;
- la politique sociale de l'entreprise, les conditions de travail et l'emploi.

Les consultations récurrentes permettent de recourir à un expert intégralement pris en charge par l'employeur sauf concernant la consultation sur les orientations stratégiques qui n'est prise en charge qu'à hauteur de 80 % par l'employeur et doit être imputée sur le budget de fonctionnement pour le reste, sauf exceptions (art. L. 2315-80 C. trav.)

### Chacune de ces 3 consultations est l'occasion d'aborder la question de l'usage et du déploiement des outils numériques et des SIA :

- **La consultation sur les orientations stratégiques** est un bon moment pour aborder, en anticipation (et en complément des informations-consultations ponctuelles) la stratégie de l'entreprise concernant l'usage des outils numériques et des SIA et sa cohérence avec d'autres objectifs, notamment en matière de Responsabilité sociale et environnementale (RSE);
- **La consultation sur la situation économique et financière** doit permettre d'interroger la politique d'investissement et de R&D ainsi que d'aborder la question des impacts (positifs ou négatifs) des outils numériques et des SIA (ex: comment sont ou seront répartis les gains de productivité estimés);
- Enfin, **la consultation sur la politique sociale** doit permettre d'aborder les impacts sur le travail et l'emploi. Quelles évolutions des activités avec les outils numériques et les SIA ? Quelles évolutions de l'emploi et des compétences ? Quelles mesures d'anticipation ? La question des risques discriminatoires du fait de l'usage d'un système algorithmique est-elle abordée dans un but préventif ?

À noter que depuis la loi Climat et résilience (n° 2021-1104 du 22 août 2021 portant sur la lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets), lors de ces consultations, le CSE doit être « *informé des conséquences environnementales de l'activité de l'entreprise* ». Ainsi, la stratégie de l'entreprise en matière d'utilisation de l'IA et des outils numériques doit faire l'objet d'une information du CSE sous l'angle de son impact environnemental. Par ailleurs, à compter de janvier 2025, certaines entreprises (grossièrement celles qui étaient soumises à la DPEF) devront consulter le CSE sur les informations en matière de durabilité, en application de la directive CSRD transposée en droit français par l'ordonnance du 6 décembre 2023.

**Pour plus d'information** sur les opportunités qu'offrent ces consultations, voir la [Fiche pratique: Comment interroger la stratégie numérique de mon entreprise?](#)



## Consultations ponctuelles

Le CSE est obligatoirement informé et consulté sur :

### L'introduction d'une nouvelle technologie

En amont de l'introduction d'une nouvelle technologie ou d'un aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail (art. L. 2312-8, II, 4° C. trav.).

En vue de cette consultation, le **CSE peut décider de désigner un expert externe pour évaluer les outils et SIA proposés et leurs impacts potentiels**, mais l'expertise devra être financée sur son budget de fonctionnement car elle ne fait pas partie des expertises prises en charge par l'employeur (art. L. 2315-94 et L.2315-80 C. trav.).

À cette occasion, le CSE doit être informé et consulté sur «*les conséquences environnementales*» de l'introduction de la nouvelle technologie de l'aménagement important des conditions de travail qu'elle induit.

#### **À partir de quand considère-t-on que l'employeur a introduit une nouvelle technologie nécessitant la consultation du CSE et ouvrant droit à expertise ?**

Il faut démontrer le caractère nouveau de la technologie en question ou l'importance de l'aménagement des conditions de travail que cela peut engendrer, ce qui n'est pas toujours simple.

Prenons l'introduction d'un logiciel de tri et de réponse automatique aux courriers simples.

En 2018, la Cour de cassation a considéré que cette introduction n'ouvrait pas le droit à consultation et expertise car, selon les juges, ce logiciel n'avait pas d'incidence négative sur les conditions de travail des salariés et que le caractère "important" de l'aménagement n'était pas démontré...

Toutefois, dans une autre affaire, les juges ont retenu le droit de désigner un expert en vue de la consultation en se basant sur les éléments suivants :

- le caractère nouveau de l'application ;
- la difficulté à appréhender les conséquences de l'application à moyen long terme.

La décision souligne en effet que «*si le chargé de clientèle reste en l'état l'interlocuteur du client appelé à valider chacune des propositions faites par le logiciel présenté comme une aide, l'outil, qui a la particularité de s'enrichir de manière continue des informations et questions transmises par le salarié et des retours sur expérience pour améliorer la pertinence de ses réponses à des questions récurrentes, va être en mesure, progressivement, de réaliser un certain nombre de tâches (...); cela aura donc nécessairement une incidence sur le contenu, l'organisation et la qualification du travail du chargé de clientèle et des fonctions support*». (TGI Paris, référé, 3 nov. 2016, n° 16/58942).

Quoiqu'il en soit, concernant les logiciels, la Cour de cassation a imposé la consultation du CSE dès lors que leur introduction impliquait la formation des salariés ou changeait substantiellement leurs habitudes de travail.

Plus récemment, il a été jugé que l'IA, par son caractère novateur, doit permettre la désignation d'un expert en vue d'étudier les répercussions potentielles de cette introduction dans l'entreprise (TJ Pontoise, 15 avril 2022, n° 22/00134)



## Les conséquences de l'usage de l'outil numérique

Lorsque l'usage d'un outil a des conséquences sur la structure ou le volume des effectifs, l'organisation économique et juridique de l'entreprise, les conditions de travail, d'emploi (art. L. 2312-8, 1° à 3° C. trav.).

Par exemple, si un SIA conduit à des licenciements, des plans de départs volontaires ou l'engagement de formations importantes entraînant le changement de catégorie professionnelle des salariés ou encore si l'usage d'un SIA conduit à la fermeture d'une filiale dans un groupe...

Le CSE devra là encore être informé et consulté sur les conséquences environnementales de la réduction ou du changement de structure des effectifs. Par exemple, le fait d'utiliser un logiciel de tri du courrier a-t-il un impact environnemental plus ou moins important que l'organisation du travail antérieure (qui supposait l'emploi d'un être humain)?

## La mise à jour du règlement intérieur ou charte informatique

Lors de la **mise à jour du règlement intérieur ou de la charte informatique de l'entreprise** (article L1321-1 C.trav.).

C'est l'employeur qui décide de mettre ou non à jour ces documents, s'ils existent, lors de l'introduction ou de la modification de la technologie. S'il procède à la mise à jour, alors il devra consulter le CSE.

## Les dispositifs de contrôle

**Sur les dispositifs de contrôle des salariés** (L.2312-38 C. trav. dernier alinéa; voir page 14 - [4. Dispositifs de contrôle et de surveillance des travailleurs](#))

## Informations ponctuelles

Le CSE est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci (art. L. 2312-38 C. trav.).

Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.

Par exemple si la gestion des RH se dote d'un logiciel de tri automatique des CV, le CSE doit en être informé.

## Ajouter un point à l'ordre du jour et/ou demander une réunion spécifique

**Dans les entreprises d'au moins 50 salariés**, les membres du CSE peuvent demander l'ajout d'un **point non prévu à l'ordre du jour par l'intermédiaire du secrétaire du CSE**. En effet, en principe l'ordre du jour est élaboré conjointement par le secrétaire du CSE et son président, c'est-à-dire l'employeur ou son représentant (art. L. 2315-29 C. trav., alinéa 1<sup>er</sup>). Attention toutefois car l'ordre du jour doit être communiqué au moins 3 jours avant!



Par ailleurs, **outre les consultations prévues par le Code du travail et la réunion mensuelle, le CSE se réunit :**

- **à la demande de la majorité de ses membres.** Dans ce cas, les questions jointes à la demande de réunion doivent nécessairement être inscrites à l'ordre du jour (art. L. 2315-28 et L.2315-31 C. trav.);
- **« à la suite de tout accident ayant entraîné ou ayant pu entraîner des conséquences graves, ainsi qu'en cas d'événement grave lié à l'activité de l'entreprise, ayant porté atteinte ou ayant pu porter atteinte à la santé publique ou à l'environnement ou à la demande motivée de deux de ses membres représentants du personnel, sur les sujets relevant de la santé, de la sécurité ou des conditions de travail ».** (art. L. 2315-27 C. trav.).

**Dans les entreprises de moins de 50 salariés, les membres du CSE sont reçus en cas d'urgence à leur demande** (art. L. 2315-21 C. trav.). Sauf cas exceptionnels, ils doivent présenter leurs demandes dans une note écrite au moins 2 jours avant d'être reçus (art. L. 2315-22 C. trav.).

## **La Base de données économique, sociale et environnementale (BDESE)**

La BDESE rassemble les informations (ou données) sur les grandes orientations économiques et sociales de l'entreprise et constitue donc une source d'information importante pour les travailleurs et leurs représentants. Elle comprend des informations obligatoires qui varient selon l'effectif de l'entreprise.

**Il est également possible de négocier les informations devant figurer dans la BDESE afin de les adapter aux caractéristiques de l'entreprise. Dans ce cas, il est utile de prévoir une clause de revoyure pour adapter les informations car les informations pertinentes peuvent évoluer avec le temps.**

**Dans les entreprises d'au moins 300 salariés,** la BDESE elle doit contenir de nombreuses informations, dont des informations concernant **l'organisation du travail et les dépenses d'amélioration des conditions de travail, mais aussi des informations en matière d'emplois, de répartition par catégories professionnelles, la formation, l'évolution des effectifs, les conséquences environnementales de l'activité...** (art. R.2312-9).

**Pour les entreprises de moins de 300 salariés,** les exigences sont relativement similaires : la BDESE doit notamment contenir les mesures envisagées en ce qui concerne l'amélioration, le renouvellement ou la transformation des méthodes de production et d'exploitation ; et les incidences de ces mesures sur les conditions de travail et l'emploi (art. R.2312-8).

Dans les deux cas, elle doit également contenir les informations relatives aux investissements matériels et immatériels en particulier les dépenses de recherche et développement.

## **Concrètement, quels documents peut-on trouver ou négocier l'intégration à la BDESE ?**

- Le Document d'évaluation des risques psycho-sociaux (DUERP).
- Le Programme annuel de Prévention des risques professionnels et d'amélioration des conditions de travail (PAPRI Pact).
- Un registre de l'outil pour chaque système algorithmique utilisé (cf. [Fiche pratique: Comment agir lors du déploiement d'un outil numérique ?](#) et [Registre des outils numériques et des SIA](#)).
- Le rapport RSE.
- Le rapport de durabilité exigible pour certaines entreprises à partir de 2025 (Ord. n°2023-1142 du 6 déc. 2023.).



S'il s'avère que la direction refuse de communiquer des informations pertinentes lors des consultations sur la stratégie de l'entreprise ou lors du déploiement d'un système algorithmique, vous pouvez vous rapprocher d'un avocat du réseau Avec pour discuter des actions possibles à engager.

### Droit d'alerte des élus

En cas d'atteinte aux droits et libertés des personnes qui n'est pas justifiée par la nature de la tâche à accomplir, ni proportionnée au but recherché, un élu peut exercer son droit d'alerte pour en avertir immédiatement l'employeur (art. L. 2312-59 C. trav.). Les algorithmes peuvent en effet générer des biais et des discriminations ou devenir trop intrusifs. On peut penser, par exemple, à un système de recrutement ou d'allocation des primes fonctionnant avec des SIA qui discriminerait certaines personnes. Une telle alerte peut également s'effectuer en cas de danger grave et imminent (art. L. 2312-60 C. trav.).

Cette alerte oblige l'employeur à procéder à une enquête, pour ensuite que celui-ci prenne les mesures propres à faire cesser l'atteinte.

Dans le cas où un employeur ne respecterait pas cette obligation, la saisine du Défenseur des droits est également possible en ligne au lien suivant : [Demande au Défenseur des droits ?](#)

La loi française sur le devoir de vigilance impose aux **sociétés employant au moins 5 000 salariés en France** (directement ou au sein de leurs filiales) **ou 10 000 salariés dans le monde** (selon les mêmes conditions) d'identifier et de prévenir les risques d'atteintes graves aux droits humains et aux libertés fondamentales, à la santé, à la sécurité des personnes, ainsi qu'à l'environnement résultant de ses activités et de celles de ses partenaires dans la chaîne de valeur (filiales, mais aussi sous-traitants, fournisseurs...). À cette fin, ces sociétés doivent élaborer **un plan de vigilance, en association avec les parties prenantes**. Celui-ci doit prévoir un mécanisme d'alerte et de recueil des signalements relatifs à l'existence ou à la réalisation des risques, établi en concertation avec les organisations syndicales représentatives dans la société.

### Le CSE doit procéder à des inspections régulières (art. L. 2312-13 Code du travail)

En matière de santé, de sécurité et des conditions de travail, ce qui peut trouver un intérêt en matière d'usage de outils numériques et des SIA.

Il réalise également des enquêtes en matière d'accident du travail ou de maladies professionnelles.

### Modification du règlement intérieur (ou la charte informatique)

L'introduction d'un SIA passe également par la mise à jour du règlement intérieur (ou de la charte informatique). En cas de modification du règlement intérieur, l'avis du CSE doit être sollicité (L. 1321-1 C. trav.).



## Création d'une commission spécialisée (art. L. 2315-45 du C. du travail)

Les élus CSE peuvent proposer la création d'une commission spécialisée au sein du CSE dédiée à l'évaluation et au suivi des outils numériques et des SIA. Cette commission peut inclure des experts en technologie et en droit du travail et assurer le suivi des accords signés sur le sujet.

## Consultation des salariés (art. L. 2312-13 du C. du travail)

Les élus CSE peuvent organiser des consultations régulières avec les salariés pour recueillir leurs préoccupations et leurs suggestions concernant l'utilisation des SIA.

## Négociations et accords collectifs

### Des thèmes de négociations peuvent être concernés par l'usage des outils numériques

- L'articulation vie pro/vie perso.
- Le droit à la déconnexion.
- L'égalité professionnelle entre les femmes et les hommes (notamment les mesures de lutte contre les discriminations, sur la qualité de vie au travail, etc.).
- La gestion des emplois et des compétences (GEPP).
- Le partage de la valeur.
- Le temps de travail et les RTT.
- Exercice du droit d'expression direct et collectif des salariés.

De plus, les outils numériques et les SIA peuvent être évoqués pendant les commissions de suivi des accords.

### Négocier le déploiement des outils numériques et des systèmes d'IA

Des règles et des repères sur le déploiement des outils numériques et des SIA dans le travail peuvent se négocier et s'élaborer collectivement. Très peu d'accords portent sur ce sujet aujourd'hui malgré 2 accords européens (l'un pour le privé, l'autre pour le public) :

- [accord sur la transformation numérique des entreprises](#)
- [accord-cadre sur la numérisation des administrations d'état et fédérales](#)

Négocier le déploiement et l'usage des outils numériques dans le travail est une bonne occasion de discuter de l'organisation du travail, des conditions de travail, du partage de la valeur et de l'évolution des emplois et des compétences. La négociation peut s'appuyer sur les éléments indiqués dans le document [Fiche pratique: Négocier les transformations numériques.](#)



## 2. PROTECTION DES DONNÉES PERSONNELLES

La grande majorité des outils numériques et des SIA fonctionnent à partir de données (cf. [Lexique et principaux usages des outils numériques et des SIA](#)). Ces données peuvent être collectés sur le lieu de travail et avoir un caractère personnel.

En ce qui concerne la protection des données personnelles, **plusieurs obligations concernent l'employeur**. Tout d'abord, un traitement de données à caractère personnel doit respecter certains principes. Ainsi, le traitement doit :

- **Être licite (art. 6 RGPD)**, pour cela il doit se baser sur l'un des 6 fondements prévus à l'article 6.1 du règlement général de protection des données (RGPD). En matière de relation de travail, l'employeur pourra se fonder par exemple sur l'exécution du contrat de travail, sur le respect d'une obligation légale ou encore sur la poursuite d'un intérêt légitime.
- **Respecter le principe de minimisation des données (art. 5 RGPD)**, les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées. Par exemple, il n'est pas nécessaire pour un employeur de collecter et de conserver le statut marital d'un salarié.
- **Respecter des « finalités déterminées, explicites et légitimes »** pour collecter des données (art. 5 RGPD). Autrement dit l'employeur ne peut collecter des données que dans un intérêt professionnel (contrôler le temps de travail par exemple). Et il ne peut détourner cette finalité, le traitement de données devant s'utiliser pour l'usage déterminé. Par exemple, un système destiné à éviter les piratages informatiques ne peut servir à évaluer les performances des salariés.
- **Avoir une durée de conservation des données limitée (art. 5 RGPD)**, les données ne peuvent être conservées indéfiniment. Une durée de conservation doit être définie en amont en fonction de l'objectif poursuivi. Une fois l'objectif réalisé, elles devront alors être supprimées (par exemple, les données d'un candidat non-retenu ne pourront pas être conservées plus de 2 ans selon la Cnil). Mais elles peuvent également être archivées avec restriction d'accès (plutôt qu'effacées) dès lors qu'elle présente encore un intérêt pour l'employeur (par exemple pour un éventuel contentieux, un contrôle Urssaf, etc) ou pour respecter une obligation légale (par exemple la conservation des fiches de paie). **Ressource utile :** <https://www.cnil.fr/fr/passer-l'action/les-durees-de-conservation-des-donnees>
- **Être transparent (Art. 5 RGPD)**, la personne doit être informée de tout traitement de ses données à caractère personnel. Cela peut par exemple prendre la forme d'une clause dans le contrat de travail.
- **Garantir la sécurité et l'intégrité des données (art. 5 RGPD)**, l'employeur doit s'assurer que les données sont bien protégées. Cela passe par exemple par des mesures de sécurité informatique ou encore par une limitation de l'accès aux données sensibles (coordonnées bancaires, etc) à certains salariés seulement.



## Deux obligations découlent en particulier de ce principe de sécurité

### 1. Obligation de l'employeur de sécuriser les données personnelles (art. 32 RGPD)

Les données personnelles des salariés doivent faire l'objet d'une vigilance spécifique en raison des différents risques existant (piratage, fuite et divulgation des données, accès non-autorisé à des données...). Ainsi, l'employeur doit prendre toutes les mesures techniques et organisationnelles appropriées pour en assurer la sécurité et la confidentialité.

- Les mesures organisationnelles peuvent être par exemple la désignation d'un DPO (Délégué à la protection des données), restreindre l'accès aux serveurs informatiques, sensibiliser aux cyberattaques, adopter une charte informatique...  
La Cnil préconise la formation obligatoire de tout le personnel sur l'identification et la notification de violations ainsi que la conduite à tenir dans ce cas<sup>1</sup>.
- Les mesures techniques vont concerner les services informatiques. Le RGPD donne des exemples comme la pseudonymisation et le chiffrement des données.

### 2. En cas de violation des données personnelles (art. 33 et 34 RGPD)

L'employeur doit documenter toute violation de données personnelles dans un registre. Il y indique les faits concernant la violation, les effets et les mesures prises pour y remédier.

#### Deux procédures de notification :

- l'une auprès de la Cnil : dès lors que l'employeur constate une violation, il doit en informer la Cnil dans les meilleurs délais et, si possible, 72 heures au plus tard ;
- l'autre auprès de la personne concernée : si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne, l'employeur doit en informer la personne concernée.

Ressource utile : <https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles>

## Obligations concernant le transfert de données

La communication, la copie ou le déplacement de données personnelles, destinées à être traitées dans un pays hors de l'Union européenne, doivent respecter le cadre posé par le chapitre V du RGPD. Il faut en particulier qu'un niveau de protection des données suffisant et approprié soit assuré.

Pour plus de précisions : <https://www.cnil.fr/fr/transferts-de-donnees-hors-ue-le-cadre-general-prevu-par-le-rgpd>

Le 22 juillet 2024, en coopération avec la Cnil, l'autorité néerlandaise de protection des données a prononcé à l'encontre des sociétés **Uber B.V.** et **Uber Technology Inc.** une amende de 290 millions d'euros pour avoir transféré des données personnelles de 170 chauffeurs VTC de la plateforme **Uber** hors UE, cela sans garanties suffisantes.

<sup>1</sup> <https://www.cnil.fr/fr/securite-gerer-les-incidents-et-les-violations>



## De plus, l'employeur doit :

- tenir **un registre des activités de traitement des données personnelles** permettant de recenser les traitements de données personnelles dans l'entreprise (art. 30 RGPD). <https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement>
- réaliser **une analyse d'impact relative à la protection des données (AIPD)**, c'est à dire, réaliser une AIPD pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes (Art. 35 RGPD). <https://www.cnil.fr/fr/ce-quit-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipddésigner>
- désigner **un délégué à la protection des données personnelles (DPO)** : (art. 37 à 39 RGPD) Celui-ci assure la protection des données personnelles au sein de l'entreprise. Sa désignation est obligatoire lorsque l'activité de l'entreprise amène à un suivi régulier et systématique à grande échelle des personnes, ou à traiter à grande échelle des données sensibles ou relatives à des condamnations pénales et à des infractions. La Cnil incite fortement à désigner un DPO même lorsque l'entreprise n'est pas formellement obligée de le faire.

Le 22 juillet 2024, la Cnil a décidé de liquider l'astreinte prononcée à l'encontre de la **commune de Kourou**, qui en tant qu'autorité publique a pour obligation de désigner un délégué à la protection des données. La commune devra payer la somme de 6 900 euros pour ne s'être toujours pas conformée à son obligation de désigner un délégué à la protection des données malgré l'injonction de la Cnil de décembre 2023.

## Les travailleurs eux disposent de nombreux leviers pour faire valoir la protection de leurs données personnelles

### Droit à l'information d'une collecte de données (art. 13 et 14 RGPD)

Lors d'une collecte de données par l'employeur, un certain nombre d'informations doivent être fournies aux salariés ou aux candidats à un emploi. L'information intervient au moment où les données sont obtenues.

- **Données collectées directement auprès de la personne concernée (par exemple, les informations données au moment de l'embauche)** : l'employeur doit lui fournir une liste d'information prévue à l'article 13 du RGPD. Par exemple, les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement, l'identité et les coordonnées du responsable du traitement ou de son représentant. Ces informations sont fournies au moment où les données sont collectées.
- **Données collectées indirectement (les données ne sont pas collectées directement auprès de la personne concernée, par exemple via internet)** : des informations complémentaires doivent être transmises. L'ensemble de ces informations sont fournies par le responsable de traitement dans un délai raisonnable, et au plus tard un mois après la collecte.



### Le droit d'accès aux données (art. 15 RGPD)

Selon la Cnil, un travailleur peut obtenir « l'accès et communication de l'ensemble des données le concernant, qu'elles soient conservées sur support informatique ou papier ». Cela peut ainsi concerner des données relatives au recrutement du salarié, à son historique de carrière, etc.

Le responsable du fichier dispose d'un délai de réponse maximal d'un mois à compter de la réception de la demande.

### Droit à la portabilité (art. 20 RGPD)

Il permet à toute personne de « recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement ».

À la différence du droit d'accès, il permet en plus de faire transmettre directement ses données à un autre responsable de traitement lorsque c'est techniquement possible. Cela renvoie typiquement à l'hypothèse de données personnelles envoyées directement d'un ex-employeur vers le nouvel employeur du salarié, ou d'une plateforme numérique de travail à une autre. En pratique, ce droit peut par exemple concerner des services de paiement.

### Droit à la rectification des données personnelles (art. 16 RGPD)

Le salarié dispose d'un droit de rectification sur ses données personnelles traitées par l'employeur. Il pourra faire corriger des données inexactes le concernant (âge, classement, rémunération, notes erronées...), ou faire compléter des données en lien avec la finalité du traitement

### Droit de refuser ou de contester une prise de décision automatisée

**Algorithme d'aide à la décision :** dans le cas où l'employeur se base sur un algorithme informatique d'aide la décision (comme le serait un tableau de bord RH recensant informatiquement la productivité de l'ensemble des salariés pour attribuer des primes), le salarié pourra contester la décision prise sur la base d'un tel traitement si l'employeur ne justifie pas d'un fondement licite (art. 6, RGPD).

**Décision exclusivement algorithmique (article 22 RGPD) :** elle est en principe prohibée : l'employeur ne peut pas laisser un programme informatique prendre une décision pour son salarié si cette décision produit des effets juridiques (annulation ou modification d'un contrat de travail, désactivation du compte, avancement de carrière, changement d'un avantage social particulier accordé par la loi ou une convention collective...), ou l'affecte de manière significative (par exemple, sur sa situation sociale ou son état de santé).

#### Toutefois, deux exceptions existent :

- lorsque cela est prévu par la loi et qu'il existe des mesures appropriées pour sauvegarder les droits et intérêts légitimes du travailleur en compensation (plutôt rare en pratique dans les relations de travail) ;
- lorsque les directives algorithmiques sont nécessaires à la conclusion ou à l'exécution du contrat entre le travailleur et l'employeur. Cela suppose que l'employeur démontre qu'il n'existait pas d'autres moyens moins intrusifs pour atteindre le même but.



**Pour les travailleurs de plateforme :** Lorsque l'employeur est une plateforme numérique de travail, la directive européenne relative à l'amélioration des conditions de travail des travailleurs de plateformes numériques interdit la prise de décision fondée exclusivement sur un algorithme, sans prévoir d'exception. **Attention néanmoins**, la directive n'a pas encore été transposée en droit français et ne produit donc pas encore ses effets.

### Droit à l'explicabilité (art. 22 RGPD)

Lorsque la décision est prise pour la conclusion ou l'exécution du contrat, le travailleur peut obtenir une intervention humaine de la part du responsable du traitement [l'employeur]. Cette personne devra dès lors expliquer au travailleur la décision algorithmique afin qu'il soit en mesure « *d'exprimer son point de vue et de contester la décision* ». Pour le travailleur, cela sous-tend un droit à l'information renforcé.

À titre d'exemple, pour une application de recrutement dont le but serait de déceler les capacités émotionnelles et cognitives du candidat, celui-ci serait bien-fondé à demander la logique sous-jacente et les critères précis ayant conduit l'algorithme à l'évincer du poste à pourvoir. L'explication doit être assez complète sans que cela nécessite de comprendre le fonctionnement de l'algorithme dans sa complexité technique.

### Droit d'opposition (art. 21 RGPD)

Lorsque l'employeur traite les données personnelles du salarié à des fins d'intérêt légitime, ce dernier peut s'y opposer à tout moment « *pour des raisons tenant à sa situation particulière* ». Applicable à tout type de traitement algorithmique de données personnelles.

L'employeur doit alors mettre fin au traitement de données, sauf s'il démontre qu'il existe des motifs impérieux et légitimes pour le traitement qui prévalent sur les intérêts et droits du salarié. En pratique, l'employeur pourra refuser la demande si le traitement de données est indispensable pour l'exécution du contrat de travail.

À titre d'exemple, une personne pourrait demander que son numéro de téléphone soit retiré du site internet de l'entreprise pour des raisons de sécurité personnelle.

### Droit d'effacement (art. 17 RGPD)

Le travailleur a le droit d'obtenir l'effacement de ses données personnelles dans les meilleurs délais par l'employeur dans 3 situations :

- lorsque le traitement est réalisé à des fins d'intérêts légitimes ou à des fins de prospections dans les mêmes conditions que le droit d'opposition ;
- lorsque de telles données « ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière » (par exemple les données d'un candidat non sélectionné à la suite d'un processus de recrutement) ;
- lorsque le traitement est illicite.

L'employeur peut refuser une telle demande s'il justifie que le traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation prévue par la loi. À titre d'exemple, les bulletins de paie émis sous format électronique doivent être conservés pendant 50 ans ou jusqu'à ce que le salarié ait atteint l'âge de départ à la retraite augmenté de 6 ans.



## 3. SANTÉ ET SÉCURITÉ

Les outils numériques et les SIA peuvent avoir des conséquences sur la santé et la sécurité des travailleurs, par exemple en augmentant la charge de travail. Ils peuvent également permettre d'améliorer la prévention en diminuant des contraintes ou en permettant de mieux identifier les risques. Pour rappel, les obligations suivantes s'appliquent à l'employeur :

### **La responsabilité de l'employeur en matière de santé et sécurité (art. L.4121-1 C. trav.)**

L'employeur prend les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Ce qui comprend notamment des actions de prévention des risques professionnels, des actions d'information et de formation et la mise en place d'une organisation et de moyens adaptés.

L'employeur ne peut s'exonérer de sa responsabilité en matière de prévention des risques.

Par exemple, un SIA utilisé pour optimiser le montage des palettes dans une entreprise de logistique peut ne pas avoir été développé en prenant en compte les conditions de « déchargement » de la palette par un travailleur à l'autre bout de la chaîne d'expédition et présenter un risque de blessure pour les personnes concernées (chute de colis). La responsabilité de l'employeur peut être mise en cause et l'adaptation du SIA demandée sur ce fondement.

### **La prévention des risques liés aux outils numériques et aux SIA (art. L. 4121-3-1 C. trav.)**

Les risques liés à l'usage des outils numériques et des SIA sur la santé et la sécurité des salariés doivent être identifiés dans le Duerp et le Papripact.

Le Duerp doit être mis à jour :

- au moins une fois par an (entreprises de plus de 11 salariés) ;
- en cas de décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail ;
- lorsqu'une information supplémentaire intéressant l'évaluation d'un risque est portée à la connaissance de l'employeur.

Il donne lieu à consultation du CSE (art. L. 2312-27 C. trav.).

En cas de risque grave identifié et actuel constaté dans l'établissement, le CSE peut recourir à un expert (L2315-94 1° C. trav.). À la différence de l'expert-comptable qui, dans le cadre sa mission d'expertise en vue de la consultation sur la politique sociale, ne peut auditionner les salariés sans l'accord de l'employeur, en cas d'expertise déclenchée sur le fondement d'un risque grave, l'expert pourra auditionner les salariés qui y consentent sans avoir à obtenir l'accord de l'employeur afin de mener à

bien sa mission (Cass. soc.10.07.24, n°22-21082).



## 4. DISPOSITIFS DE CONTRÔLE ET DE SURVEILLANCE

Si le contrôle et la surveillance des travailleurs n'ont pas attendu le numérique pour exister, les outils numériques (caméras, clavier, etc) et les SIA peuvent à la fois les renforcer et les invisibiliser, les rendant ainsi plus difficiles à prévenir et à corriger. Ces outils peuvent être utilisés par les directions pour évaluer (par exemple avec un classement des travailleurs) ou pour surveiller (géolocalisation). On peut également penser à un outil destiné à contrôler le temps de travail des salariés dans le but de s'assurer du respect des temps de repos, mais dont l'utilisation peut dériver en un contrôle excessif.

**Toutefois, plusieurs dispositions encadrent ces pratiques.**

### Le principe de justification et de proportionnalité

*« 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. »* (art. L. 1121-1 C. trav.).

Ainsi, dans l'exercice de son pouvoir de contrôle, l'employeur doit être en mesure de justifier que le dispositif mis en œuvre ne porte pas une atteinte excessive aux droits et libertés des salariés.

Une atteinte serait disproportionnée dès lors que le même résultat peut être obtenu par un moyen moins restrictif des libertés.

Ainsi, un employeur ne pourrait pas utiliser de logiciel d'enregistrement des mouvements de la souris et des touches du clavier pour s'assurer que les travailleurs sont bien en ligne, cela étant de toute évidence disproportionné.

Le 27 décembre 2023, la Cnil a sanctionné **Amazon France Logistique** d'une amende de 32 millions d'euros pour avoir mis en place un système de surveillance de l'activité et des performances des salariés excessivement intrusif. La société est également sanctionnée pour de la vidéosurveillance sans information et insuffisamment sécurisée.

### L'obligation de transparence de l'employeur

#### Information des salariés

*« Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »* (Art. L. 1222-4 C. trav.).

Ainsi, l'employeur a l'obligation d'informer l'ensemble des salariés avant toute mise en place d'un dispositif de contrôle.

#### Information et consultation des élus

Le CSE *« est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés »* (art. L. 2312-38 C. trav.).



Les données collectées à l'aide d'un dispositif mis en place sans respect de cette double obligation ne pourront servir à fonder une sanction disciplinaire.

## **Respect d'une finalité légitime, explicite et déterminée par l'employeur (art. 5 RGPD)**

Voir page 8 : [2. Principes d'un traitement de données à caractère personnel](#) pour plus de précisions.

La finalité du dispositif mis en place ne peut être détournée. Ainsi, un système de vidéosurveillance destinée à assurer la sécurité d'un bâtiment ne peut servir à contrôler l'activité des salariés.

# **5. RÈGLES EN COURS DE CONSTRUCTION OU PAS ENCORE APPLICABLES**

## **Travailleurs de plateforme (salariés)**

La directive relative à l'amélioration des conditions de travail des travailleurs de plateformes numériques prévoit qu'une évaluation des risques que présentent les systèmes de surveillance et de prise de décision automatisés en matière d'accident du travail et de risques psycho-sociaux doit avoir lieu. Les systèmes exerçant une pression indue sur la santé physique et mentale des travailleurs de plateforme doivent être bannis. Des mesures de prévention et de protection appropriées doivent être mises en place, en particulier contre la violence et le harcèlement par exemple au moyen de canaux de signalement efficaces (article 12).

Attention, la directive n'est pas encore transposée donc pas encore applicable dans une loi.

## **Règlement européen sur l'IA**

Entrée en vigueur progressive en fonction des règles à partir de février 2025. Ce tableau de bord évoluera en fonction de ces entrées en application.

Le règlement européen sur l'IA (ou "AI Act" en anglais) constitue la première tentative dans le monde de création d'un cadre légal sur les systèmes d'IA. Pour ce faire, il classe les systèmes d'IA en **4 niveaux de risques** et auquel est rattaché **4 niveaux de mise en conformité** :

- **risque « minime »**, accompagné de **codes de conduites** ;
- **risque « faible »** accompagné d'une **obligation d'information** ;
- systèmes d'IA à **« haut risque »** qui sont permis **sous certaines conditions** ;
- ceux enfin qui emportent un **risque « inacceptable »** et qui sont **par conséquent, interdits**.

Les systèmes d'IA utilisés dans le domaine du travail pour le recrutement, l'évolution des carrières, le licenciement ou encore l'évaluation des performances, sont classés à « haut risque ». De fait, plusieurs obligations s'appliquent, comme : l'analyse des risques avant la mise sur le marché, le contrôle humain



sur la machine, l'information des travailleurs et représentants avant le déploiement, un système de gestion des risques, une étude d'impact sur les droits fondamentaux quand cela concerne des organismes publics ou privés fournissant un service d'intérêt général, un mécanisme de plainte (qui reste à préciser) et un droit à l'explicabilité.

Pour les **modèles d'IA à usage général** (ex: ChatGPT), des obligations spécifiques s'appliquent concernant la qualité des données, le respect du droit d'auteur, la cybersécurité, la transparence sur la consommation énergétique.

Pour aller plus loin, lire [la présentation de la Cnil et son analyse comparative sur le règlement sur l'IA et le RGPD](#).

## RESSOURCES COMPLÉMENTAIRES

### DOCUMENTS Cnil ([www.cnil.fr](http://www.cnil.fr))

- [Les règles pour la gestion du personnel](#)
- [Les questions/réponses sur le télétravail](#)
- [Ce qu'il faut savoir sur les AIPD](#)
- [Guide de sensibilisation au RGPD pour les organisations syndicales](#)
- [Guide de la sécurité des données personnelles](#)

### Pour en savoir plus sur les régulations européennes portant sur la donnée et les systèmes d'IA :

- [WEB-Guide-Data-AI-Regles-VF. pdf](#) (interconnectes.com)
- *Le guide de l'intelligence artificielle au travail, vos droits face aux algorithmes.* De Franca Salis Madinier (CFDT Cadres) aux Éditions Eyrolles. Voir [Le Catalogue - Les indispensables de l'action syndicale \(CFDT\)](#).

