CLOUDY MAG

A T-ON LE DROIT DE VIVRE EN PAIX ???

Bien , un peu lourd ce poly de droit, heureusement Patrick Cloudy est là pour essayer de condenser tout ça !

"C’est la meilleure période de l’année… si vous êtes insomniaque ou adepte des cafés quadruples. Deux DS d’affilée, c’est comme un marathon : sauf que là, on court avec des pages de cours et des surligneurs en guise de chaussures. Entre la CNIL et les hmm yeah de Master Vanuxem, il faut jongler avec des dates, des définitions, et un peu d’impro pour survivre. Courage à tous : après cette semaine, c’est promis, on prendra un vrai week-end (ah bah non c’est encore pire la semaine prochaine)."

-SOURCE PATRICK DLOUDY

Chapitre 1 : La CNIL

Définitions clés

- **AAI (Autorité Administrative Indépendante)** :
  - Structure autonome sans lien hiérarchique avec le gouvernement.
  - Chargée de réguler un domaine spécifique (ex. CNIL pour les données personnelles).
- **Données personnelles** :
  - Informations permettant d'identifier directement ou indirectement une personne (ex. nom, adresse, numéro de téléphone, identifiant IP).
- **Données sensibles** :
  - Données révélant des détails intimes tels que l'origine raciale, la santé, les convictions religieuses, les opinions politiques, ou l'orientation sexuelle.

Organisation de la CNIL

- **Création** : 1978, via la loi Informatique et Libertés.
- **Missions** :
  1. **Informer** le public sur leurs droits.
  2. **Contrôler** les organismes pour garantir la conformité avec la loi.
  3. **Sanctionner** en cas de manquement (amendes RGPD pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial).
  4. **Conseiller** les entreprises et administrations.

Les 9 droits informatiques et libertés

1. **Droit d'accès** : Consulter ses données personnelles collectées.
2. **Droit de rectification** : Corriger ou compléter des informations erronées.
3. **Droit d'effacement** : Demander la suppression des données non nécessaires.
4. **Droit à la limitation** : Restreindre l'usage des données.
5. **Droit à la portabilité** : Obtenir et réutiliser ses données dans un autre service.
6. **Droit d'opposition** : Refuser l'utilisation des données à certaines fins (ex. marketing).
7. **Droit d'information** : Être informé de l'utilisation des données.
8. **Droit de ne pas faire l'objet de décisions automatisées** : Contester un traitement basé uniquement sur des algorithmes.
9. **Retrait du consentement** : Révoquer son accord pour le traitement des données.

Chapitre 2 : La surveillance en entreprise

Introduction : Les enjeux de la surveillance

La surveillance en entreprise est encadrée par le droit afin de concilier deux impératifs:

- Les droits et libertés des salariés, notamment leur droit à la vie privée (article 9 du Code civil).
- Les intérêts légitimes de l'employeur, comme la protection de ses biens ou la productivité.

1. Respect de la vie privée et charte d'utilisation

- **Vie privée au travail** : Le salarié conserve son droit à une vie privée, même sur son lieu de travail.
    - Ce principe s'étend à l'utilisation d'outils numériques (emails, navigation internet).
    - Décision clé : **Arrêt Nikon (2001)**, qui affirme qu'un employeur ne peut surveiller des communications personnelles sans en avertir le salarié.
- **Charte d'utilisation des outils numériques** :
    - Permet à l'employeur de définir les règles pour l'usage professionnel et privé.
    - **Exemple** : Limitation de l'accès à certains sites web (réseaux sociaux, streaming).
    - Obligation de transparence:
        - Les salariés doivent être informés de la mise en place d'un dispositif de surveillance.
        - La charte doit être communiquée et validée par les représentants du personnel.
- **Risques d'un usage privé excessif** :
    - Un salarié peut être sanctionné pour des abus (par exemple, utiliser l'ordinateur de l'entreprise pour des activités personnelles pendant les heures de travail).
    - Les preuves recueillies par l'employeur doivent respecter la vie privée (ex. contrôle des emails uniquement après information préalable).

2. Géolocalisation des employés

- **Utilisation encadrée** :
    - Justifiée uniquement par des raisons professionnelles:
        - Optimisation des trajets (livraisons, interventions techniques).
        - Sécurité des salariés (notamment pour les métiers à risque).
    - L'employeur doit informer les salariés en amont et préciser les finalités du dispositif.
- **Limites légales** :
    - La géolocalisation ne doit pas porter atteinte à la vie privée des salariés:
        - **Surveillance hors des heures de travail interdite** (arrêt CNIL, 2018).
        - La géolocalisation continue (24h/24) est illégale sauf pour des raisons exceptionnelles.
- **Exemple** : Un livreur géolocalisé en temps réel peut contester la surveillance en dehors de ses horaires de travail.

3. Surveillance au domicile (télétravail)

- **Surveillance des outils numériques** :
    - L'employeur peut surveiller l'activité des salariés en télétravail pour garantir leur productivité, mais sous conditions:
        - Les moyens doivent être proportionnés (ex. limitation à des outils d'analyse anonymes).
        - Les salariés doivent être informés de ces dispositifs.
- **Limites de la surveillance à domicile** :
    - La vie privée est protégée:
        - Aucune caméra ou logiciel espion ne peut être installé sans consentement explicite.
        - Les outils de surveillance doivent être liés exclusivement à l'activité professionnelle.
- **Décisions de justice** :
    - Un employeur condamné pour avoir installé un logiciel espion sur l'ordinateur professionnel sans prévenir le salarié (Arrêt Cass. soc. 2013).

4. Surveillance et données sensibles

- L'utilisation d'outils numériques en entreprise implique souvent le traitement de **données personnelles** des salariés.
    - Par exemple: Emails, historique de navigation, accès à des fichiers partagés.
- **Règles imposées par la CNIL**:
    - L'employeur doit respecter les principes du RGPD (Règlement Général sur la Protection des Données):
        - **Transparence** : Informer les salariés des finalités du traitement.
        - **Proportionnalité** : Ne pas collecter de données excessives.
        - **Sécurité** : Protéger les données contre les accès non autorisés.

5. Surveillance et décisions clés

1. **Emails professionnels et privés** :
    - Les emails identifiés comme "personnels" (par leur objet ou contenu) ne peuvent être ouverts par l'employeur.
    - Les emails professionnels sont consultables, mais uniquement si l'employeur informe le salarié.
2. **Utilisation des caméras** :
    - Les caméras ne peuvent filmer des lieux à caractère privé (ex. vestiaires, toilettes).
    - Les enregistrements doivent être justifiés par une finalité légitime (ex. sécurité) et ne peuvent être conservés indéfiniment.
3. **Internet et réseaux sociaux** :
    - La navigation sur internet peut être surveillée, mais dans les limites fixées par la charte d'utilisation.
    - Un salarié licencié pour avoir critiqué son employeur sur les réseaux sociaux peut contester la décision s'il prouve que ses propos relevaient de la sphère privée.

Chapitre 3 : La protection de la création

Définitions clés

- **Droit d'auteur** :
  - Protège les œuvres originales (textes, logiciels, musique, etc.).
  - Assure au créateur des droits exclusifs sur l'exploitation et la diffusion.
- **Titulaire du droit** :
  - L'auteur (individu).
  - Employeur (pour les œuvres collectives ou de collaboration).

Les types de droits et leur utilisation

1. **Droits moraux** (inaliénables, perpétuels) :
   - **Droit de divulgation** : Décider de rendre publique ou non l'œuvre.
   - **Droit de paternité** : Exiger la mention de l'auteur.
   - **Droit au respect** : Interdire des modifications dénaturant l'œuvre.
   - **Droit de retrait** : Reprendre l'œuvre en renonçant à son exploitation.
2. **Droits patrimoniaux** (transférables, limités dans le temps) :
   - **Droit de reproduction** : Autoriser ou interdire la copie de l'œuvre.
   - **Droit de représentation** : Contrôler la diffusion publique.
   - **Droit d'adaptation** : Régir les transformations (ex. film basé sur un livre).
   - Durée : 70 ans après le décès de l'auteur (prolongation possible pour des raisons de guerre).
3. **Droits spécifiques selon le type d'œuvre** :
   - Œuvres collectives (ex. journaux) : Les droits appartiennent à l'entité qui coordonne.
   - Œuvres de collaboration (ex. films) : Les droits sont partagés entre les co-auteurs.

Hadopi

- **Création** : Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet.
- **Mission** : Lutter contre le téléchargement illégal et promouvoir les offres légales.

Chapitre 4 : Logiciels, bases de données et noms de domaine

Tableau : Éléments protégés vs. non protégés

Protégés	Non protégés
Code source	Cahier des charges
Code objet	Langages de programmation
Versions successives	Méthodes ou algorithmes mathématiques
Documentation technique	Idées ou concepts abstraits
Interface utilisateur (originale)	Analyse fonctionnelle

Logiciels

- **Définition** : Ensemble de programmes exécutables par une machine.
- **Critères de protection** :
  - Originalité (effort intellectuel).
  - Création intellectuelle propre à l'auteur.
- **Techniques de protection** : Droits d'auteur, brevets, licences.
- **Prérogatives de l'auteur** :
  - Exploiter l'œuvre.
  - Autoriser ou interdire la modification.
- **Prérogatives de l'utilisateur** (Code de la propriété intellectuelle - CPI) :
  - Droit d'utiliser le logiciel.
  - Droit de correction des bugs.
  - Droit de sauvegarde.
  - Droit d'interopérabilité.
- **Distinction** :
  - Œuvre de collaboration : Contributions distinctes (ex. développement).
  - Œuvre collective : Droits détenus par l'entité commanditaire.

Bases de données

- **Protection** :
  - Par les droits d'auteur (structure originale).
  - Par le droit du producteur (investissement financier).
- **Droits opposables** : Protéger l'extraction des données.

Noms de domaine

- **Statut juridique** : Élément distinctif d'une marque.
- **Actions possibles** : Opposition, saisie judiciaire en cas de litige.

Chapitre 5 : La protection des salariés

Introduction : Principes fondamentaux

La protection des salariés repose sur deux principes clés: **la prévention des risques professionnels** et **le respect de la santé physique et mentale** des travailleurs. Ces principes découlent du Code du travail (articles L4121-1 et suivants) et sont renforcés par des directives européennes.

1. Prévention vs précaution

- **Prévention** :
    - Vise à anticiper les risques identifiés dans l'environnement de travail.
    - Fondée sur des mesures proactives: analyse des risques, formations, équipements de sécurité.
    - Exemples :
        - Établir un plan de prévention des incendies.
        - Formation des salariés sur les bonnes pratiques ergonomiques pour éviter les troubles musculo-squelettiques.
- **Précaution** :
    - S'applique en présence d'un risque **potentiel**, mais non avéré, en tenant compte des incertitudes scientifiques.
    - Exemples :
        - Limiter l'exposition à des substances chimiques non encore pleinement étudiées.
        - Adapter les procédures pendant une pandémie (ex. télétravail).

Différence principale : La prévention traite des dangers identifiés, tandis que la précaution concerne les risques incertains.

2. Santé physique et mentale des salariés

- **Évolution de la notion de santé au travail** :
    - Initialement axée sur les blessures physiques.
    - Aujourd'hui, inclut la santé mentale (stress, burn-out, harcèlement moral).
    - **Harcèlement moral** :
        - Reconnu depuis la loi de 2002.
        - Se caractérise par des actes répétés (humiliations, isolement, surcharge de travail).
        - Obligation pour l'employeur de prévenir et sanctionner ces comportements.
- **Risques psychosociaux** :
    - Stress, surcharge, absence de reconnaissance.
    - Conséquences: baisse de productivité, absentéisme, troubles psychologiques.
- **Contrôle de la santé des salariés** :
    - Médecine du travail : Suivi obligatoire (visites médicales).
    - Objectif: Identifier les risques, adapter les postes.

3. Situation de danger grave et imminent

- **Droit de retrait** :
    - Permet au salarié de quitter son poste sans sanction en cas de danger immédiat pour sa vie ou sa santé (article L4131-1 du Code du travail).
    - Exemples :
        - Fuite de gaz sur le lieu de travail.
        - Utilisation d'une machine défectueuse.
- **Procédure** :
    - Informer l'employeur ou le responsable hiérarchique.
    - L'employeur doit immédiatement remédier à la situation.

4. Principes généraux de prévention

Les employeurs doivent suivre les **9 principes généraux de prévention** (article L4121-2 du Code du travail):

1. Éviter les risques (supprimer le danger).
2. Évaluer les risques qui ne peuvent être évités.
3. Combattre les risques à la source.
4. Adapter le travail à l'homme (ex. ergonomie des postes).
5. Tenir compte de l'évolution technique (ex. nouveaux équipements).
6. Remplacer ce qui est dangereux par ce qui ne l'est pas ou l'est moins.
7. Planifier la prévention.
8. Prendre des mesures collectives en priorité sur les mesures individuelles.
9. Donner les instructions appropriées aux salariés.

Exercice d’application

Cas pratique :

Marie, salariée dans une usine chimique, signale à son employeur une exposition régulière à des émanations toxiques. Elle constate que plusieurs collègues présentent des symptômes similaires (maux de tête, nausées). L’employeur minimise la situation en expliquant que les masques sont facultatifs.

Marie décide de se retirer de son poste. Est-ce légal ?

Quelles mesures l’employeur aurait dû mettre en place ?

Identifiez les principes de prévention applicables.

Correction :

Droit de retrait :

Oui, Marie peut exercer son droit de retrait. Les émanations toxiques représentent un danger grave et imminent pour sa santé. L’absence de mesures appropriées justifie son retrait.

Mesures de l’employeur :

Évaluer le risque via une analyse des émanations.
Installer des dispositifs de ventilation ou filtrage.
Fournir des équipements de protection (masques obligatoires).
Former les salariés sur les dangers des substances manipulées.

Principes de prévention applicables :

Éviter les risques : Supprimer ou limiter les émanations toxiques.
Évaluer les risques : Mesurer les niveaux de toxicité.
Adapter le travail à l’homme : Fournir des équipements adaptés.
Planifier la prévention : Mettre en place des protocoles en cas de fuite ou exposition accidentelle.

Exercice d'application
Cas pratique :

Paul est technicien dans une entreprise qui l'équipe d'un véhicule avec un dispositif de géolocalisation. Ce système enregistre ses trajets, y compris en dehors des heures de travail. Un jour, l'entreprise utilise ces données pour le licencier, arguant qu'il a fait un détour non justifié pendant ses heures de travail.

1. La géolocalisation continue est-elle légale?
2. L'utilisation des données pour un licenciement est-elle justifiée?
3. Que peut invoquer Paul pour contester cette décision?

Correction :

1. **Légalité de la géolocalisation continue** :
    - Non. La surveillance hors des heures de travail est interdite. Le dispositif aurait dû être désactivé une fois la journée terminée.
2. **Utilisation des données pour le licenciement** :
    - L'employeur peut utiliser les données de géolocalisation pour prouver un abus professionnel, mais uniquement si :
        - Les salariés ont été informés du dispositif et de son usage.
        - Le dispositif respecte les principes de proportionnalité.
3. **Arguments de Paul** :
    - Contester la **géolocalisation continue** en violation de son droit à la vie privée (décision CNIL, 2018).
    - Argumenter sur l'absence de communication claire concernant l'utilisation des données.