**CH2 : LA PROTECTION DES PERSONNES DANS L’UNIVERS NUMERIQUE**

|  |  |
| --- | --- |
| **OBJECTIFS** | A l’issu du chapitre, vous devez être capable de :   * Caractériser les conséquences juridiques des choix opérés par l’entreprise sur la protection des personnes, des données |

**INTRODUCTION**

|  |  |
| --- | --- |
| **IMPORTANCE** | La protection des données personnelles et la surveillance au travail sont cruciales pour préserver les droits individuels à l'ère numérique.  La loi sur la protection des données personnelles, renforcée par le RGPD, vise à protéger les individus contre l'exploitation abusive de leurs données, assurant ainsi leur vie privée et leur sécurité. Les obligations imposées aux organisations, telles que la sécurisation des données et l'information des personnes concernées, sont essentielles pour éviter les violations de la vie privée.  Dans le contexte professionnel, les restrictions sur la surveillance garantissent un équilibre entre le pouvoir de l'employeur et les droits des employés, assurant que les contrôles ne portent pas atteinte à leurs libertés fondamentales.  Ces mesures contribuent à établir un cadre juridique où les droits des individus sont respectés, malgré l'usage croissant des technologies numériques. |
| **NOTIONS CLES** | * Le rôle de la CNIL * La protection de la personne : les données à caractère personnel, l’identité numérique, l’usage du numérique dans l’activité de travail |

Plan de cours

[1. Définitions des notions clés 2](#_Toc175539404)

[2. La protection dans la sphère privée 2](#_Toc175539405)

[3. La protection dans la sphère professionnelle 4](#_Toc175539406)

[4. Résumé 5](#_Toc175539407)

[5. Exercice 1 6](#_Toc175539408)

[6. Exercice 2 6](#_Toc175539409)

[7. Exercice 3 7](#_Toc175539410)

**LE COURS**

## Définitions des notions clés

|  |
| --- |
| * **CNIL** (Commission Nationale de l'Informatique et des Libertés) : Autorité administrative indépendante chargée de veiller à la protection des données personnelles et à la vie privée. Elle dispose de pouvoirs de sanction en cas de non-conformité. * **Données à caractère personnel** : Toute information permettant d’identifier directement ou indirectement une personne physique (ex : nom, adresse, numéro de téléphone, adresse IP). * **Identité numérique** : Ensemble des traces laissées par une personne sur Internet, pouvant être volontairement publiées ou non (ex : comptes sur les réseaux sociaux, historique de navigation). * **Traitement de données personnelles** : Toute opération sur des données personnelles, telles que la collecte, le stockage, l’utilisation ou la suppression. * **RGPD** (Règlement Général sur la Protection des Données) : Règlement européen harmonisant la protection des données personnelles au sein de l’Union européenne. Il renforce les droits des individus sur leurs données, et introduit des sanctions significatives en cas de non-respect. * **Droit à l’oubli** : Droit pour une personne de demander l’effacement de ses données personnelles lorsque celles-ci ne sont plus nécessaires aux finalités pour lesquelles elles ont été collectées. * **Analyse d'impact relative à la protection des données (AIPD)** : Processus d’évaluation des risques que le traitement des données peut poser aux droits et libertés des personnes. * **Consentement explicite** : Accord clair et affirmatif donné par une personne pour le traitement de ses données personnelles, après avoir été informée de ses droits. Il doit être donné par une action positive (cocher une case, signer un formulaire), et non supposé par le silence ou l’inactivité. |

## La protection dans la sphère privée

**CONTEXTE JURIDIQUE ET RÔLE DE LA CNIL**

Avec l’évolution des technologies numériques, chaque action en ligne (comme envoyer un email, faire des achats en ligne, ou poster sur les réseaux sociaux) laisse des **traces numériques**. Ces traces, ou **données personnelles**, peuvent être collectées et analysées par des entreprises, souvent sans que les utilisateurs en soient pleinement conscients. C’est pourquoi des régulations strictes sont nécessaires pour encadrer ces pratiques et protéger les **droits fondamentaux** des individus, tels que le droit à la vie privée.

La **CNIL**, en tant qu’autorité de contrôle, est au cœur de ce dispositif. Créée par la loi Informatique et Libertés de 1978, son rôle a été renforcé par le **RGPD**. La CNIL a un double rôle : d’une part, informer et conseiller les entreprises et les particuliers sur leurs droits et obligations en matière de données personnelles ; d’autre part, contrôler et sanctionner les pratiques illégales, avec des amendes pouvant aller jusqu’à 20 millions d’euros ou 4% du chiffre d’affaires annuel mondial d’une entreprise.

**OBLIGATIONS DES ENTREPRISES SOUS LE RGPD**

Le **RGPD** a introduit un cadre juridique harmonisé dans toute l’Union européenne. Les entreprises, en tant que **responsables de traitement**, doivent se conformer à plusieurs obligations strictes :

* **Obligation de sécurité et de confidentialité** :
  + Les entreprises doivent mettre en œuvre des mesures techniques et organisationnelles pour garantir un niveau de sécurité adapté au risque. Cela peut inclure le **chiffrement** des données, des procédures strictes de gestion des accès, et des audits réguliers de sécurité. Par exemple, une entreprise qui stocke des données bancaires doit s'assurer que ces informations sont protégées par des méthodes de chiffrement avancées et que seuls les employés autorisés peuvent y accéder.
* **Obligation de minimisation des données** :
  + Le principe de **minimisation** exige que les entreprises ne collectent que les données strictement nécessaires pour atteindre l'objectif du traitement. Par exemple, pour l’inscription à une newsletter, il est généralement suffisant de demander une adresse email ; toute demande supplémentaire (comme l’adresse postale ou le numéro de téléphone) doit être justifiée par une raison légitime.
* **Obligation d'information** :
  + Les entreprises doivent fournir aux individus des informations claires et transparentes sur la manière dont leurs données seront utilisées, les finalités du traitement, la durée de conservation, et les droits dont ils disposent (accès, rectification, opposition, etc.). Par exemple, un site e-commerce doit expliquer sur sa page d’inscription comment les données des utilisateurs seront utilisées (pour l’envoi de newsletters, de promotions, etc.) et pendant combien de temps elles seront conservées.
* **Nomination d’un Délégué à la Protection des Données (DPO)** :
  + Les organisations, en particulier celles qui traitent des données sensibles ou en grandes quantités, sont tenues de désigner un **DPO**. Ce dernier a pour mission de veiller à la conformité avec le RGPD, de conseiller et former les employés, de mener des audits internes, et de servir d’interlocuteur avec la CNIL. Le DPO doit avoir une expertise en matière de droit et de pratiques concernant la protection des données, et il doit être indépendant dans l’exercice de ses fonctions.
* **Droit à la portabilité des données** :
  + Ce droit permet aux individus de récupérer les données personnelles qu’ils ont fournies à une entreprise, dans un format structuré, couramment utilisé et lisible par machine, et de les transférer à une autre entreprise. Par exemple, un utilisateur de services de streaming peut demander à ce que ses listes de lecture et ses préférences soient transférées à un autre fournisseur de services.

**LES DROITS DES PERSONNES CONCERNÉES**

Le **RGPD** a renforcé les droits des individus sur leurs données. Outre le **droit d’accès** (consulter les données que possède une entreprise sur eux) et le **droit de rectification** (corriger des données inexactes), le **droit à l’oubli** est particulièrement important. Il permet à une personne de demander la suppression de ses données dans des circonstances spécifiques, comme lorsque les données ne sont plus nécessaires ou que le consentement est retiré. Ce droit est essentiel dans un contexte où les informations personnelles circulent facilement sur le web, et où leur accumulation peut poser des risques pour la vie privée des individus.

## La protection dans la sphère professionnelle

**CONTEXTE JURIDIQUE ET SURVEILLANCE EN ENTREPRISE**

Dans le cadre professionnel, l'employeur dispose du droit de surveiller l’activité de ses salariés pour des raisons légitimes (par exemple, assurer la sécurité des biens ou vérifier le respect des horaires de travail). Cependant, ce droit est encadré par le **principe de proportionnalité** : les moyens de surveillance doivent être justifiés par la nature du travail et proportionnés à l’objectif poursuivi. Par exemple, un employeur peut installer des caméras de surveillance pour prévenir les vols, mais ces caméras ne doivent pas filmer les espaces réservés aux pauses des employés, car cela porterait atteinte à leur vie privée.

**OBLIGATIONS D'INFORMATION ET DE TRANSPARENCE**

L'employeur est tenu d'informer préalablement les salariés et leurs représentants (comme le comité social et économique, CSE) de tout dispositif de surveillance mis en place.

Cette information doit être claire, précise, et inclure des détails sur la finalité du dispositif, les modalités de fonctionnement, et les droits des salariés (droit d’accès aux données collectées, droit de rectification, etc.). Par exemple, si une entreprise installe un logiciel pour surveiller l'utilisation d'Internet par les employés, elle doit en informer clairement ces derniers et leur expliquer comment les données seront utilisées.

**REGISTRE DES ACTIVITÉS DE TRAITEMENT ET IMPLICATION DU DPO**

Les systèmes de contrôle et de surveillance doivent être inscrits dans le **registre des activités de traitement** tenu par l’employeur. Ce registre permet de garantir la transparence et la conformité avec la législation en vigueur. Si un DPO a été désigné, il doit être impliqué dans la mise en place et la surveillance de ces dispositifs, assurant ainsi que les droits des salariés sont respectés et que les traitements ne présentent pas de risques disproportionnés.

**EXEMPLES PRATIQUES :**

1. **Cas d'une entreprise qui utilise des caméras de surveillance** :
   * L'installation de caméras dans une entreprise doit être justifiée (par exemple, pour éviter les vols) et ne doit pas empiéter sur la vie privée des salariés (par exemple, les caméras ne doivent pas être placées dans les vestiaires). Avant leur installation, l’employeur doit consulter le CSE et informer les employés.
2. **Demande de suppression de données** :
   * Si un ancien employé demande la suppression de ses données personnelles, l’entreprise doit répondre à cette demande, sauf si elle a une obligation légale de conserver ces données (comme des documents relatifs à la paie pour des raisons fiscales).
3. **Utilisation de logiciels de surveillance informatique** :
   * L’employeur peut installer des logiciels pour surveiller l’utilisation des ordinateurs professionnels (par exemple, pour éviter les usages non autorisés d’Internet). Cependant, il doit informer les salariés à l’avance et s’assurer que les mesures prises sont proportionnées aux risques identifiés.

## Résumé

**A. Protection des données personnelles et CNIL : une régulation multifacette**

La **CNIL** veille au respect du **RGPD** en imposant aux entreprises et aux organisations une série d’obligations strictes, telles que la **minimisation des données**, le **consentement explicite** et la **sécurité** des informations traitées.

**Minimisation des données** : Ce principe fondamental exige que les entreprises ne collectent et ne traitent que les données strictement nécessaires à la finalité déclarée. La **CNIL** surveille de près le respect de ce principe, car toute dérogation peut conduire à une atteinte disproportionnée à la vie privée des individus.

**Consentement explicite** : La CNIL garantit que les entreprises obtiennent un consentement éclairé et explicite des personnes avant de traiter leurs données. Ici encore, la **CNIL** intervient pour s’assurer que les pratiques respectent cette exigence et pour sanctionner les infractions.

**Sécurité des données** : La **CNIL** impose aux entreprises de mettre en place des mesures techniques et organisationnelles pour protéger les données personnelles contre toute forme de perte, d’accès non autorisé, ou de divulgation. Cela inclut l’utilisation de technologies comme le chiffrement, ainsi que la mise en place de protocoles de gestion des incidents

**B. Application des obligations du RGPD dans le cadre professionnel**

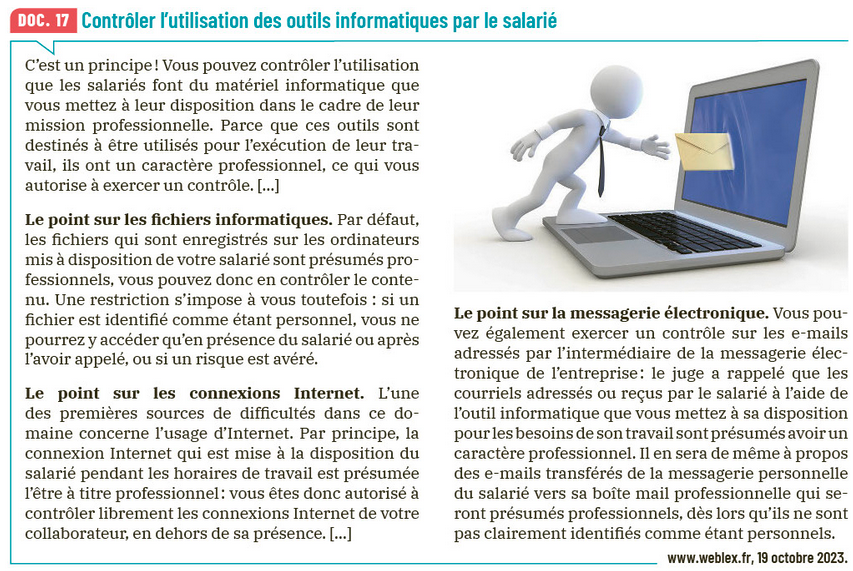
Dans la sphère professionnelle, les obligations imposées par le RGPD se traduisent par des pratiques de gestion des données et de surveillance qui doivent respecter les **droits des salariés**. Le **principe de proportionnalité** est ici crucial : les outils de surveillance et de contrôle mis en place par les employeurs doivent être justifiés par la nature de l’activité et proportionnés aux objectifs visés.

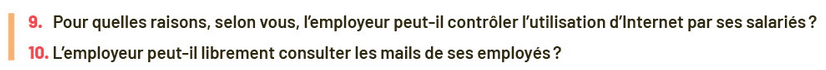
**Proportionnalité dans la surveillance** : Par exemple, l’installation de caméras de surveillance dans un entrepôt pour prévenir les vols peut être justifiée, mais l’employeur ne peut pas justifier la mise en place de caméras dans les salles de pause des employés, car cela constituerait une atteinte excessive à leur vie privée.

**Transparence et information** : Les employeurs sont également tenus d’informer les salariés et leurs représentants des dispositifs de surveillance mis en place, conformément à l’article L.1222-4 du Code du travail. Cette obligation de transparence permet aux salariés de connaître les modalités de surveillance et d’exercer leurs droits en conséquence, comme le droit d’accès aux données les concernant ou le droit de rectification.

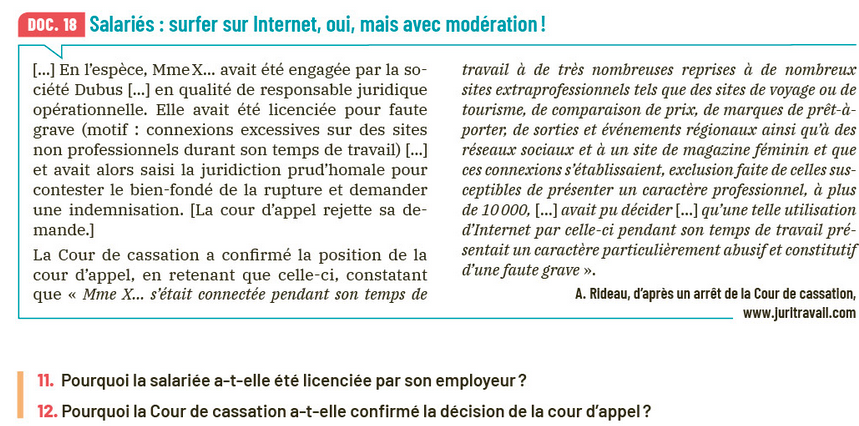
**Délégué à la Protection des Données (DPO)** : Le DPO est chargé de veiller à ce que les dispositifs de surveillance respectent les droits des salariés, de mener des analyses d’impact lorsque nécessaire, et de servir de point de contact avec la CNIL en cas de doute sur la légalité des pratiques de l’employeur.

## Exercice 1





## Exercice 2



## Exercice 3





