

Sensibilisation aux lois numériques

Support de cours pour la formation Sensibilisation aux lois numériques en
développement web de Décembre 2024

Formateur : Dufrène Valérian

“Déclaration d’activité enregistrée sous le numéro 32800232680 auprès du préfet de
région HAUTS-DE-FRANCE”

Objectifs

- Comprendre les enjeux juridiques du numérique en France.
- Identifier les principales lois encadrant l'utilisation des outils numériques.
- Apprendre à adopter des pratiques conformes et responsables.

Déroulé

- **Contexte et enjeux du cadre juridique numérique**
- **Les principales lois numériques françaises**
 - ◆ Loi Informatique et Libertés
 - ◆ RGPD (Règlement Général sur la Protection des Données)
 - ◆ Loi pour une République Numérique
 - ◆ Lois relatives à la cybersécurité
- **Responsabilités et droits des utilisateurs**
 - ◆ Respect de la vie privée et gestion des données personnelles
 - ◆ Cyberharcèlement et contenus illicites
 - ◆ Propriété intellectuelle et droits d'auteur
- **Bonnes pratiques numériques**
 - ◆ Adopter une posture éthique en ligne
 - ◆ Prévenir les risques (phishing, cyberattaques, etc.)
 - ◆ Sensibilisation au respect de la législation dans un contexte professionnel
- QCM

Contexte et enjeux du cadre juridique numérique

Pourquoi des lois numériques ?

- Explosion des usages digitaux : réseaux sociaux, e-commerce, données personnelles.
- Prolifération des cybermenaces (fraudes, hameçonnage, ransomwares).
- Besoin de protéger les individus et les entreprises.

Les grands principes du droit numérique :

- **Protection des données personnelles** : garantir la vie privée des citoyens.
- **Responsabilité juridique** : encadrer les comportements en ligne.
- **Sécurité numérique** : prévenir les cyberattaques.
- **Accessibilité et neutralité du web** : favoriser un accès égal au numérique.

Les principales lois numériques françaises

Loi Informatique et Libertés (1978, amendée en 2018)

- **Objectif** : Protéger les citoyens contre les abus liés au traitement des données personnelles.
- **Principes clés** :
 - ◆ Consentement pour la collecte des données.
 - ◆ Droit d'accès, de rectification et de suppression.
 - ◆ Régulation par la [CNIL](#) (Commission Nationale de l'Informatique et des Libertés).
- **Source** : <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>

RGPD (2018)

- **Portée** : Règlement européen applicable en France.
- **Obligations** :
 - ◆ Transparence dans l'utilisation des données.
 - ◆ Désignation d'un DPO (Délégué à la Protection des Données) dans certaines organisations.
 - ◆ Signalement des violations de données dans les 72 heures.
- **Sanctions** : Amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du CA mondial.
 - ◆ **Exemple concret** : En 2020, une entreprise française a été condamnée à une amende de 250 000 € pour avoir stocké des données bancaires sans protection suffisante, ce qui a exposé ses clients à des fraudes potentielles.
- **Source** : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

Loi pour une République Numérique (2016)

- **Objectifs** :
 - ◆ Encourager l'innovation numérique.
 - ◆ Renforcer la transparence administrative.
 - ◆ Améliorer la gestion des données publiques.
- **Points clés** :
 - ◆ Accès aux données publiques ([open data](#)).
 - ◆ [Droit à l'oubli pour les mineurs](#).
 - ◆ [Portabilité des données](#).
- **Source** : https://www.economie.gouv.fr/files/files/PDF/DP_LoiNumerique.pdf

Lois relatives à la cybersécurité

→ **Loi de Programmation Militaire (2019)** : obligation de sécuriser les systèmes d'information critiques.

◆ **Source** : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028338825>

→ **Règles sur la notification des incidents de sécurité (ANSSI).**

◆ **Exemple concret** : En 2021, un pirate informatique ayant diffusé un ransomware sur une application bancaire a été arrêté. L'attaque avait provoqué une paralysie temporaire des services, entraînant une perte financière estimée à plusieurs millions d'euros pour l'entreprise.

◆ **Source** : <https://cyber.gouv.fr/notifications-reglementaires>

Responsabilités et droits des utilisateurs

Respect de la vie privée

→ Importance de la confidentialité dans les interactions en ligne.

→ Droits des utilisateurs : refuser le suivi (cookies), demander l'effacement de leurs données.

Cyberharcèlement et contenus illicites

→ **Définition** : agissements malveillants visant une personne sur une plateforme numérique.

→ **Sanctions** : peines d'amende et d'emprisonnement en fonction de la gravité.

→ **Signalement** : plateformes dédiées ([Pharos](#), [e-Enfance](#)).

Propriété intellectuelle

→ Règles :

- ◆ Respect des [droits d'auteur](#).
- ◆ Interdiction de la reproduction sans autorisation.

→ Exemples d'infraction : partage illégal de films, logiciels piratés, applications piratées.

- ◆ **Exemple concret** : En 2019, une plateforme de streaming illégale a été condamnée à une amende de 100 000 € pour diffusion sans autorisation de contenus protégés par le droit d'auteur.

Bonnes pratiques numériques

Adopter une posture éthique

- Éviter les [contenus diffamatoires ou mensongers](#).
- Respecter les différences d'opinion.

Prévenir les risques

- Reconnaître les [tentatives de phishing](#).
- Utiliser des mots de passe complexes et uniques.
- Mettre à jour régulièrement ses logiciels.

Environnement professionnel

- **Sensibilisation interne** : création de [chartes d'utilisation des outils numériques](#).
- **Responsabilité des employeurs** : conformité à la RGPD pour les données clients et employés.

QCM (10 questions, une réponse par question)

<https://forms.gle/JpxUuiS6TYXpw4FCA>

- 1. Quel organisme est chargé de veiller à l'application de la loi Informatique et Libertés en France ?**
 - a. L'ANSSI
 - b. Le Conseil d'État
 - c. La CNIL
 - d. L'ARCEP

- 2. Selon la RGPD, quel est le délai pour notifier une violation de données à la CNIL ?**
 - a. 24 heures
 - b. 72 heures
 - c. Une semaine
 - d. Un mois

- 3. Quelle est la sanction maximale prévue par le RGPD pour une violation grave ?**
 - a. 50 000 euros
 - b. 2 % du chiffre d'affaires mondial
 - c. 4 % du chiffre d'affaires mondial ou 20 millions d'euros
 - d. Une suspension temporaire des activités

- 4. Quel droit est garanti par la loi pour une République Numérique aux mineurs ?**
 - a. Droit à la portabilité des données
 - b. Droit à l'oubli
 - c. Droit de rectification des données
 - d. Droit de refuser les cookies

5. **Que signifie l'acronyme ANSSI ?**
- a. Association Nationale pour la Sécurité Systématique et Informatique
 - b. Agence Nationale de la Sécurité des Systèmes d'Information
 - c. Autorité Nationale de la Sécurité des Sites Internet
 - d. Administration Nationale des Standards et de l'Informatique
6. **Quel est l'objectif principal des lois relatives à la cybersécurité en France ?**
- a. Augmenter les taxes sur les entreprises technologiques
 - b. Assurer la protection des systèmes d'information critiques
 - c. Encourager le développement des logiciels libres
 - d. Imposer des certifications pour les utilisateurs d'Internet
7. **En cas de cyberharcèlement, quel outil officiel permet de signaler les contenus illicites en ligne ?**
- a. e-Enfance
 - b. Pharos
 - c. CyberSecFrance
 - d. AntiHarcèlement.fr
8. **Quel exemple constitue une violation de la propriété intellectuelle ?**
- a. Publier une photo prise soi-même sur un réseau social
 - b. Partager une vidéo sous licence Creative Commons
 - c. Diffuser un film protégé par le droit d'auteur sans autorisation
 - d. Acheter un logiciel payant en ligne
9. **Quel est le risque principal d'utiliser un mot de passe faible ?**
- a. Une amende par la CNIL
 - b. Une perte de performance de l'ordinateur
 - c. Une vulnérabilité accrue face au piratage
 - d. Une désactivation automatique du compte

10. Quel est l'avantage principal d'adopter une posture éthique en ligne ?

- a. Éviter tout risque de poursuite judiciaire
- b. Améliorer sa réputation et contribuer à un environnement numérique sûr
- c. Obtenir un certificat d'éthique numérique
- d. Réduire ses impôts