RÉPUBLIQUE TUNISIENNE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DE MONASTIR
Institut Supérieur d'Informatique
et de Mathématiques de Monastir

Droit d'informatique, protection des données et éthiques

Enseignante: Wejdene Allali Ammar

AU: 2025/2026

Auditoires: L2_INFO

Introduction générale:

- Dans notre société numérique, la protection des données personnelles est devenue un enjeu majeur. Chaque jour, nous générons d'énormes quantités de données, que ce soit en naviguant sur Internet, en utilisant des applications mobiles ou en partageant des informations en ligne. Ces "traces numériques" – nom, adresse e-mail, préférences, etc. sont précieuses et nécessitent une protection adéquate.
- Cette nécessité a donné naissance au droit de l'informatique, un domaine juridique qui encadre les activités liées aux technologies de l'information et de la communication (TIC).
- Il couvre notamment la protection des données personnelles, la sécurité des systèmes d'information, le commerce électronique et la propriété intellectuelle dans le domaine numérique.

- Pourquoi est-il si crucial de protéger nos données ? Sans une protection adéquate, nos informations peuvent être utilisées à notre insu, entraînant des conséquences graves telles que le vol d'identité, la fraude, la discrimination ou des atteintes à notre réputation.
- En Tunisie, la protection des données personnelles est formalisée par la loi organique n° 63 du 27 juillet 2004 , qui établit les principes fondamentaux pour le traitement des données personnelles. Cette loi s'inscrit dans un cadre constitutionnel plus large, l'article 24 de la Constitution Tunisienne affirmant que "l'État protège la vie privée.
- Le droit de l'informatique aura double objectifs respectifs d'une part il doit assurer l'intégrité des données personnelles à l'occasion de toutes opérations numériques et d'autre part il doit assurer une protection de la propriété intellectuelle à propos de toute innovation ou invention technologique en matière de l'informatique.
- Ces doubles préoccupations feront l'objet de ces cours.
- Chapitre1: éthiques, données personnelles et principes fondamentaux .
- Chapitre2: le cadre règlementaires normatif et institutionnel de la protection des données.
- Chapitre 3: protection de la propriété intellectuelle dans l'environnement numérique.

Section 1ère : Approche conceptuelle: éthiques et données personnelle

I. **La définition de l'éthique informatique:**

Le concept éthique est ambigu. Il recouvre à la fois une attitude, un comportement relevant de la responsabilité individuelle et les mœurs. Il s'agit d'un ensemble des principes moraux qui sont à la base de la conduite de quelqu'un (définition Larousse). L'éthique se situe en amont des normes morales et des lois. Elle vise donc à réfléchir au comportement de l'individu et à l'adapter en fonction de valeurs que l'on juge essentielles. Elle s'éloigne en cela du droit, dont les règles s'imposent par peur de la sanction en cas de violation.

On trouve que les choix éthiques de l'individu dépendent de lui-même et aussi de la communauté (la société) à laquelle il appartient; c.à.d. « l'entité » qui peut être réduite à une organisation ou un ensemble d'individu exerçant un travail commun d'où la notion « des éthiques appliquées ».

Exemple: « éthique médicale, éthique informatique… »

L'éthique informatique est une branche de l'éthique appliquée qui traite de la façon dont les usages et les professionnels de l'informatique font un usage de l'information et prennent des décisions au regard des critères éthiques.

Exemple: - protéger soi-même (adopter un logiciel antivirus).
- protéger et respecter les autres.
- respecter l'environnement.

II. Les données personnelles:

les données personnelles se définissent comme toute information se rapportant à une personne physique identifiée ou identifiable. En d'autre termes il s'agit de toute information permettant d'identifier, directement ou indirectement un individu (article 4 de la loi organique n° 63 du 27 juillet 2004 relative à la protection des données personnelles).

Ces données incluent des informations évidentes comme:

-Nom et prénom: informations basiques d'identification.

- Adresse e-mail: Moyen de communication souvent lié à des comptes numérique.

- N° de téléphone: permet d'identifier et de contacter une personne.

- Adresse IP: chaque appareil connecté à Internet dispose d'une adresse unique qui peut être utilisée pour localiser un utilisateur.

- Données de localisation: les lieux visités via un smartphone ou une application GPS.
- Préférences et comportement en ligne: les habitudes d'achats, les interactions sur les réseaux sociaux ou les historiques de navigation.

➡ Les données personnelles peuvent être classées en différentes catégories en fonction de leur sensibilité:

1) données d'identification se sont les informations standards permettant d'identifier une personne (nom, adresse CIN …)

2) données financières (n° compte bancaire, carte crédit …)

3) données de santé: état de santé, maladie et les dossiers médicaux
 elles doivent être bien protégées.

4) données sensibles: l'origine raciale ou ethniques, opinions politiques, les conviction religieuses ou philosophiques , la vie sexuelle ou les orientations sexuelles d'une personne.
 Ces données nécessitent une protection particulière car leur divulgation peut entrainer des discriminations ou des préjudices graves.

5) données interdites: certaines données sont interdites de traitement, sauf dans des cas exceptionnels.
Exp: les condamnations pénales…

Section 2: Les principes fondamentaux de la protection des données personnelles:

- Pour protéger efficacement les données personnelles il est essentiel de mettre en œuvre trois principes fondamentaux:

1) **La confidentialité:** s'assurer que seules les personnes autorisées ont accès aux données personnelles. Cela implique la mise en place de mesures de sécurité rigoureuse pour empêcher tout accès non autorisé. Les mesures courantes:
   + système de contrôle d'accès: utilisation des mots de passe robustes…
   + gestion stricte des droits d'accès: Attribution de droits d'accès spécifiques en fonction des rôles et des responsabilités de chaque utilisateur au sein de l'entreprise.

2) **L'intégrité:** s'assurer que les données sont justes et vraies et qu'elle n'ont pas été modifiées ou supprimées sans autorisation par erreur ou par quelqu'un n'ayant pas le droit de le faire.

➡ Si les informations sont fausses cela peut causer des problèmes, il est important de vérifier régulièrement les informations (contrôle des bases des données) protéger les données contre les modifications non autorisées, faire des copies de sauvegarde.

➡ Assure l'intégrité de D.P.

3) **La disponibilité:** s'assurer que les D.P sont accessibles aux utilisateurs autorisés lorsqu'en ont besoin. Alors à la fin d'y garantir des mesures doivent être mises en place:

- Sauvegardes régulières : effectuer des copies de sauvegarde des données à intervalles réguliers pour pouvoir les restaurer en cas de perte de corruption.
- Systèmes robustes contres les interruptions comme système de sécurité pour prévenir les attaques informatiques.

- La protection des D.P est essentielle pour garantir le respect de la vie privée de chaque individu dans notre société numérique. En effet, l'art 1er de loi 27/07/2004 déclare que: toute personne a le droit à la protection des données à caractère personnel relatif à sa vie privée.

➡ La protection des D.P est l'un des moyens concret de mettre en œuvre le droit au respect de la vie privée dans le contexte numérique. En effet, chaque individu a le droit de contrôler ses informations personnelles et empêcher toute divulgation non autorisée ce qui peut entrainer des violations à la vie privée et donc engager la responsabilité juridique.