Exercice 1 :

Dissertation :

Le paradoxe de Byung-Chul Han : La quête de transparence numérique entre en tension avec le droit à l'intimité fait référence au besoin permanent et constant des utilisateurs de pouvoir voir tout ce qui passe ou est présent dans l'espace et parallèlement leur besoin permanent de garder leur intimité et données personnelles hors de la portée de tous. De ce fait est-il réellement possible de pouvoir obtenir la transparence numérique tout cherchant la privatisation de ses données personnelles ?

I. Les atouts et la nécessité de la transparence numérique

1. **Un gage de confiance et de démocratie**
    - Les citoyens réclament la transparence des institutions et des dirigeants : publication des budgets, lutte contre la corruption, accès aux données publiques.
    - La transparence numérique favorise la responsabilité et le contrôle citoyen.
2. **Un outil d'efficacité et de progrès**
    - L'open data et le partage d'informations permettent des avancées dans la recherche, la santé ou l'innovation technologique.
    - La transparence dans les entreprises (traçabilité des produits, éthique numérique) améliore la confiance des consommateurs.
3. **Une arme contre la criminalité et les abus**
    - Les technologies de surveillance et de traçage numérique aident la police judiciaire à lutter contre la cybercriminalité, le terrorisme ou les fraudes.
    - Les réseaux sociaux révèlent certains abus qui seraient restés invisibles.

II. Les risques et les atteintes au droit à l'intimité

1. **L'exposition excessive des individus**
    - Les réseaux sociaux poussent à partager sa vie privée, créant une vulnérabilité face au harcèlement, au vol de données ou à l'usurpation d'identité.
    - La recherche permanente de transparence mène parfois à une perte du "jardin secret" de chacun.
2. **La surveillance généralisée**
    - Les États ou entreprises collectent et stockent d'immenses quantités de données personnelles (Big Data, traçage GPS, caméras intelligentes).

- Cela entraîne une forme de contrôle social permanent, contraire aux libertés individuelles.

3. **Le paradoxe de la transparence**
    - Si tout doit être transparent, l'individu perd son droit fondamental à l'intimité.
    - La quête d'une société totalement transparente peut glisser vers une forme de **"dictature numérique"** où chacun est observé en permanence.

Conclusion

La quête de la transparence numérique est une valeur moderne qui favorise la démocratie, la sécurité et l'innovation. Cependant, elle ne peut s'imposer sans limites, car elle menace un droit essentiel : l'intimité de la vie privée. Le véritable défi de nos sociétés est donc de trouver un équilibre entre ces deux pôles. La transparence doit être appliquée principalement aux institutions, aux entreprises et aux espaces publics, tandis que le respect de la sphère privée des individus doit rester protégé par des lois strictes (comme le RGPD en Europe).
En définitive, une société libre et juste ne peut exister que si elle concilie **la clarté des actions collectives** et **la préservation du secret individuel**.

2-

Exemple concret : cas d'un smartphone saisi lors d'une enquête criminelle

Un suspect est arrêté dans le cadre d'une enquête sur un réseau de cybercriminalité. La police judiciaire saisit son **smartphone personnel**, considéré comme une source potentielle de preuves (messages, photos, contacts, historique de navigation, géolocalisation).

La quête de transparence numérique de transparence se manifeste ici par :

Les enquêteurs qui ont besoin d'**accéder à l'ensemble des données** du téléphone pour établir la vérité.

Car cela permet de :

- Prouver la participation du suspect au réseau criminel,
- Retracer les échanges avec ses complices,
- Localiser les lieux fréquentés grâce aux données GPS,
- Identifier d'éventuelles victimes.

Le droit à l'intimité se manifeste ici par :

Le smartphone contient aussi des **informations strictement privées** : photos personnelles, conversations intimes, documents médicaux.

Ces données n'ont **aucun lien avec l'enquête**, mais elles risquent d'être vues par les enquêteurs

3-

Comme solutions Kantiennes à ce paradoxe, je peux proposer :

A- Principe de finalité humaine

- Les données numériques ne doivent être exploitées que dans la mesure où cela **respecte la dignité de la personne**.
- Autrement dit, l'investigation doit viser la **justice** sans transformer l'individu en objet d'investigation totale.

B- Universalisation de la règle

- Avant de fouiller un appareil numérique, l'enquêteur devrait se demander : *"Serait-il acceptable que cette règle d'investigation s'applique à tous, y compris à moi-même ?"*
- Cela évite les abus, car une surveillance sans limites ne pourrait pas être universalisée sans créer une société oppressive.

C- Encadrement moral et juridique

- Seules les données **strictement pertinentes** pour l'enquête doivent être examinées.
- Les informations intimes non liées à l'affaire doivent être protégées par un principe d'**intégrité morale** : elles ne sont pas un simple outil de preuve, mais une partie de la personne qui mérite respect.

Exercice 2 :

1-

Conception de l'être chez Heidegger

Heidegger analyse l'**être humain** comme un **Dasein** (*être-là*) : l'homme est toujours déjà **dans le monde**, engagé dans un contexte, dans des relations et dans un temps.

Le Dasein est caractérisé par :

- **L'ouverture au monde** (il comprend son existence à travers les choses et les autres).
- **La temporalité** (l'être est toujours projeté vers le futur, marqué par la finitude et la mort).

Adaptation numérique :

Le Dasein connecté

- Aujourd'hui, l'homme est un *être-au-monde-numérique*.
- Il est « jeté » dans un environnement technologique fait de réseaux sociaux, d'algorithmes, de données massives.
- Son existence se déploie aussi bien dans l'espace physique que dans le **cyberspace**.

Temporalité numérique

Le temps vécu par le Dasein est bouleversé :

- **Instantanéité** (notifications, flux permanents d'informations).
- **Mémoire numérique infinie** (les traces laissées en ligne rendent le passé toujours présent).

Cela peut renforcer l'angoisse de la finitude ou, au contraire, créer l'illusion d'une immortalité numérique (profils posthumes, archives éternelles).

2-

Qu'entend-on par « être-par-la-trace » ?

- Dans la philosophie contemporaine du numérique, l'**être-par-la-trace** désigne la manière dont l'existence humaine est médiatisée par les **empreintes numériques** que nous laissons : publications, photos, likes, historiques, géolocalisation, etc.
- L'individu **n'existe pas seulement en présence physique**, mais aussi à travers les **traces qu'il dépose en ligne**, qui continuent d'agir même en son absence.

Étude d'un profil social complet (exemple fictif)

Prenons le cas d'**Amina**, étudiante de 24 ans, très active sur Instagram, LinkedIn et TikTok :

- **Instagram** : elle publie des photos de ses voyages, de ses sorties, de ses repas, et partage des "stories" quotidiennes.
- **LinkedIn** : elle expose son parcours académique, ses stages, ses compétences en informatique.
- **TikTok** : elle poste des vidéos humoristiques et suit des tendances virales.
- **Traces invisibles** : historiques de navigation, commentaires laissés, localisation GPS enregistrée par son smartphone.

Analyse philosophique : être-par-la-trace

a) Une existence délocalisée

- Amina **existe au-delà de son corps** : son profil est visible et actif même lorsqu'elle dort ou qu'elle n'est pas connectée.
- Ses traces numériques assurent une **présence continue dans le monde social numérique**, indépendante de sa présence physique.

b) Une identité fragmentée et façonnée

- Sur LinkedIn, elle apparaît comme une professionnelle sérieuse.
- Sur TikTok, elle est perçue comme drôle et légère.
- Sur Instagram, elle se met en scène dans un style de vie "idéal".

3-

Transformation ontologique : de l'être-présent à l'être-par-la-trace

Traditionnellement, la preuve légale reposait sur des **faits matériels et tangibles** (témoignages, documents signés, empreintes physiques, objets saisis).
Or, dans l'ère numérique, l'individu se manifeste et existe aussi **par ses traces numériques** (messages, géolocalisations, métadonnées, historiques).

Nouvelles possibilités offertes par la trace numérique

- **Multiplication des indices** : chaque action en ligne laisse une trace (clic, connexion, transaction).
- **Fiabilité technique** : une métadonnée peut établir avec précision la date, l'heure et le lieu d'une action.
- **Reconstruction des faits** : la chronologie numérique (logs, SMS, emails) permet de reconstituer des événements avec une exactitude parfois supérieure aux témoignages humains.

Fragilisation et nouveaux défis pour la preuve

Cependant, cette transformation entraîne aussi des **risques majeurs** :

1. **Surabondance des preuves**
    - Trop de traces disponibles → difficulté de sélection, risque d'atteinte à la vie privée.
    - Le juge doit déterminer quelles traces sont **pertinentes et recevables**.
2. **Manipulabilité des traces**
    - Contrairement à une empreinte physique, une trace numérique peut être **effacée, falsifiée, créée artificiellement**.

- Cela soulève des problèmes d'**authenticité et d'intégrité**.