Devoir Investigations Numériques

Nom : MINYANDA YONGUI JOSÉ LOÏC

Matricule : 22P071

CIN-4

Exercice 1

Dissertation (≈ 500 mots) : Le paradoxe de la transparence

La société numérique contemporaine valorise la transparence comme un idéal : gouvernements, institutions et plateformes affirment que plus de transparence conduit à plus de démocratie, de responsabilité et de confiance. Cependant, Byung-Chul Han montre que cette transparence généralisée engendre une nouvelle forme de violence subtile : elle supprime l'opacité nécessaire à l'intimité et transforme la vie privée en marchandise.

Le paradoxe de la transparence consiste à constater que, bien qu'elle promette égalité et vérité, elle aboutit à une exposition permanente qui détruit la confiance elle-même. En effet, une relation humaine fondée uniquement sur la transparence absolue devient invivable, car l'homme a besoin de zones de retrait pour préserver sa liberté intérieure et sa créativité.

Dans le champ de l'investigation numérique, ce paradoxe se manifeste clairement. L'investigateur a pour mission de rechercher la vérité, ce qui suppose collecte et analyse de données, mais il doit en même temps protéger la dignité et l'intimité des personnes. Par exemple, lors d'une enquête sur la corruption, il est nécessaire de collecter des courriels et métadonnées. Ces données révèlent la vérité sur les faits, mais dévoilent aussi la vie privée de personnes tierces n'ayant aucun lien avec l'affaire. La quête de transparence produit donc une atteinte collatérale à l'intimité.

Pour résoudre ce paradoxe, l'éthique kantienne peut être mobilisée. Kant affirme que l'homme doit toujours être considéré comme une fin en soi, et jamais seulement comme un moyen. Transposé à l'investigation numérique, cela signifie que la recherche de vérité ne doit pas instrumentaliser la personne ni exposer inutilement son intimité.

Une proposition pratique est donc d'appliquer :

1. L'anonymisation par défaut : publier les preuves en masquant les informations personnelles non pertinentes.

2. La minimisation des données : collecter seulement ce qui est strictement nécessaire et proportionné à l'affaire.

3. La justification éthique : lorsqu'une donnée intime est exploitée, documenter la raison et l'intérêt public de cette utilisation.

4. Un contrôle indépendant : soumettre la diffusion de preuves sensibles à une instance d'arbitrage éthique.

Ainsi, l'investigation numérique peut concilier transparence et respect de la vie privée. La vérité est recherchée et révélée, mais sans détruire l'intimité qui fait partie intégrante de la dignité humaine.

Exercice 2

Transformation ontologique et lecture d'un profil social

Chez Heidegger, la technique n'est pas seulement un outil mais une manière de dévoiler le monde. Dans le contexte numérique, l'homme devient un « être-par-la-trace » : son identité se construit à travers les traces numériques qu'il laisse (publications, métadonnées, interactions).

Un profil social peut donc être lu comme un ensemble de traces constituant une ontologie :

- Les publications expriment les intentions.
- Les métadonnées révèlent le contexte temporel et spatial.
- Les interactions montrent le réseau de relations et de significations.

Pour l'investigation numérique, cette lecture implique que la preuve n'est plus seulement matérielle mais aussi immatérielle et volatile. La validité d'une preuve dépend alors de la conservation des traces numériques, de l'authenticité des métadonnées et de la confiance dans la chaîne technique (hash, signature, horodatage).

Exercice 3

Script Python de calcul d'entropie + règle pratique

```
import sys, math

from collections import Counter


def entropie_fichier(path):

   with open(path, "rb") as f:

      data = f.read()
```

```
    if not data:
        return 0.0
    counts = Counter(data)
    n = len(data)
    H = 0
    for c in counts.values():
        p = c / n
        H -= p * math.log2(p)
    return H

if _name_ == "_main_":
    print(entropie_fichier("fichier_exemple"))
```

Règle pratique :

- Texte naturel : entropie basse (≈1,5 bits).
- Image JPEG : entropie moyenne (≈7 bits).
- Fichier chiffré : entropie proche de 8 bits.

→ Si H ≥ 7,6 bits/octet, il est probable que le fichier soit chiffré.

Exercice 4

Algorithme pour détecter les nœuds critiques dans un graphe de communications

1. Représenter chaque numéro de téléphone comme un nœud.
2. Ajouter une arête entre deux nœuds pour chaque appel.
3. Attribuer un poids (nombre ou durée d'appels).
4. Calculer les mesures de centralité : degré, intermédiarité, proximité.
5. Identifier les nœuds à forte centralité d'intermédiarité → ce sont les intermédiaires critiques.
6. Visualiser le graphe en dimension 2 ou 3 pour interpréter les clusters.

Exercice 5

Effet papillon et estimation d'un exposant de Lyapunov

- On dispose de 1000 événements corrélés.
- Une petite perturbation (±30 s sur un timestamp) se propage dans la chronologie.
- Méthode : comparer la séquence originale et la séquence modifiée ; calculer à chaque étape la différence cumulative.
- Approximer la croissance : $\delta(t) \approx \delta(0)\, e^{\{\lambda t\}}$.
- Par régression linéaire de $\ln(\delta(t)/\delta(0))$ en fonction de t, on estime λ.
- Exemple simplifié : si la différence double tous les 5 événements, alors $\lambda \approx (\ln 2)/5 \approx 0{,}1386$.

Exercice 6

Analogie du chat de Schrödinger appliquée au numérique

Un fichier chiffré dont la clé est incertaine est à la fois accessible et inaccessible tant qu'il n'a pas été « observé ».

→ Oui, il existe une forme de « superposition numérique ».

Impact juridique : la preuve devient probabiliste, dépendant de l'acte d'observation.

Protocole pour minimiser l'effet :

- Horodater et hasher le fichier avant toute manipulation.
- Conserver un journal des opérations.
- Effectuer les mesures de façon séquentielle et contrôlée par un tiers indépendant.

Exercice 7

Calculs sur la sphère de Bloch ($\theta=\pi/3$, $\phi=\pi/4$)

État :

$|\psi\rangle = \cos(\pi/6)|0\rangle + e^{i\pi/4}\sin(\pi/6)|1\rangle$

$\cos(\pi/6) = \sqrt{3}/2 \rightarrow P(0) = (\sqrt{3}/2)^2 = 0{,}75$

$\sin(\pi/6) = 1/2 \rightarrow P(1) = (1/2)^2 = 0{,}25$

Probabilités de mesure :

- $P(|0\rangle) = 0{,}75$
- $P(|1\rangle) = 0{,}25$

Exercice 8

Théorème de non-clonage et conséquences forensiques

- Le théorème de non-clonage affirme qu'il est impossible de copier parfaitement un état quantique inconnu.
- Conséquence : on ne peut pas dupliquer une preuve quantique pour l'examiner plusieurs fois.
- L'investigation doit donc se baser sur protocoles d'observation prudents et accepter une marge d'incertitude.

Exercice 9

Formalisation numérique de l'inégalité $A(P)\cdot C(P) \leq 1-\delta$

Exemple :

- Système A : A=0,9 ; C=0,4 → produit = 0,36 (≤ 0,9 si δ=0,1).
- Système B : A=0,6 ; C=0,95 → produit = 0,57.
- Système C : A=0,95 ; C=0,1 → produit = 0,095.

Méthode : mesurer expérimentalement les incertitudes ΔA et ΔC ; vérifier que $\Delta A \cdot \Delta C \geq \hbar num/2$.

Exercice 10

Proof-of-concept Python pour un protocole ZK-NR

```
import hashlib, secrets

def commit(msg):
```

```
    salt = secrets.token_bytes(16)
    c = hashlib.sha256(salt+msg.encode()).hexdigest()
    return c, salt

def prove(salt, msg, challenge):
    return hashlib.sha256(salt+msg.encode()+challenge).hexdigest()

msg = "preuve confidentielle"
c, s = commit(msg)
ch = secrets.token_bytes(16)
resp = prove(s, msg, ch)
print("Commitment:", c)
print("Response:", resp)
```

Ce code illustre comment prouver la possession d’une information sans la révéler directement.