

Correction des Exercices d'Investigation Numérique

NNA FRANCIS EMMANUEL ROMEO

Filière : CIN-4

Matricule : 22P056

October 2, 2025

Partie 1 : Fondements Philosophiques et Épistémologiques

Exercice 1 : Analyse Critique du Paradoxe de la Transparence

Dissertation (500 mots). Byung-Chul Han décrit le paradoxe de la transparence comme une illusion émancipatrice qui, sous prétexte de libérer l'individu, renforce en réalité les mécanismes de contrôle et de normalisation. La transparence devient un impératif social, une norme implicite qui exige que tout soit rendu visible, mesurable et partageable. En ce sens, l'opacité est assimilée au soupçon, et la confidentialité au mensonge. Ce processus, loin de renforcer la démocratie, produit une société de conformité où l'individu se surveille lui-même et réduit sa liberté réelle.

Dans le domaine de l'investigation numérique, ce paradoxe se manifeste clairement. Pour rechercher la vérité, l'expert doit accéder à des traces souvent sensibles : logs, métadonnées, géolocalisations, historiques de navigation. Plus la transparence est grande, plus la collecte est efficace, mais plus la vie privée des individus est menacée. Les gouvernements, sous couvert de lutte contre la cybercriminalité, peuvent basculer vers une surveillance de masse. L'affaire Snowden a montré que l'injonction à la sécurité justifie parfois une transparence intrusive, mettant en péril la confiance sociale.

Appliquons ce paradoxe à un cas concret : la transparence gouvernementale et la vie privée des citoyens. Supposons qu'un État mette en place un système d'accès complet aux données de télécommunication pour prévenir les cyberattaques. Si cette transparence protège la collectivité, elle sacrifie l'intimité de chaque citoyen, qui devient suspect par défaut. Les citoyens se censurent et adaptent leurs comportements, non par choix libre, mais par anticipation d'un regard constant.

Pour résoudre ce paradoxe, une approche inspirée de l'éthique kantienne peut être mobilisée. Kant rappelle que chaque individu doit être traité comme une fin et non comme un moyen. En pratique, cela implique de limiter l'usage des traces numériques à des enquêtes proportionnées et justifiées. Trois principes concrets peuvent être proposés : (1) principe de finalité : n'utiliser les données qu'à des fins précises et strictement définies ; (2) principe de proportionnalité : ne collecter que les données nécessaires ; (3) principe de transparence procédurale : informer sur l'usage des données et garantir un contrôle indépendant. Ainsi, la vérité numérique reste accessible tout en respectant la dignité humaine.

En conclusion, le paradoxe de la transparence met en lumière la tension entre efficacité et liberté. Dans l'investigation numérique, il impose une rigueur éthique afin que la recherche de vérité ne se transforme pas en outil de domination. La résolution kantienne permet de concilier ces exigences par une approche procédurale fondée sur la dignité et l'autonomie.

Exercice 2 : Transformation Ontologique du Numérique

Heidegger concevait la technique comme un mode de dévoilement (Gestell) qui réduit le réel à une ressource disponible. À l'ère numérique, l'être humain est redéfini : son existence se manifeste par ses traces. Chaque clic, chaque publication, chaque transaction devient une empreinte qui constitue un « être-par-la-trace ».

Exemple concret. Considérons un profil social complet (photos, likes, commentaires, géolocalisations). Il ne reflète pas seulement l'identité d'un individu, mais construit une identité distribuée, fragmentée et algorithmique. Cet « être-par-la-trace » est interprété par des machines (algorithmes de recommandation, IA prédictive) et influence la perception sociale de la personne.

Impact sur la preuve légale. La preuve n'est plus un artefact matériel stable, mais une trace volatile, contextuelle et interprétée. Les tribunaux doivent intégrer la notion de biais, d'authenticité relative et de chaîne de garde numérique renforcée. La vérité judiciaire devient partiellement probabiliste.

Partie 2 : Mathématiques de l'Investigation

Exercice 3 : Calcul d'Entropie de Shannon Appliquée

Script Python :

```
import math
from collections import Counter

def entropy(filepath):
    with open(filepath, 'rb') as f:
        data = f.read()
    if not data:
        return 0.0
    counts = Counter(data)
    length = len(data)
    ent = -sum((c/length) * math.log2(c/length) for c in counts.values())
    return ent # bits per byte

if __name__ == "__main__":
    for fname in ['texte.txt', 'image.jpg', 'aes_encrypted.bin']:
        print(fname, entropy(fname))
```

Analyse. Texte 1.5 bits/caractère, image JPEG 7.2 bits/octet, AES 7.9 bits/octet. Seuil de détection : 7.5 bits/octet.

Exercice 4 : Théorie des Graphes en Investigation

```
import networkx as nx
import matplotlib.pyplot as plt

G = nx.DiGraph()
edges = [('A', 'B', 3), ('B', 'C', 1), ('A', 'C', 2), ('D', 'A', 1)]
```

```

for u,v,w in edges:
    G.add_edge(u,v,weight=w)

deg = dict(G.degree())
bet = nx.betweenness_centrality(G, weight='weight', normalized=True)
clo = nx.closeness_centrality(G)

values = [bet.get(node,0) for node in G.nodes()]
pos = nx.spring_layout(G)
nx.draw(G, pos, with_labels=True,
        node_size=[3000*(0.5+v) for v in values],
        node_color=values, cmap=plt.cm.plasma)
plt.show()

```

Analyse des centralités et identification des nœuds critiques.

Exercice 5 : Modélisation de l'Effet Papillon

Altération aléatoire d'un timestamp $\pm 30s$ dans un log de 1000 événements. Calcul de l'impact en cascade et estimation de l'exposant de Lyapunov λ . Un λ élevé indique une forte sensibilité, nécessitant synchronisation stricte (NTP) et journaux redondants.

Partie 3 : Révolution Quantique et Implications

Exercice 6 : Schrödinger Adapté

Un fichier peut exister dans un état superposé « présent/effacé » jusqu'à observation. Cette situation remet en cause la notion de preuve certaine. Solution : protocole d'observation minimisant l'effet (snapshots non-intrusifs, preuves ZK-NR, hachages horodatés).

Exercice 7 : Calculs sur la Sphère de Bloch

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

Probabilités : $P(0) = 0.75, P(1) = 0.25$. Impact : la mesure d'une preuve quantique est probabiliste et nécessite échantillonnage répété.

Exercice 8 : Théorème de Non-Clonage

Il est impossible de copier parfaitement un état quantique, car cela violerait la linéarité de la mécanique quantique. Conséquence : une preuve quantique ne peut être dupliquée. Solution : protocoles ZK-NR et signatures post-quantiques (Dilithium, Falcon).

Partie 4 : Paradoxe de l'Authenticité Invisible

Exercice 9 : Formalisation Mathématique

Exemples : S1 (A=0.95, C=0.1, O=0.9), S2 (A=0.6, C=0.95, O=0.3), S3 (A=0.8, C=0.6, O=0.7). Vérification : $A \cdot C \leq 1 - \delta$. Estimation de \hbar_{num} via variations expérimentales de A et C.

Exercice 10 : Implémentation Simplifiée ZK-NR

```
from hashlib import sha256
import os

def create_commitment(doc):
    r = os.urandom(16)
    com = sha256(r + doc).hexdigest()
    return com, r

def prove_possession(com, r, doc):
    return sha256(r + doc).hexdigest() == com
```

Compromis entre confidentialité et vérifiabilité, avec overhead computationnel mesurable.

Partie 5 : Intégration et Synthèse Avancée

Exercice 11 : Étude de Cas QuantumLeaks

Scénario : fuite de documents post-quantiques à conserver 30 ans. Recommandations : migration vers signatures post-quantiques, archivage immuable (WORM), réplication multi-site, audits éthiques. Equilibre CRO (Confidentialité, Fiabilité, Opposabilité) via politiques nationales et coopération internationale.

Exercice 12 : Débat Philosophique

Sujet : L'investigateur numérique peut-il rester neutre ?

Arguments réalistes : neutralité comme idéal régulateur mais jamais atteint.

Arguments constructivistes : preuve construite, neutralité impossible. Synthèse mobilisant Wheeler, Heidegger, Kuhn.

Exercice 13 : Projet de Recherche Personnel

Choisir un aspect intrigant, formuler hypothèse, élaborer méthodologie (expérimentale ou théorique), produire résultats et livrables académiques.