RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
****
DÉPARTEMENT DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****
UNIVERSITY OF YAOUNDE I
****
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
****
DEPARTMENT OF COMPUTER ENGINEERING
****

EXERCICES

Philosophie et Fondements de l'Investigation Numérique

Option :

Cybersécurité et Investigation Numérique

Rédigé par :
BAALAWE LIONEL JOSSELIN, *24P822*

Sous l'encadrement de :
Expert Thierry MINKA

Année académique 2025 / 2026

Le paradoxe de la transparence selon Byung-Chul Han

Introduction

À l'ère numérique, la transparence est devenue une valeur centrale des sociétés contemporaines. Gouvernements, entreprises et individus sont incités à rendre visibles leurs actions, leurs données et même leurs émotions. Le philosophe germano-coréen **Byung-Chul Han** analyse cette exigence comme un paradoxe : plus nous cherchons la transparence, plus nous fragilisons la confiance et l'intimité. L'investigation numérique, discipline qui cherche la vérité dans l'espace digital, se situe précisément au cœur de cette tension entre visibilité totale et respect de la vie privée. Comment comprendre ce paradoxe, et quelles solutions peut-on envisager pour le dépasser ?

Historiquement, la transparence est associée à des valeurs positives : elle garantit la reddition des comptes, réduit l'arbitraire du pouvoir et renforce la démocratie. Dans le monde numérique, elle est également perçue comme une condition de sécurité : plus d'informations partagées équivalent à une meilleure traçabilité des actions, donc à une meilleure justice. Ainsi, la surveillance algorithmique, les bases de données publiques et les technologies de traçage sont présentées comme des instruments de vérité.

Cependant, Byung-Chul Han met en garde contre une telle absolutisation. Selon lui, la transparence ne libère pas toujours : elle peut aussi devenir une forme de contrainte sociale, voire un nouvel outil de domination. Quand tout doit être visible et mesurable, l'espace de l'intime se réduit drastiquement.

Le paradoxe soulevé par Byung-Chul Han réside dans l'idée que **l'excès de transparence détruit la confiance qu'elle est censée renforcer**.

— **Érosion de l'intimité** : plus les individus sont exposés à travers leurs données (messages privés, historiques de navigation, géolocalisation), plus ils perdent la maîtrise de leur identité numérique. Or, la confiance suppose un espace de secret et de vulnérabilité ; sans opacité, il n'y a plus de véritable relation humaine.

— **Multiplication des vérités** : à force de produire une transparence totale, on génère en réalité une confusion. Les informations brutes, sorties de leur contexte, peuvent être manipulées ou interprétées différemment, ce qui alimente la désinformation.

— **Surveillance et auto-censure** : une société de transparence permanente se rapproche d'une société de contrôle. L'individu, conscient d'être observé, adapte ses comportements, réduit sa liberté d'expression et se conforme à une norme implicite.

Ainsi, la quête de transparence, censée protéger, aboutit paradoxalement à un climat de méfiance et de contrôle généralisé.

Face à ce paradoxe, il ne s'agit pas de rejeter la transparence mais de la réinscrire dans un cadre éthique. Inspiré de la philosophie kantienne, un compromis est envisageable :

— **Transparence proportionnée** : elle doit s'appliquer en priorité aux institutions publiques, garantes de l'intérêt général, et non s'imposer indistinctement à tous les citoyens.

— **Protection de l'intimité** : un droit fondamental à l'opacité doit être reconnu, permettant à chacun de préserver une sphère privée hors de la surveillance numérique.

— **Chaînes de confiance numériques** : plutôt que de tout rendre visible, il convient de mettre en place des protocoles cryptographiques garantissant la vérifiabilité sans divulgation totale (ex. preuves à divulgation nulle de connaissance, ZK-proofs).

Ces approches permettent de réconcilier vérité et intimité, transparence et liberté.

Conclusion

Le paradoxe de la transparence identifié par Byung-Chul Han révèle une tension fondamentale de la société numérique : la volonté de tout rendre visible peut finir par anéantir la confiance, l'intimité et même la vérité qu'elle prétend protéger. L'investigation numérique doit donc évoluer vers un modèle qui conjugue rigueur, proportionnalité et respect de la sphère privée. La véritable éthique du numérique n'est pas une transparence absolue, mais une transparence encadrée, orientée vers la justice et respectueuse de la dignité humaine.

Application du paradoxe de la transparence à un cas concret

Cas concret : transparence gouvernementale vs. vie privée des citoyens

Imaginons une enquête numérique menée par un gouvernement pour lutter contre la corruption dans l'attribution des marchés publics. Dans un souci de transparence, toutes les transactions financières des ministères, des entreprises sous-traitantes et même des individus impliqués (fonctionnaires, entrepreneurs) sont publiées sur une plateforme en libre accès.

— **Aspect positif** : la transparence favorise la reddition des comptes. Les citoyens, journalistes et associations peuvent contrôler directement l'usage de l'argent public. Elle réduit le risque de dissimulation et de manipulation comptable.

— **Aspect négatif** : cette transparence peut empiéter sur la vie privée. Par exemple, si les salaires des agents publics ou les données personnelles des entrepreneurs (adresses, comptes bancaires, dépenses personnelles liées aux marchés) sont rendus visibles, cela crée une exposition excessive et parfois injustifiée.

Ainsi, le paradoxe de Byung-Chul Han apparaît clairement : la transparence, censée renforcer la confiance, engendre une perte d'intimité, des risques d'atteintes à la dignité et même un climat de méfiance généralisée.

Résolution inspirée de l'éthique kantienne

L'éthique kantienne repose sur l'*impératif catégorique* :

> « Agis uniquement d'après la maxime qui fait que tu peux vouloir en même temps qu'elle devienne une loi universelle. »

Appliqué à ce cas :

1. **Respect de la dignité humaine** : la transparence ne doit pas transformer les citoyens ou les fonctionnaires en simples « objets d'observation ». Ils doivent toujours être considérés comme des fins en soi, non comme de simples moyens de contrôle.
2. **Universalisation** : une politique de transparence qui exposerait totalement la vie privée de tous ne pourrait pas être universalisée sans nuire à la liberté humaine. En revanche, rendre publiques uniquement les données pertinentes aux fonds publics (contrats, montants, bénéficiaires institutionnels) est universalisable et conforme à l'impératif moral.
3. **Proportionnalité et séparation des sphères** : la transparence doit s'appliquer principalement aux institutions et à l'usage des fonds collectifs, et non aux sphères privées des individus. Les données personnelles doivent rester protégées, sauf nécessité strictement démontrée par l'enquête.

Synthèse

Une résolution pratique inspirée de Kant consisterait à :

— Publier toutes les informations liées aux marchés publics (contrats, budgets, prestataires) pour garantir la transparence institutionnelle.

— Protéger les données personnelles des individus impliqués (comptes privés, vie familiale, localisation), car elles relèvent de la dignité humaine.

— Mettre en place des mécanismes techniques (cryptographie, pseudonymisation) permettant de vérifier la régularité des transactions sans exposer inutilement les personnes.

Ainsi, on trouve un équilibre entre **transparence démocratique** et **respect de la vie privée**, fidèle à la logique kantienne où la vérité et la justice ne doivent jamais se faire au détriment de la dignité humaine.

Transformation ontologique du numérique

A — Comparaison : la conception de l'être chez Heidegger vs adaptation à l'ère numérique

Heidegger, dans *Être et Temps*, place l'être au centre de la question philosophique en insistant sur le *Dasein* : l'être-là humain qui se comprend dans ses possibilités, son souci, son rapport au monde et aux autres. Deux traits essentiels se dégagent :

— **Temporalité** : l'existence est structurée par le temps (projet, retentissement, passé/avenir).

— **Mise-en-œuvre (Gestell)** : la technique n'est pas neutre ; elle révèle le monde comme « disponibilité » (*standing-reserve*) et modifie la manière dont les choses et les humains se laissent rencontrer.

À l'ère numérique, ces traits prennent de nouvelles formes :

— **Multiplicité temporo-spatiale** : l'« être » n'est plus uniquement incarné et temporellement linéaire ; il est doublé par des traces persistantes et réplicables (profils, journaux, copies dans le cloud). La temporalité devient superposée (instantané vs archivage indéfini).

— **Révélation numérique** : la technique digitale révèle le monde en données et en métriques. Comme chez Heidegger, la technique façonne ce qui apparaît, mais ici l'humain lui-même est révélé comme profil exploitable (métriques comportementales, scores).

— **Aliénation et dispersion** : le Dasein centré est désormais distribué ; l'identité est fragmentée entre plusieurs plateformes, rôles et traces.

En bref, Heidegger nous aide à voir que la technique reconfigure la modalité d'être ; le numérique transforme l'être en un « être-par-la-trace », un mode d'existence fondé sur la visibilité, la persistance et la quantification.

B — Étude d'un profil social complet comme manifestation d'« être-par-la-trace »

Considérons un profil social type : photos, publications, *likes*, historiques de localisation, interactions, métadonnées (horodatages, appareils), ainsi que données liées (achats, contacts). Ce profil constitue :

— **Indexation de l'existence** : chaque interaction laisse une marque corrélée à des états, préférences et relations. L'individu « existe » aussi par ces marques.

— **Persona performatif** : le profil ne reflète pas seulement l'individu, il le façonne (comportements anticipés, publicités ciblées, modélisations prédictives).

— **Archivage et persistance** : contrairement à l'oralité fugace, la trace numérique perdure, permettant des reconstitutions futures (historique judiciaire, réputation sociale).

Analyse : Le profil social devient une « ontologie secondaire » — il n'est pas qu'un miroir mais un acteur. Les algorithmes recommandent, les institutions évaluent. L'*être-par-la-trace* signifie que l'identité est co-construite par les technologies qui la produisent, la mesurent et la redistribuent.

C — Impact sur la notion de preuve légale

La transformation ontologique entraîne plusieurs conséquences pour la preuve numérique :

— **Nature immatérielle et volatile** : la preuve n'est plus un objet tangible mais un agrégat de traces numériques (bits, journaux) susceptibles d'altération, suppression ou falsification.

— **Contextualisation nécessaire** : une trace isolée a peu de valeur ; la chaîne de contexte (métadonnées, provenance, horodatage, intégrité) devient cruciale pour l'admissibilité judiciaire.

— **Preuves probabilistes** : l'archétype de la preuve certaine s'affaiblit ; on raisonne en probabilités (corrélations, scores de confiance) plutôt qu'en certitudes absolues.

— **Authenticité et opposabilité** : qui a généré la trace et dans quelles conditions ? Les mécanismes cryptographiques (horodatage signé, hachage, journaux immuables) deviennent essentiels pour garantir authenticité et non-répudiation.

— **Éthique et droits** : l'usage des traces pose un problème de proportionnalité et de respect de la vie privée ; l'acquisition massive de données peut violer des droits fondamentaux et invalider une preuve malgré sa valeur factuelle.

Exercice 3 : Calcul d'Entropie de Shannon Appliquée

L'entropie de Shannon mesure l'imprévisibilité d'un fichier :

$$H(X) = -\sum_i p(x_i) \log_2 p(x_i)$$

où $p(x_i)$ est la probabilité d'apparition du symbole x_i.

Objectif : comparer trois types de fichiers (texte, image JPEG, fichier chiffré AES). Résultats attendus :

— Texte naturel : $H \approx 1.5$ bits/caractère

— Image JPEG : $H \approx 7.0$–7.5 bits/octet

— Fichier AES : $H \approx 7.9$–8.0 bits/octet

Seuil de détection de chiffrement automatique : $H > 7.5$.

```python
import math
from collections import Counter

def shannon_entropy(data: bytes) -> float:
    if not data:
        return 0
    freq = Counter(data)
    n = len(data)
    return -sum((count/n) * math.log2(count/n) for count in freq.values())

files = {
    "Texte": "document.txt",
    "JPEG": "image.jpeg",
    "AES": "fichier_chiffre.aes"
}

for name, path in files.items():
    with open(path, "rb") as f:
        data = f.read()
    H = shannon_entropy(data)
    print(f"{name}: H     {H:.2f} bits/octet")
```

Listing 1 – Calcul d'entropie de Shannon en Python

—

Exercice 4 : Théorie des Graphes en Investigation Criminelle

On modélise un réseau de communications téléphoniques par un graphe orienté :

— Sommets = personnes

— Arêtes = appels téléphoniques

Les métriques utilisées : centralité en degré, intermédiarité, proximité. L'algorithme de Freeman permet d'identifier le **nœud critique**.

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

communications = [
    ("Alice", "Bob"),
    ("Bob", "Charlie"),
    ("Alice", "Charlie"),
    ("Charlie", "David"),
    ("David", "Alice"),
    ("Eve", "Alice"),
    ("Eve", "Charlie"),
]

G = nx.DiGraph()
G.add_edges_from(communications)

deg_centrality = nx.degree_centrality(G)
bet_centrality = nx.betweenness_centrality(G)
closeness = nx.closeness_centrality(G)

critical_node = max(bet_centrality, key=bet_centrality.get)

print("Noeud critique (Freeman):", critical_node)

plt.figure(figsize=(6,6))
node_colors = [deg_centrality[n]*10 for n in G.nodes()]
nx.draw(G, with_labels=True, node_size=1500,
        node_color=node_colors, cmap=plt.cm.plasma)
plt.show()
```

Listing 2 – Analyse de graphes en Python avec NetworkX

—

Exercice 5 : Modélisation de l'Effet Papillon en Forensique

Une petite modification dans un log ($\pm$30s) peut entraîner un effet en cascade sur la reconstruction d'une timeline. La divergence est mesurée par l'exposant de Lyapunov λ :

$$\delta(t) \approx \delta(0)e^{\lambda t}$$

```python
import numpy as np
import matplotlib.pyplot as plt

np.random.seed(42)
n = 1000
timestamps = np.cumsum(np.random.exponential(scale=5, size=n))

idx = np.random.randint(0, n)
perturbation = np.random.choice([-30, 30])
timestamps_perturbed = timestamps.copy()
timestamps_perturbed[idx] += perturbation

delta = np.abs(timestamps - timestamps_perturbed)
lyapunov = np.mean(np.log(1 + delta))
```

```
15
16 plt.plot(delta[:200], label="Diff rence cumul e")
17 plt.xlabel("   vnement   ")
18 plt.ylabel("Divergence temporelle (s)")
19 plt.title("Effet papillon en reconstruction forensique")
20 plt.legend()
21 plt.show()
22
23 print(f"Exposant de Lyapunov effectif     {lyapunov:.3f}")
```

Listing 3 – Simulation de l'effet papillon en Python

—

Exercice 6 : Expérience de Pensée de Schrödinger Adaptée

On conçoit une version numérique du chat de Schrödinger : un fichier peut être dans un état « présent » ou « effacé », mais avant l'analyse, l'investigateur ignore sa réalité. On peut modéliser son état par une superposition :

$$|\Psi\rangle = \alpha|Présent\rangle + \beta|Effacé\rangle.$$

Impact sur la preuve

— La preuve devient **probabiliste** et non certaine.

— Les juges devront accepter des preuves accompagnées d'un **intervalle de confiance**.

Protocole d'observation minimal-invasif

1. Utiliser des snapshots immuables en lecture seule.
2. Calculer immédiatement des hachages et les signer.
3. Journaliser toutes les opérations avec horodatage.
4. Minimiser les lectures directes en utilisant des attestations cryptographiques.

—

Exercice 7 : Calculs sur la Sphère de Bloch

État donné :

$$|\psi\rangle = \cos\frac{\pi}{6}|0\rangle + e^{i\pi/4}\sin\frac{\pi}{6}|1\rangle = \tfrac{\sqrt{3}}{2}|0\rangle + \tfrac{1}{2}e^{i\pi/4}|1\rangle.$$

Probabilités de mesure

$$P(0) = \left|\tfrac{\sqrt{3}}{2}\right|^2 = 0.75, \quad P(1) = \left|\tfrac{1}{2}\right|^2 = 0.25.$$

Coordonnées Bloch

$$(x, y, z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) = (0.612,\ 0.612,\ 0.5).$$

Code de visualisation

```python
import numpy as np
import matplotlib.pyplot as plt

theta = np.pi/3
phi = np.pi/4
x = np.sin(theta)*np.cos(phi)
y = np.sin(theta)*np.sin(phi)
z = np.cos(theta)

fig = plt.figure()
ax = fig.add_subplot(111, projection='3d')
u, v = np.mgrid[0:2*np.pi:100j, 0:np.pi:50j]
xs = np.cos(u)*np.sin(v)
ys = np.sin(u)*np.sin(v)
zs = np.cos(v)
ax.plot_surface(xs, ys, zs, alpha=0.1)
ax.scatter([x],[y],[z],s=80,c='r')
plt.show()
```

Listing 4 – Représentation d'un état sur la sphère de Bloch

—

Exercice 8 : Analyse du Théorème de Non-Clonage

Pourquoi le clonage est impossible

Supposons un opérateur U tel que :

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle.$$

En comparant deux états non orthogonaux, on obtient :

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2,$$

ce qui est absurde sauf si $\langle\psi|\phi\rangle \in \{0, 1\}$.

Conséquences forensiques

— Impossibilité de copier parfaitement une preuve quantique.

— Obligation d'utiliser des engagements et horodatages classiques pour garantir l'opposabilité.

Alternative ZK-NR

1. Créer un engagement cryptographique (hash).
2. Produire une preuve Zero-Knowledge.
3. Signer l'engagement pour la non-répudiation.

—

Exercice 9 : Formalisation du Paradoxe de l'Authenticité Invisible

On définit : A (authenticité), C (confidentialité), O (opposabilité). Inégalité fondamentale :

$$A \cdot C \leq 1 - \delta.$$

Exemple numérique :

— Système public signé : $A = 0.95,\ C = 0.05 \Rightarrow \delta \approx 0.95$.

— Système chiffré non signé : $A = 0.6,\ C = 0.7 \Rightarrow \delta \approx 0.58$.

— Système ZK-NR : $A = 0.85,\ C = 0.6 \Rightarrow \delta \approx 0.49$.

Inégalité d'incertitude :

$$\Delta A \cdot \Delta C \geq \frac{\hbar_{num}}{2}.$$

—

Exercice 10 : Implémentation Simplifiée ZK-NR

```python
import hashlib, time
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import rsa, padding

def commit(data, nonce):
    return hashlib.sha256(nonce + data).hexdigest()

def gen_keys():
    priv = rsa.generate_private_key(public_exponent=65537, key_size=2048)
    return priv, priv.public_key()

def sign(priv, msg):
    return priv.sign(msg,
        padding.PSS(mgf=padding.MGF1(hashes.SHA256()),
                    salt_length=padding.PSS.MAX_LENGTH),
        hashes.SHA256())

def verify(pub, sig, msg):
    try:
        pub.verify(sig, msg,
            padding.PSS(mgf=padding.MGF1(hashes.SHA256()),
                        salt_length=padding.PSS.MAX_LENGTH),
            hashes.SHA256())
        return True
    except Exception:
        return False

# Exemple
data = b"secret doc"
nonce = b"random123"
C = commit(data, nonce).encode()
priv, pub = gen_keys()
sig = sign(priv, C)
print("Commit:", C.decode())
```

```
print("Signature valide?", verify(pub, sig, C))
```

Listing 5 – Prototype pédagogique de ZK-NR en Python

—

Exercice 11 : Étude de Cas — QuantumLeaks

Scénario : fuite de documents classifiés protégés par chiffrement post-quantique. Preuves à conserver pour plus de 30 ans.

Stratégie

1. **Acquisition immédiate** : image bit-à-bit, stockage en WORM.
2. **Engagement post-quantique** : signatures PQC (Dilithium, Falcon).
3. **Stockage redondant** : migration cryptographique planifiée.
4. **Documentation** : journaux signés, TPM, certificats.
5. **Accès contrôlé** : workflow légal, pseudonymisation partielle.

Exercice 12 : Débat Philosophique Structuré

Sujet

« L'investigateur numérique peut-il rester neutre dans l'ère quantique ? »

Introduction

L'ère quantique, caractérisée par l'incertitude fondamentale et l'impossibilité du clonage parfait, remet en cause la neutralité supposée de l'investigateur numérique. Deux approches se confrontent : le réalisme et le constructivisme.

Position réaliste

— Inspirée de Wheeler (*it from bit*), la réalité existe indépendamment de l'observateur.

— L'investigateur a pour rôle de révéler les faits de manière objective, en rapportant des probabilités mesurables.

— La neutralité est donc possible : l'investigateur n'est qu'un témoin des probabilités quantiques.

— **Trilemme éthique :** priorité donnée à la vérité (Vérité > Vie privée > Responsabilité sociale).

Position constructiviste

— Avec Heidegger, la technique est un mode de dévoilement : l'investigation n'est jamais neutre.

— Avec Kuhn, l'interprétation des traces dépend de paradigmes conceptuels (outils, modèles juridiques).

— La neutralité est impossible : l'investigateur choisit ce qu'il observe et construit la réalité de l'enquête.

— **Trilemme éthique :** priorité donnée à la dignité humaine et à la protection des droits fondamentaux.

Synthèse

Une approche intégrative admet :

— la nécessité d'outils rigoureux et de méthodes reproductibles (réalisme),

— mais aussi la dimension située et contextuelle de l'observation (constructivisme).

L'investigateur est « neutre en intention » mais « situé en pratique ».

Conclusion

Dans l'ère quantique, la neutralité absolue est un idéal régulateur, non une réalité empirique. L'investigateur doit reconnaître sa position située et arbitrer le trilemme éthique entre vérité, responsabilité et respect des droits.

—

Exercice 13 : Projet de Recherche Personnel

Thème choisi

La fiabilité des preuves probabilistes issues de systèmes quantiques dans les procès judiciaires.

Hypothèse de recherche

Les preuves numériques quantiques, bien que probabilistes, peuvent être juridiquement fiables si elles sont accompagnées de mécanismes d'attestation et de redondance statistique.

Protocole expérimental

1. **Simulation théorique :** modélisation d'un qubit mesuré dans différents états.
2. **Expérimentation numérique :** génération de séries de mesures avec bruit (simulateur quantique).
3. **Analyse statistique :** calcul des intervalles de confiance selon le nombre de mesures (théorème de Hoeffding).
4. **Traduction juridique :** formalisation des résultats en termes de seuils de confiance présentables en justice.

Résultats attendus

— Détermination d'un nombre minimal de mesures pour rendre une preuve statistiquement acceptable.

— Définition d'un cadre d'admissibilité probabiliste adapté aux tribunaux.

Plan d'article académique

1. **Introduction :** enjeux de la preuve quantique en contexte judiciaire.
2. **Cadre théorique :** Wheeler, incertitude de Heisenberg, non-clonage.
3. **Méthodologie :** simulation et protocoles statistiques.
4. **Résultats :** seuils de mesures et niveaux de confiance.
5. **Discussion :** implications juridiques et éthiques.
6. **Conclusion :** vers un standard de preuve quantique.

—