

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE  
YAOUNDE

Département : Génie Informatique  
Filière : Cybersécurité et Investigation Numérique  
Classe : Niveau 4  
Année académique : 2025/2026

---

DEVOIR D'INVESTIGATION  
NUMERIQUE : Chapitre 1

---

Nom de l'étudiant : MELONE André Vladmir

Matricule : 22P059

# Table des matières

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Partie 1 : Fondements Philosophiques et Épistémologiques</b>  | <b>2</b> |
| 1.1      | Exercice : Analyse Critique du Paradoxe de la Transparence . . . . .   | 2        |
| 1.1.1    | —> Dissertation de sur le paradoxe identifié par Byung-Chul Han . . . . .  | 2        |
| 1.1.2    | —> Application de ce paradoxe à un cas concret d’investigation (ex :<br>balance entre transparence gouvernementale et vie privée des citoyens) . . . | 2        |
| 1.1.3    | —> Proposition de résolution pratique inspirée de l’éthique kantienne . . .  | 2        |
| 1.2      | Transformation Ontologique du Numérique . . . . .  | 3        |
| 1.2.1    | —> Comparaison de la conception de l’être chez Heidegger et son adap-<br>tation à l’ère numérique . . . . .  | 3        |
| 1.2.2    | —>Étude d’un profil social complet et analyse comme manifestation d’«<br>être-par-la-trace » . . . . .   | 3        |
| 1.2.3    | —>impact cette transformation ontologique sur la notion de preuve légale ?   | 3        |
| <b>2</b> | <b>Partie 2 : Mathématiques de l’Investigation</b>   | <b>4</b> |
| 2.1      | Calcul d’Entropie de Shannon Appliquée . . . . .   | 4        |
| 2.2      | Théorie des Graphes en Investigation Criminelle . . . . .  | 4        |
| <b>3</b> | <b>Revolution Quantique et Ses Implications</b>  | <b>4</b> |
| 3.1      | Expérience de Pensée Schrödinger Adaptée . . . . .   | 4        |
| 3.2      | Analyse du Théorème de Non-Clonage . . . . .   | 5        |
| <b>4</b> | <b>Paradoxe de l’Authenticité Invisible</b>  | <b>5</b> |

# 1 Partie 1 : Fondements Philosophiques et Épistémologiques

## 1.1 Exercice : Analyse Critique du Paradoxe de la Transparence

### 1.1.1 —> Dissertation de sur le paradoxe identifié par Byung-Chul Han

A l'ère où les TIC prennent de plus en plus de place dans notre vie, la transparence est devenue d'autant plus cruciale. Chacun voudrait justement savoir comment sont gérées ses données par les grandes entreprises qui détiennent nos données personnelles. Les Etats exigent de ce fait aux entreprises de montrer les détails du processus de gestions des données personnelles de leurs utilisateurs. Toutefois, cette quête absolue de visibilité s'accompagne d'un paradoxe fondamental : Si tout est visible alors il y'a moins d'intimité et de confidentialité ce qui favorise une surveillance permanente des sujets. C'est dans ce sens que Byung Chul Han soulève le paradoxe de la transparence qui cherche a trouver un bon milieu entre le besoin de transparence et le besoin de préserver sa vie privée.

Selon Han, la transparence excessive transforme les individus en objets observables et mesurables, ce qui réduit l'espace de liberté et de retrait nécessaire à l'épanouissement personnel. Alors que la transparence est censée protéger contre les abus et renforcer la confiance, elle peut paradoxalement engendrer une forme de contrôle social et psychologique insidieux. Les données personnelles deviennent des instruments de pouvoir, utilisés non seulement pour la sécurité ou l'efficacité des services, mais aussi pour influencer les comportements et limiter l'autonomie des individus. Ainsi, le paradoxe réside dans le fait que la transparence absolue, loin d'être uniquement bénéfique, comporte des effets négatifs sur l'intimité et la liberté. Byung-Chul Han invite à une réflexion sur la nécessité de frontières claires entre ce qui doit être transparent et ce qui doit rester privé. Il propose que la société numérique recherche une transparence sélective et éthique, permettant à la fois une information suffisante pour garantir la responsabilité des acteurs et un espace de confidentialité protégeant la dignité et l'autonomie des individus.

En conclusion, le paradoxe de la transparence souligne que la quête d'ouverture et de visibilité ne peut se faire au détriment de la vie privée. Il s'agit d'un équilibre délicat entre connaissance et confidentialité, entre contrôle et liberté, qui reste un défi majeur à l'ère du numérique.

### 1.1.2 —> Application de ce paradoxe à un cas concret d'investigation (ex : balance entre transparence gouvernementale et vie privée des citoyens)

D'un côté, les gouvernements et institutions exigent une plus grande transparence des données pour garantir la sécurité nationale, lutter contre la cybercriminalité et prévenir le terrorisme. Cela se traduit par la collecte massive de données, la surveillance des communications ou encore l'obligation faite aux entreprises de fournir des informations sur leurs utilisateurs. **Dans ce sens, la transparence est présentée comme une nécessité pour assurer la confiance et protéger les citoyens.** D'un autre côté, cette transparence se transforme en instrument de contrôle social. **Les citoyens, en exposant leurs données personnelles, deviennent eux-mêmes des objets de surveillance.** Ainsi, ce qui devait renforcer la liberté risque de l'affaiblir.

### 1.1.3 —> Proposition de résolution pratique inspirée de l'éthique kantienne

Pour résoudre ce dilemme, l'éthique kantienne peut offrir une orientation précieuse. Selon Kant, chaque individu doit être traité comme une fin en soi et jamais uniquement comme un moyen pour atteindre un objectif. Appliqué au contexte numérique et gouvernemental, cela implique que la collecte et l'usage des données doivent respecter la dignité et l'autonomie des citoyens. Les mesures de transparence ne doivent pas instrumentaliser les individus pour la sécurité ou le contrôle social, mais viser leur protection réelle et leur participation éclairée.

Concrètement, cela se traduit par plusieurs principes :

- La **limitation de la collecte** aux données strictement nécessaires, afin de ne pas traiter les citoyens uniquement comme des sources d'information.
- La **consentement éclairé** : les individus doivent être informés de manière claire et compréhensible sur la façon dont leurs données seront utilisées.
- La **responsabilité et transparence éthique** des gouvernements et institutions, qui doivent justifier leurs actions et garantir que la sécurité ne se fasse pas au détriment de la dignité humaine.

Ainsi, l'éthique kantienne permet de concilier la transparence nécessaire à la protection collective avec le respect fondamental de la vie privée, en faisant de chaque citoyen un sujet et non un objet de surveillance. Cette approche favorise une transparence réfléchie et éthique, où sécurité et liberté coexistent.

## 1.2 Transformation Ontologique du Numérique

### 1.2.1 —> Comparaison de la conception de l'être chez Heidegger et son adaptation à l'ère numérique

Chez Heidegger, l'être humain, ou Dasein, se définit par sa présence dans le monde, ses actions et ses relations avec autrui. Chaque action laisse des traces paroles, écrits, interactions qui témoignent de son existence. Ainsi, l'être est conçu comme un « être-par-la-trace », dont la réalité se manifeste à travers les effets produits dans le monde. À l'ère numérique, cette conception se transforme : l'individu se manifeste désormais largement par des traces immatérielles telles que les publications, messages, historiques de navigation ou fichiers partagés. L'existence devient en partie définie par ces manifestations digitales, illustrant un « être-par-la-trace numérique » où l'identité se construit à travers la corrélation de ces traces plutôt que par la seule présence physique.

### 1.2.2 —> Étude d'un profil social complet et analyse comme manifestation d'« être-par-la-trace »

Un profil social complet, comprenant publications, likes, partages, photos, vidéos et historiques de connexion, constitue une projection de l'existence numérique de l'individu. Chaque élément du profil est une trace de ses choix, de ses interactions et de sa présence temporelle et géographique. Ainsi, analyser un tel profil revient à observer l'être numérique à travers ses manifestations, chaque donnée révélant une facette de l'existence de la personne. L'accumulation et la corrélation de ces traces permettent de reconstruire un portrait cohérent du Dasein numérique, où l'existence est matérialisée non pas par la présence physique mais par les effets et empreintes laissés sur les systèmes numériques.

### 1.2.3 —> impact cette transformation ontologique sur la notion de preuve légale ?

La transformation de l'être vers un état numérique a un impact significatif sur la notion de preuve légale. Les traces numériques, profils, logs, messages, fichiers deviennent des preuves primaires, reflétant l'existence et les actions de l'individu. Cependant, elles sont fragiles et facilement altérables, ce qui nécessite des méthodes strictes pour garantir l'authenticité et l'intégrité de la preuve, telles que le hashing, l'horodatage, les copies bit-à-bit et les procédures forensiques. Cette évolution oblige la justice à adapter ses pratiques, car l'existence distribuée par la trace numérique devient un élément central pour établir la preuve, rendant la notion traditionnelle de preuve « certaine » plus complexe à appliquer dans le contexte numérique.

## 2 Partie 2 : Mathematiques de l'Investigation

### 2.1 Calcul d'Entropie de Shannon Appliquée

Le script utilisé est le suivant :

```
C:\> Users > Vladimir M > Desktop > ACADEMIE DEV ST VLAD > Travaux Investigation numerique > entropie > entropie.py > ...
1 import os
2 import math
3 from collections import Counter
4
5 def calcul_entropie(fichier):
6     """Calcule l'entropie de Shannon d'un fichier donné."""
7     with open(fichier, "rb") as f:
8         data = f.read()
9
10    if len(data) == 0:
11        return 0 # éviter division par zéro
12
13    freq = Counter(data)
14    taille = len(data)
15    entropie = -sum((count/taille) * math.log2(count/taille) for count in freq.values())
16    return entropie
17
18 # Utiliser automatiquement le dossier où se trouve le script
19 dossier = os.path.dirname(os.path.abspath(__file__))
20
21 print(f"\nEntropies des fichiers dans le dossier : {dossier}\n")
22
23 for nom_fichier in os.listdir(dossier):
24     chemin_fichier = os.path.join(dossier, nom_fichier)
25     if os.path.isfile(chemin_fichier):
26         ent = calcul_entropie(chemin_fichier)
27         print(f"{nom_fichier} : {ent:.4f} bits par octet")
28
```

FIGURE 1 – code python pour calculer l'entropie des differents fichiers inclus dans un dossier

Analyse des resultats :  $H(\text{texte}) \approx 1.5$  bits/caractère  $H(\text{JPEG}) \approx 7.2$  bits/octet  $H(\text{AES}) \approx 7.9$  bits/octet

| Résultat                                     | Analyse   |
|--|---|
| $H(\text{texte}) \approx 1.5$ bits/caractère | Faible entropie : texte très structuré et redondant.                    |
| $H(\text{JPEG}) \approx 7.2$ bits/octet      | Entropie élevée : données compressées mais avec une certaine structure. |
| $H(\text{AES}) \approx 7.9$ bits/octet       | Très forte entropie : données presque aléatoires (chiffrement).         |

TABLE 1 – Analyse des entropies en fonction de leurs valeurs

Déterminons un seuil de détection de chiffrement automatique : a partir d'une valeur d'entropie de 7,7bits/octet on admet que le fichier est certainement chiffré.

### 2.2 Théorie des Graphes en Investigation Criminelle

## 3 Revolution Quantique et Ses Implications

### 3.1 Expérience de Pensée Schrödinger Adaptée

1. Conception une version numérique du chat de Schrödinger.

Un PC est infecté par un virus qui corrompt les fichiers .docx sur le disque l'un après l'autre. L'utilisateur du PC se souvient avoir saisi son devoir d'investigation numérique sous word mais a oublié le nom d'enregistrement du fichier en question encore moins le répertoire. Il ne peut donc pas récupérer son dossier rapidement. Il se demande si le fichier est déjà corrompu par le virus.

Dans ce cas d'usage le fichier existe dans un état corrompu et sain à la fois.

2. Un fichier existe-t-il dans un état superposé «présent/effacé » avant analyse ?

Réponse : OUI

3. Quel impact sur la notion de preuve « certaine » en justice ? Problématique : en droit, une preuve doit être objective, intègre et vérifiable.

Si un fichier peut être considéré comme simultanément présent ou effacé :

Incertitude sur l'existence → la preuve peut être contestée avant extraction.

Effet de l'observation : certaines méthodes de récupération peuvent modifier ou corrompre le fichier, compromettant son intégrité.

Conséquence juridique : l'extraction de preuve doit être faite selon un protocole garantissant que l'observation n'altère pas l'objet de la preuve (principe de conservation des données numériques).

4. Rédigez un protocole d'observation minimisant l'effet sur le système.

Poser le curseur sur le repertoire contenant le fichier ou utiliser un logiciel capable de scanner le repertoire sans l'ouvrir.

### **3.2 Analyse du Théorème de Non-Clonage**

1. Expliquez pourquoi le théorème de non-clonage empêche la copie parfaite d'état quantiques

## **4 Paradoxe de l'Authenticité Invisible**