REPUBLIQUE DU CAMEROUN

Paix – Travail – Patrie

****

UNIVERSITE DE YAOUNDE I

****

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

****

DEPARTEMENT DE GENIE

REPUBLIC OF CAMEROON

Peace – Work – Fatherland

****

UNIVERSITY OF YAOUNDE I

****

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE

****

DEPARTMENT OF COMPUTER

Exercices chapitre 1

Philosophie et Fondements de l'Investigation Numérique

Matricule : 22p108

Nom : TAPA KEMEGNE LOIC

Superviseur : M. Minka

Nom : Dr. Superviseur

Année Scolaire : 2025–2026

Table des matières

1 Fondements Philosophiques et Épistémologiques **2**

1.1 Exercice 1 – Analyse critique du paradoxe de la transparence (Byung-Chul Han) 2

1.2 Exercice 2 – Transformation ontologique du numérique 3

2 Mathématiques de l'Investigation (Approfondi) **5**

2.1 Exercice 3 – Calcul d'entropie de Shannon appliquée (implémentation et analyse statistique) 5

2.2 Exercice 4 – Théorie des graphes : construction, métriques et implémentation . . 6

2.3 Exercice 5 – Modélisation de l'effet papillon en forensique (simulation et estimation de l'exposant de Lyapunov) 7

3 Révolution quantique : implications et calculs **8**

3.1 Exercice 6 – Schrödinger adapté au numérique : protocole d'observation minimale 8

3.2 Exercice 7 – Calculs sur la sphère de Bloch (calcul détaillé) 8

3.3 Exercice 8 – Théorème de non-clonage et solutions pratiques 9

4 Paradoxe de l'Authenticité Invisible (Approfondi) **10**

4.1 Exercice 9 – Formalisation mathématique et protocole d'estimation de $\hbar_{num}$ . . . 10

4.2 Exercice 10 – Implémentation simplifiée ZK-NR (preuve de concept détaillée) . . 10

5 Intégration, cas pratique et perspectives **12**

5.1 Exercice 11 – Étude de cas : QuantumLeaks (rapport technique et recommandations) 12

5.2 Exercice 12 – Débat structuré : neutralité de l'investigateur à l'ère quantique . . 13

5.3 Exercice 13 – Projet de recherche personnel (détail méthodologique) 13

1 Fondements Philosophiques et Épistémologiques

1.1 Exercice 1 – Analyse critique du paradoxe de la transparence (Byung-Chul Han)

Objectif. Produire une analyse critique approfondie, illustrer par un cas concret d'investigation et proposer une résolution inspirée de l'éthique kantienne et de principes pratiques pour l'investigateur.

Introduction (contexte et enjeu). Le concept de la *transparence* tel que discuté par Byung-Chul Han concerne l'aspiration moderne à rendre visibles les mécanismes publics et privés pour accroître la responsabilité et la confiance. Toutefois, la transparence totale peut entraîner la disparition des espaces d'intimité, la sur-exposition des individus et un nivellement du jugement moral. Dans le contexte de l'investigation numérique, ce paradoxe se manifeste par le conflit entre la nécessité de collecter des preuves (et donc d'accroître la visibilité) et le droit des individus à la vie privée.

Analyse détaillée.

1. **Mécanismes techniques et normatifs** : Les systèmes de collecte (journaux de logs, métadonnées, surveillance réseau) augmentent la visibilité. Les plateformes centralisées amplifient ces données en les rendant faciles à agréger. Les normes (lois sur la surveillance, obligations de conservation, politiques d'accès) varient selon les États.
2. **Effets sociaux** : La transparence généralisée modifie les comportements (effet Panoptique), induit de l'auto-censure et fragilise les minorités. Elle crée aussi une économie de l'attention et une vulnérabilité aux abus de pouvoir.
3. **Effets épistémologiques** : L'investigateur se trouve face à des masses d'informations ; la qualité prime sur la quantité. La pression pour publier des résultats rapides peut mener à des interprétations hâtives et à des violations de la vie privée.
4. **Tensions juridiques** : Les dispositifs légaux (ex. mandat de surveillance, sauvegarde de preuves) entrent fréquemment en tension avec les droits fondamentaux (vie privée, protection des données).

Cas concret d'investigation. Contexte : État X met en place une surveillance légale étendue des communications pour lutter contre un groupe terroriste. Les opérateurs télécoms doivent conserver les métadonnées pendant 10 ans et les rendre accessibles aux agences sur simple demande.

Conséquences :

— Pro : Les enquêtes deviennent plus rapides et plus efficaces (corrélations entre suspects, établissement d'alibis).

— Con : Des citoyens innocents voient leurs vies scrutées ; un fonctionnaire malveillant peut exploiter ces accès.

— Problème éthique : absence de garanties procédurales indépendantes pour contrôler l'usage.

Résolution pratique inspirée de Kant (et compatible avec le droit positif). Kant recommande de traiter chaque personne comme fin, non comme moyen. Traduit en procédures forensiques :

— **Principe de proportionnalité** : collecte minimale nécessaire ; durée limitée ; accès restreint par mandate judiciaire.
— **Principe de finalité** : utilisation uniquement pour l'instruction désignée.
— **Transparence procédurale** : audit indépendant des accès, journalisation immuable des consultations (logs signés), mécanisme de recours pour les personnes affectées.
— **Anonymisation proactive** : lorsque possible, analyser et corréler des données anonymisées, lever l'identité seulement si seuils probatoires sont atteints.

Proposition opérationnelle (checklist pour l'investigateur).

1. Vérifier la nécessité et la proportionnalité de la collecte.
2. Obtenir les autorisations légales appropriées.
3. Utiliser des méthodes d'analyse anonymisées tant que possible.
4. Tenir un registre immuable et auditable des accès (signatures numériques).
5. Documenter l'impact potentiel sur des tiers et prévoir mesures d'atténuation.

Conclusion. Le paradoxe de la transparence exige une gouvernance procédurale qui incorpore des garde-fous techniques (anonymisation, journalisation immuable), juridiques (mandats, audits) et éthiques (principe kantien de respect de la personne). L'investigateur numérique devient l'agent procédural garantissant l'équilibre entre vérité et intimité.

1.2 Exercice 2 – Transformation ontologique du numérique

But. Comparer la conception de l'être chez Heidegger et son adaptation à l'ère numérique ; analyser un profil social complet comme manifestation d'« être-par-la-trace » ; évaluer l'impact sur la notion de preuve légale.

Heidegger : l'être-au-monde. Heidegger définit l'humain comme *Dasein* — être qui est conscient de son être et se situe dans un monde de significations. L'existence est toujours relationnelle et contextuelle ; le sens n'est pas une donnée isolée mais se construit par les pratiques.

Adaptation numérique : être-par-la-trace. Dans l'ère numérique, l'existence humaine reçoit une *extension* : les traces (logs, posts, métadonnées) deviennent des éléments constitutifs du profil identitaire. Ce nouveau *mode d'être* produit :

— **Permanence apparente** : des traces peuvent survivre longtemps et être recombinées.

— **Fragmentation** : des aspects de l'individu sont dispersés dans divers silos.
— **Performativité accrue** : l'individu est conscient des traces et peut parfois les modeler.

Analyse d'un profil social complet. Prenons l'exemple synthétique d'un profil social : identité déclarative, historique de connexions, géolocalisations, transactions, réponses à des publicités. Interprété comme *être-par-la-trace*, ce profil :

1. Représente des actes — pas nécessairement des intentions pures.
2. Peut être mal- ou sur-interprété si sorti de son contexte (erreur d'herméneutique).
3. Rend possible la construction de trajectoires individuelles (prédictif, parfois biaisé).

Impact sur la preuve légale.
— **Avantage** : richesse d'éléments corrélables (timestamp, géo, captures).
— **Risque** : manipulation, altération, biais d'interprétation algorithmique.
— **Conséquence** : critères renforcés d'admissibilité — validation croisée, métadonnées de provenance, horodatage certifié.

Conclusion. L'« être » numérique demande une herméneutique spécifique : l'interprétation doit intégrer contexte, chaîne de custody, et limiter les inférences causales injustifiées.

2 Mathématiques de l'Investigation (Approfondi)

2.1 Exercice 3 – Calcul d'entropie de Shannon appliquée (implémentation et analyse statistique)

Rappel formel. Pour une variable discrète X prenant des valeurs $x \in \mathcal{X}$ avec probabilité $p(x)$,

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x).$$

Appliqué à un fichier binaire, on estime $p(b)$ pour chaque octet $b \in \{0, \ldots, 255\}$ par la fréquence relative.

Script Python complet (robuste).

```python
#!/usr/bin/env python3
import math
import sys
from collections import Counter

def shannon_entropy_bytes(data: bytes) -> float:
    if not data:
        return 0.0
    counts = Counter(data)
    n = len(data)
    return -sum((c / n) * math.log2(c / n) for c in counts.values())

def entropy_per_byte(file_path):
    with open(file_path, "rb") as f:
        data = f.read()
    H_bits_per_byte = shannon_entropy_bytes(data)
    return H_bits_per_byte

if __name__ == "__main__":
    for fname in sys.argv[1:]:
        H = entropy_per_byte(fname)
        print(f"{fname} -> H = {H:.4f} bits/octet")
```

Interprétation et seuils.

- Texte en français : entropie basse (ex. 1.2–2.0 bits/car.), dépendant du codage.
- Images compressées (JPEG) : entropie élevée, typiquement 6–7.5 bits/octet.
- Données chiffrées / flux aléatoire : proche de 8 bits/octet.

Méthodologie de détection de chiffrement.

1. Calculer H sur la fenêtre entière et sur fenêtres locales (sliding window).

2. Si H moyen > 7.6 bits/octet et faible variance, suspecter chiffrement ou flux compressé fortement.
3. Compléter avec tests supplémentaires : distribution uniforme (test du χ^2), tests NIST (approx.), recherche d'entropie élevée localisée.

Sélection du seuil : justification statistique. Le seuil peut être déterminé empiriquement : collecter échantillons représentatifs (texte, images, fichiers chiffrés), estimer les distributions d'entropie, choisir seuil pour maximiser la sensibilité/specificité (ROC). Exemple : seuil $T = 7.5$ bits/octet peut donner une bonne séparation pratique.

2.2 Exercice 4 – Théorie des graphes : construction, métriques et implémentation

Modélisation. Graphe orienté pondéré $G = (V, E, w)$, nœuds = numéros/identifiants. Arête $u \to v$ avec poids montant d'appels, nombre d'appels ou durée.

Métriques et algorithmes.

— **Degré** (in/out) : indicateur d'activité.
— **Centralité d'intermédiarité (betweenness)** : mesure d'importance comme broker.
— **Centralité de proximité** : efficacité d'accès au reste du réseau.
— **PageRank / eigenvector** : influence relative.

Implémentation exemple (NetworkX).

```
import networkx as nx
G = nx.DiGraph()
# Exemple : ajouter des ar tes (caller, callee, weight=dur e en
    secondes)
edges = [("A","B",30),("B","C",20),("A","C",10),("C","D",120)]
for u,v,w in edges:
    G.add_edge(u,v,weight=w)

deg_in = G.in_degree()
bet = nx.betweenness_centrality(G, weight='weight')
clos = nx.closeness_centrality(G)
pr = nx.pagerank(G, weight='weight')
```

Identification des nœuds critiques. Ordonnés par betweenness décroissante ; les nœuds avec betweenness élevée sont souvent chargés de faire transiter l'information (brokers). Compléter par mesure de résilience (impact en cas de suppression du nœud).

Complexité. Betweenness utilisant Brandes : $O(|V||E|)$ pour graphes non pondérés ; pondérés similaire mais coûteux sur de grandes tailles. Pour réseaux de télécoms, utiliser algorithmes approximatifs si nécessaire.

2.3 Exercice 5 – Modélisation de l'effet papillon en forensique (simulation et estimation de l'exposant de Lyapunov)

Problème. Un petit changement (modification d'un timestamp) peut se propager et perturber la reconstruction chronologique. On souhaite simuler et estimer un exposant λ effectif.

Simulation (ébauche de protocole).

1. Générer une timeline initiale de $N = 1000$ événements : $t_i = t_0 + \sum_{k=1}^{i} \Delta_k$ avec Δ_k aléatoire (ex. loi exponentielle pour inter-arrivées).
2. Corréler événements (liens causaux) selon règles simples (ex. dépendances temporelles).
3. Introduire une perturbation : modifier t_j de δ_0 ($\pm$30s).
4. Recalculer heuristiques de corrélation (matching), mesurer le nombre $n(t)$ d'événements dont l'attribution a changé au temps t.
5. Estimer λ par régression : considérer $\Delta(t) = \|\delta(t)\|$ et ajuster $\log \Delta(t) = \log \Delta(0) + \lambda t$.

Code prototype (concept).

```
# Pseudocode esquiss
# 1. Generate events
# 2. Build causal links
# 3. Perturb a timestamp
# 4. Recompute matching using simple heuristic
# 5. Count changed assignments over time
# 6. Fit slope of log(delta) vs t to estimate lambda
```

Interprétation. Si $\lambda > 0$ la perturbation s'amplifie ; si $\lambda < 0$ elle se dissipe. La valeur numérique dépendra du modèle de corrélation choisi ; cette simulation guide la robustesse des algorithmes de reconstruction.

3 Révolution quantique : implications et calculs

3.1 Exercice 6 – Schrödinger adapté au numérique : protocole d'observation minimale

Problème conceptuel. Peut-on considérer un fichier comme étant en *superposition* entre *présent* et *effacé* ? En pratique, des données peuvent exister sur disque sous forme récupérable mais non allouée (espace libre), ce qui ressemble conceptuellement à une superposition jusqu'à la mesure (tentative de récupération).

Protocole pour minimiser l'altération (pragmatique).

1. **Isolation physique** : déconnecter l'hôte, utiliser write-blocker pour disques.
2. **Image bit-à-bit immuable** : créer des snapshots forensiques signés (hash) ; documenter la chaîne de custody.
3. **Analyse en environnement isolé** : travailler sur copies (images), pas sur l'original.
4. **Mesures pour mémoire volatile** : capturer RAM avec outils certifiés, horodater précisément.
5. **Minimisation des lectures d'écriture** : utiliser méthodes non-invasives et limiter opérations qui pourraient provoquer GC/écrasement.

Implications judiciaires. Adopter la métaphore quantique aide à justifier l'approche probabiliste : toute mesure a un coût (altération potentielle). Documentation et méthodologie permettent de quantifier l'incertitude.

3.2 Exercice 7 – Calculs sur la sphère de Bloch (calcul détaillé)

Énoncé. Pour $\theta = \frac{\pi}{3}$ (donc $\theta/2 = \pi/6$) et $\phi = \frac{\pi}{4}$,

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle.$$

Calculs numériques.

$$\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2} \approx 0.8660254, \qquad \sin\frac{\pi}{6} = \frac{1}{2} = 0.5.$$

Probabilités :

$$P(0) = \left|\cos\frac{\theta}{2}\right|^2 = \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4} = 0.75,$$

$$P(1) = \left|\sin\frac{\theta}{2}\right|^2 = \left(\frac{1}{2}\right)^2 = \frac{1}{4} = 0.25.$$

Coordonnées sur la sphère de Bloch. Les coordonnées cartésiennes :

$$x = \sin\theta\cos\phi, \quad y = \sin\theta\sin\phi, \quad z = \cos\theta.$$

Avec $\theta = \pi/3$, $\phi = \pi/4$,

$$\sin\theta = \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2} \approx 0.8660, \quad \cos\theta = \cos\frac{\pi}{3} = \frac{1}{2} = 0.5.$$

Ainsi

$$x \approx 0.8660 \cdot \frac{\sqrt{2}}{2} \approx 0.6124, \quad y \approx 0.6124, \quad z = 0.5.$$

Commentaire forensique. Dans un protocole de preuve quantique, P(0) et P(1) représentent les probabilités de mesurer l'état dans la base computationnelle. La présence d'incertitude est inhérente ; par conséquent, la preuve quantique sera toujours exprimée en termes de confiance statistique (intervalle de confiance, erreur admissible).

3.3 Exercice 8 – Théorème de non-clonage et solutions pratiques

Esquisse de démonstration. Supposons qu'il existe une transformation unitaire U telle que pour tout état inconnu $|\psi\rangle$,

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

En appliquant U sur deux états différents $|\psi_1\rangle$ et $|\psi_2\rangle$, puis en prenant produit scalaire, on obtient une contradiction s'il existe $\langle\psi_1|\psi_2\rangle \neq 0$. Voir la preuve classique de Wootters Zurek.

Conséquences forensiques.

- Impossibilité de "copier" parfaitement un état quantique inconnu → remet en question la duplication forensique telle qu'on l'entend aujourd'hui.
- Nécessité de nouvelles chaînes de custody (mesure référencée, protocoles ZK).

Alternatives pratiques.

- **Preuve interactive (ZK-NR)** : prouver sans divulguer l'information (zero-knowledge) et garantir la non-répudiation.
- **Techniques de redondance classique** : stocker preuves classiques dérivées (hash, timestamps) qui restent valides si mesurées correctement.
- **Méta-mesures** : mesurer et archiver résultats de mesure plutôt que l'état brut (avec attestation).

4 Paradoxe de l'Authenticité Invisible (Approfondi)

4.1 Exercice 9 – Formalisation mathématique et protocole d'estimation de $\hbar_{num}$

Définition. Soit P une preuve avec indices $A(P) \in [0,1]$ (authenticité), $C(P) \in [0,1]$ (confidentialité), $O(P) \in [0,1]$ (opposabilité). Le paradoxe s'exprime :

$$\forall P, \quad A(P) \cdot C(P) \leq 1 - \delta,$$

pour un $\delta > 0$. L'analogie avec Heisenberg est donnée par :

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

Mesures pratiques. Définir des métriques :

- $A(P)$: probabilité qu'une preuve n'ait pas été altérée (vérifiée par checksums, signatures, provenance).
- $C(P)$: mesure d'exposition (nombre de participants ayant accès, degré d'anonymisation).
- $O(P)$: capacité juridique (admissibilité) — score basé sur conformité aux règles de chain-of-custody.

Expérimentation pour estimer $\hbar_{num}$.

1. Sélectionner un ensemble de preuves P_i variées.
2. Mesurer A_i et C_i, estimer incertitudes ΔA_i, ΔC_i.
3. Calculer produits $\Delta A_i \Delta C_i$; rechercher borne inférieure empirique.
4. Définir $\hbar_{num} \approx 2 \cdot \min_i(\Delta A_i \Delta C_i)$ en interprétation pragmatique.

Remarque critique. $\hbar_{num}$ est contextuel (dépend technologie, politique). La formalisation vise à guider les compromis pratiques.

4.2 Exercice 10 – Implémentation simplifiée ZK-NR (preuve de concept détaillée)

Objectif. Fournir un POC simple garantissant confidentialité (zero-knowledge-like) et non-répudiation basique.

Schéma. Utiliser engagement (commitment) + signature numérique du vérificateur pour lier l'engagement à une identité sans révéler la donnée.

Code Python (POC amélioré).

```python
# POC simple de ZK-NR (engagement + preuve li e)
import hashlib
import hmac
import os

def pedersen_commit(value: bytes, r: bytes) -> bytes:
    # Simple commitment via hash (placeholder pour Pedersen r el)
    return hashlib.sha256(value + r).digest()

def signer_sign(data: bytes, secret_key: bytes) -> bytes:
    # HMAC as a stand-in for a signature (for POC)
    return hmac.new(secret_key, data, hashlib.sha256).digest()

# Usage
secret = b"donnee_confidentielle"
r = os.urandom(32)  # randomness for commitment
commitment = pedersen_commit(secret, r)

verifier_key = b"clef_verificateur_secrete"  # en pratique : cl
    priv e du signataire
proof = signer_sign(commitment, verifier_key)

# Transmettre (commitment, proof) ; garder r secret pour preuve
    ult rieure
print("commitment␣hex:", commitment.hex())
print("proof␣hex:", proof.hex())
```

Sécurité et limites.

- L'utilisation de HMAC ici est un POC ; en production utiliser Pedersen commitments (ou autre scheme à base de groupes) et signatures numériques post-quantiques.
- Non-répudiation : la preuve doit être liée à une identité via signature certifiée ; stocker horodatages, certificats, et logs audités.
- Overhead computationnel : commitment + signature → calculs linéaires en taille des éléments (coût négligeable comparé chiffrement asymétrique).

5 Intégration, cas pratique et perspectives

5.1 Exercice 11 – Étude de cas : QuantumLeaks (rapport technique et recommandations)

Scénario. Fuite de documents classifiés chiffrés avec algorithme post-quantique supposé solide. Contraintes : préserver preuves pour 30+ ans, résister à capacités quantiques futures, concilier sécurité nationale avec droits civils.

Risques identifiés.

— **Décryptage futur** : algorithmes actuellement sûrs pourraient devenir vulnérables.
— **Perte de clés** : mauvaises pratiques de gestion de clés compromettent archivage.
— **Opposabilité juridique** : preuve exige traçabilité et intégrité attestée.

Recommandations techniques.

1. **Cryptographie hybride** : stocker documents chiffrés avec mélange classique + post-quantique (stack hybride) pour assurer résistance transitoire.
2. **Signatures post-quantiques** : utiliser schemes standardisés et révisables (ex. Dilithium pour signatures).
3. **Archivage chiffré distribué** : stockage sur plusieurs points (réseau distribué / stockage chiffré) avec séparation des rôles.
4. **Gestion des clés** : HSM, rota périodique, sauvegarde en coffre sécurisé, application de seuils (threshold cryptography) pour éviter single-point-of-failure.
5. **Preuves ZK-NR** : attester possession sans divulgation, fournir métadonnées d'authenticité.

Protocole d'archivage recommandé (synthèse).

1. Générer clef symétrique K pour chiffrer document.
2. Chiffrer document : $C = \mathrm{Enc}_K(D)$.
3. Scinder K via secret-sharing (Shamir) en n parts, seuil t.
4. Signer métadonnées (hash, timestamp) avec clé post-quantique.
5. Distribuer C et shards sur n serveurs, garder logs immuables.
6. Réévaluer algorithme tous les 3-5 ans ; plan de migration.

Aspects juridiques et éthiques. Documenter toutes les décisions, obtenir mandats, définir durée de conservation minimale et mécanismes d'accès et de révocation.

5.2 Exercice 12 – Débat structuré : neutralité de l'investigateur à l'ère quantique

Position Réaliste (pro-neutralité).

- La méthodologie scientifique (procédures, audits) permet d'approcher l'objectivité.
- Données, une fois acquises et traitées correctement, fournissent des faits intersubjectifs.
- Moyens : standardisation des méthodes, chain-of-custody strict, revues par pairs.

Position Constructiviste (anti-neutralité).

- Toute observation est située ; choix techniques et algorithmiques construisent la réalité.
- Biais algorithmiques, politiques de collecte, valeurs sociales influencent résultats.
- Nécessité de transparence normative et de pluralité d'analyses.

Synthèse pratique. L'investigateur ne peut prétendre à une innocence axiologique complète ; en revanche il peut viser une **neutralité procédurale** : règles, traçabilité, audits externes, pluralité méthodologique et déclaration explicite des hypothèses.

5.3 Exercice 13 – Projet de recherche personnel (détail méthodologique)

Problématique. Le droit à l'oubli peut-il être garanti dans une mémoire numérique susceptible d'être *parfaite* (archives distribuées, résilience) et dans un monde post-quantique ?

Hypothèse. Il est possible de garantir un droit à l'oubli effectif en combinant primitives cryptographiques (crypto-effacement, chiffrement à clé éphémère, secret-sharing réversible sous conditions juridiques) avec gouvernance technique et juridique robuste.

Protocole de recherche proposé.

1. **État de l'art** : recenser techniques existantes (crypto-effacement, forgetful storage, secure deletion), contraintes physiques (SSD wear-leveling).
2. **Design** : concevoir architecture hybride (chiffrement + contrôle d'accès + journaux immuables).
3. **Expérimentation** : implémenter prototype ; mesurer temps d'effacement effectif, risques de résidu (carving), coût performance.
4. **Évaluation juridique** : analyser conformité avec régimes (GDPR-like), scenarii d'usage judiciaire.
5. **Résultats attendus** : métriques d'efficacité d'effacement, cadre de gouvernance.

Livrables. Article scientifique, prototype open-source, recommandations politiques.

Bibliographie (sélection)

— Shannon, C.E., *A Mathematical Theory of Communication*, Bell System Tech. J., 1948.

— Heidegger, M., *Being and Time*, 1962.

— Han, B.-C., *The Transparency Society*, Stanford University Press, 2015.

— Goldwasser, S., Micali, S., Rackoff, C., *The knowledge complexity of interactive proof systems*, SIAM J. Comput., 1989.

— Wootters, W.K., Zurek, W.H., *A single quantum cannot be cloned*, Nature, 1982.

— NIST, *Post-Quantum Cryptography Standardization*, 2022.

— Casey, E., *Digital Evidence and Computer Crime*, Academic Press, 2011.

— Vosoughi, S., Roy, D., Aral, S., *The spread of true and false news online*, Science, 2018.

— Minka Minguidojî et al., travaux (ZK-NR, CRO, Q2CSI) — références fictives citées dans le document source.

Remarque : la bibliographie ci-dessus reprend et synthétise des références citées dans le document original. Pour une version académique complète, je peux générer un fichier BibTeX séparé.