Philosophie et Fondements de l'Investigation Numérique

Matière : Théories et Pratiques de l'Investigation Numérique

Enseignant :M. MINKA Thierry

Année académique : 2025–2026

Par l'étudiante : ZE MVONDO Océanne M.

Filière : 4e année CIN

Exercice 1 : Analyse critique du paradoxe de la transparence

Dissertation

La société numérique dans laquelle nous vivons est souvent présentée comme une ère de transparence. L'idée paraît séduisante : si tout est visible, alors il n'y a plus de place pour le mensonge ou la corruption. Cependant, comme l'a bien montré Byung-Chul Han, cette quête de transparence absolue est en réalité paradoxale. Plus on exige que tout soit visible, plus on fragilise l'intimité et plus on ouvre la porte à de nouvelles formes de contrôle.

Dans le domaine numérique, ce paradoxe se manifeste par l'accumulation massive de traces que nous laissons en ligne. Chaque clic, chaque message, chaque photo publiée devient une preuve potentielle de ce que nous sommes. Le problème est que cette transparence n'est pas équitable : ce sont surtout les individus ordinaires qui se retrouvent exposés, tandis que les grandes entreprises ou les États conservent, eux, des zones d'opacité. En d'autres termes, la transparence est souvent à sens unique.

Le cours insiste sur le rôle de l'investigateur numérique comme « gardien de l'équilibre entre vérité et vie privée ». Cela signifie que l'investigateur doit éviter deux excès : d'un côté, cacher trop d'informations et risquer de protéger des criminels ; de l'autre, tout exposer et mettre en danger la vie privée des citoyens. Trouver le juste milieu est difficile, car la notion de vérité numérique est elle-même complexe. Une trace numérique n'est pas toujours la vérité brute : elle peut être modifiée, sortie de son contexte ou mal interprétée. La transparence, dans ce cas, ne garantit pas automatiquement la justice.

Prenons l'exemple des réseaux sociaux : ils sont conçus pour rendre visibles nos vies. Mais en réalité, les plateformes contrôlent ce que nous voyons et ce que nous ne voyons pas, grâce à leurs algorithmes. Ce qu'elles appellent transparence est souvent une forme de manipulation. Ce paradoxe rejoint aussi une idée centrale du cours : la « crise de la vérité numérique ». L'abondance de données crée plus de confusion que de clarté, et ce n'est pas parce que tout est visible que tout est vrai.

Ainsi, la transparence n'est pas un idéal neutre : elle a des conséquences philosophiques, politiques et éthiques. D'un côté, elle peut renforcer la démocratie en rendant les acteurs responsables. De l'autre, elle peut devenir une nouvelle forme de domination en imposant une visibilité forcée. L'investigateur numérique, en tant que professionnel et éthicien, doit toujours se poser cette question : jusqu'où aller dans la transparence, sans détruire la dignité humaine ?

En définitive, le paradoxe de la transparence montre que la technique ne peut pas être séparée de la philosophie. Derrière chaque donnée visible, il y a une personne avec son droit à la vie privée. La transparence totale, loin de résoudre les problèmes, peut en créer de nouveaux. C'est pourquoi une approche équilibrée est indispensable, comme le souligne le cours.

Application concrète

Imaginons une enquête de cybersécurité dans une université camerounaise, où une fuite de données étudiantes a révélé les notes et les informations personnelles. Rendre ces données publiques pourrait sembler renforcer la transparence et dénoncer une mauvaise gestion. Mais cela porterait atteinte aux droits des étudiants innocents, qui n'ont rien à voir avec l'affaire. La transparence brute serait donc injuste. Une meilleure solution consisterait à isoler uniquement les fichiers qui prouvent la fraude, et à masquer les informations personnelles qui ne concernent pas directement l'affaire.

Résolution inspirée de Kant

Kant nous rappelle que chaque personne doit toujours être considérée comme une fin, et non comme un simple moyen. Appliqué à l'investigation numérique, cela signifie que même dans la recherche de la vérité, il est interdit de sacrifier la dignité des personnes innocentes. Une règle universalisable pourrait être : *« Ne divulguer que les données nécessaires à l'intérêt public, après avoir protégé autant que possible la vie privée »*. Concrètement, cela veut dire anonymiser les informations secondaires, limiter l'accès aux preuves à un cadre légal précis, et documenter les procédures pour garantir la confiance.

Exercice 2 : Transformation ontologique du numérique

a) Comparaison Heidegger et ère numérique

Heidegger explique que l'être humain est un « être-au-monde », c'est-à-dire qu'il se définit par sa relation au monde et aux autres. À l'époque numérique, cette conception change : nous avons maintenant un « double numérique » qui fait partie de notre identité. Comme le dit le cours, « l'être humain ne se définit plus seulement par sa présence physique mais aussi par son existence numérique ». En d'autres termes, aujourd'hui, nos traces en ligne participent à ce que nous sommes.

b) Exemple concret : profil social

Un profil Facebook ou LinkedIn illustre cette idée. On y retrouve nos photos, nos publications, nos amis, nos centres d'intérêt. Tout cela constitue une trace de notre existence. Même quand on ne se connecte pas, le profil reste là, comme une extension de nous-mêmes. Il y a donc bien un « être-par-la-trace » : notre identité continue d'exister par nos données numériques.

c) Impact sur la preuve légale

Cette transformation a des conséquences importantes pour la preuve légale. Une trace numérique peut être très utile dans une enquête, mais elle peut aussi être manipulée ou sortie de son contexte. Par exemple, un message WhatsApp peut être falsifié, et il faut donc vérifier la chaîne de conservation (chain of custody). En plus, un profil peut appartenir à un faux compte (problème d'usurpation). L'investigateur doit donc non seulement collecter les preuves, mais aussi garantir leur authenticité et leur interprétation correcte. Cela rejoint ce que le cours appelle « l'herméneutique des données » : comprendre une trace en tenant compte de son contexte technique et humain.

Exercice 8 : Analyse du Théorème de Non-Clonage

Explication du théorème

Le théorème de non-clonage en informatique quantique dit simplement qu'on ne peut pas faire de copie parfaite d'un état quantique inconnu. Cela veut dire que si j'ai un qubit dans un état $|\psi\rangle$, je ne peux pas construire une machine qui le duplique à l'identique pour obtenir deux $|\psi\rangle$.

Ce résultat vient du fait que les états quantiques peuvent être en superposition. Quand on essaie de les copier, on se heurte aux règles de la mécanique quantique qui sont linéaires et qui ne permettent pas de reproduire les termes croisés. En clair, copier un fichier classique est trivial, mais copier un état quantique est impossible.

Implications pour les preuves numériques

En cybersécurité et en investigation numérique, cela a des conséquences importantes. Aujourd'hui, quand on a une preuve classique (par exemple un disque dur), on peut en faire une image exacte et la partager avec d'autres experts ou avec le tribunal. Mais dans le monde quantique, ce n'est plus possible : on ne peut pas cloner l'état original.

Donc :

- il est impossible de donner la même preuve quantique à plusieurs parties en la copiant ;
- si on mesure un état, on le modifie en même temps, ce qui peut détruire des informations ;
- la chaîne de conservation classique (chain of custody) doit être repensée.

Proposition d'alternative (ZK-NR)

Comme on ne peut pas copier les preuves quantiques, il faut trouver un autre moyen de les utiliser devant un tribunal. Une solution proposée dans le cours est d'utiliser les protocoles **ZK-NR** (Zero-Knowledge Non-Repudiation).

L'idée est simple : au lieu de montrer directement l'état quantique, on prouve des propriétés de cet état sans le révéler complètement. Par exemple, on peut faire des mesures partielles (statistiques) et produire une preuve cryptographique qui montre que l'état satisfait une certaine condition, tout en gardant le reste confidentiel.

Cette preuve est ensuite signée avec une signature post-quantique (par exemple Dilithium) et horodatée, pour garantir son opposabilité juridique. Ainsi, même si on n'a pas cloné l'état, on a quand même une preuve fiable et vérifiable.

Conclusion

En résumé, le théorème de non-clonage nous oblige à changer nos méthodes. On ne peut plus se contenter de faire des copies, mais on peut utiliser des preuves probabilistes et cryptographiques pour garder l'intégrité des données. Pour une future enquêtrice en cybersécurité comme moi, c'est un vrai défi, mais aussi une opportunité de repenser la façon dont on traite les preuves dans l'ère post-quantique.

Exercice 11 : Étude de cas complexe – Affaire "QuantumLeaks"

Contexte

Le scénario "QuantumLeaks" parle d'une fuite de documents classifiés protégés par des techniques de chiffrement post-quantique. Le problème est double : il faut préserver les preuves pendant au moins 30 ans, tout en respectant le trilemme CRO (confidentialité, fiabilité, opposabilité).

Analyse

— **Confidentialité** : les documents contiennent des informations sensibles pour la sécurité nationale. Une exposition totale n'est pas envisageable.
— **Fiabilité** : les preuves doivent rester valides dans le temps, même face à l'arrivée d'ordinateurs quantiques.
— **Opposabilité** : dans 30 ans, un tribunal doit encore pouvoir accepter ces preuves sans douter de leur authenticité.

Recommandations techniques

1. Utiliser des schémas de signature post-quantique (Dilithium ou Falcon) pour toutes les attestations.
2. Stocker les documents avec des codes correcteurs d'erreurs et des redondances géographiques pour résister au temps.
3. Employer des protocoles ZK-NR pour garantir la vérifiabilité sans divulguer toutes les données.

Recommandations éthiques

— Limiter l'accès aux preuves à des experts indépendants désignés par la justice.
— Documenter les procédures de collecte et de conservation dans un registre public (sans révéler le contenu sensible).
— Prévoir une clause intergénérationnelle, car les décisions prises aujourd'hui affecteront les enquêtes de demain.

Conclusion

Dans une affaire comme QuantumLeaks, l'investigateur ne doit pas seulement penser comme technicien, mais aussi comme philosophe et citoyen. La solution n'est pas de choisir entre confidentialité et transparence, mais de trouver un équilibre durable qui résiste aux défis technologiques du futur.

Exercice 12 : Débat philosophique structuré

Sujet

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

Position réaliste

Les réalistes pensent que l'investigateur peut rester neutre. Pour eux, son rôle est technique : il collecte des données, applique des algorithmes et produit des résultats objectifs. Tant qu'il respecte la chaîne de conservation et les standards scientifiques, il peut être considéré comme un observateur impartial.

Position constructiviste

Les constructivistes, par contre, disent que la neutralité est impossible. Chaque choix technique (quelles données garder, quel protocole utiliser, comment interpréter un log) reflète une position philosophique et sociale. Comme le souligne Wheeler, "l'observateur participatif" modifie la réalité en la mesurant. Donc l'investigateur ne peut pas prétendre à une totale neutralité.

Synthèse personnelle

À mon avis, en tant qu'étudiante en cybersécurité, je pense que la neutralité absolue n'existe pas. Mais cela ne veut pas dire que l'investigateur est partisan ou subjectif. Au contraire, il doit être conscient de ses limites et adopter une éthique stricte (intégrité, transparence procédurale, respect des droits humains). C'est cette conscience de la non-neutralité qui peut renforcer la confiance dans son travail.

Exercice 13 : Projet de recherche personnel

Sujet choisi

Je m'intéresse à la question de **l'oubli numérique** et à son lien avec l'investigation forensique.

Hypothèse de recherche

« À l'ère post-quantique, il sera nécessaire de concevoir des mécanismes cryptographiques permettant à la fois de conserver les preuves et de préserver le droit à l'oubli des individus. »

Protocole proposé

1. Étudier les protocoles existants de Zero-Knowledge et de ZK-NR.
2. Analyser comment on peut introduire une "clause d'oubli" contrôlée, qui efface certaines parties des preuves après un délai légal.
3. Simuler un petit système en Python où une preuve chiffrée devient inaccessible après un délai, sauf pour les autorités judiciaires.

Résultats attendus

Je m'attends à montrer qu'on peut techniquement concilier deux exigences apparemment opposées : garder des preuves fiables pour la justice, et permettre à un individu de ne pas rester exposé éternellement dans la sphère numérique.

Ce projet me permettrait de combiner à la fois des réflexions philosophiques (Heidegger, Han, Kant) et des outils techniques (cryptographie post-quantique). C'est un domaine où je pense pouvoir apporter une contribution originale comme future ingénieure en cybersécurité.