

Checklists OSINT

À imprimer et à cocher à chaque enquête. Formation OSINT.

1. Avant de commencer : cadre et légalité

Si une seule case reste vide, ne commencez pas.

- ☐ La question est **écrite**, précise et limitée dans son périmètre.
- ☐ La finalité est **légitime** et j'ai un mandat (employeur, client) ou il s'agit de moi-même.
- ☐ Aucune source prévue ne nécessite de contourner une protection (identifiant, faille, URL devinée).
- ☐ Si des données personnelles sont concernées : base légale identifiée, minimisation prévue.
- ☐ Pas de données sensibles (santé, opinions, religion, orientation...) ni de personne mineure.
- ☐ Si l'activité est faite pour un tiers à titre professionnel : cadre CNAPS vérifié.
- ☐ Une date de fin et de suppression des données est fixée.

2. Avant chaque session : OPSEC

Protéger votre identité, votre matériel et l'enquête.

- ☐ Profil de navigateur (ou machine virtuelle) dédié aux enquêtes ouvert.
- ☐ Aucun compte personnel connecté.
- ☐ Bloqueur de traqueurs actif, VPN actif si nécessaire.
- ☐ Journal d'enquête ouvert, horloge et fuseau horaire notés.
- ☐ Dossier d'enquête chiffré monté, outil d'archivage prêt.
- ☐ Réflexe : ne rien « aimer », suivre, commenter ni contacter.

3. Pour chaque élément trouvé : archivage

Le web change : archiver au moment où l'on consulte.

- ☐ URL complète notée.
- ☐ Date, heure et fuseau horaire notés.
- ☐ Capture pleine page enregistrée et nommée (AAAA-MM-JJ_HHMM_source).
- ☐ Fichier source conservé si utile (HTML, image originale, vidéo).
- ☐ Empreinte SHA-256 calculée et reportée dans le journal.
- ☐ Source évaluée (A à F) et information évaluée (1 à 6).

4. Avant de conclure : vérification

Une information non recoupée n'est qu'une hypothèse.

- ☐ Chaque fait important est confirmé par au moins deux sources **indépendantes**.
- ☐ Les homonymies ont été écartées par des éléments distincts (dates, identifiants, photos).
- ☐ J'ai cherché activement ce qui pourrait **réfuter** mon hypothèse.
- ☐ Faits établis, déductions et hypothèses sont clairement séparés.
- ☐ Chaque conclusion porte un niveau de confiance.

5. Avant de diffuser : rapport

Diffuser le nécessaire, rien de plus.

- ☐ Le rapport répond à la question posée, et seulement à elle.
- ☐ Aucune donnée personnelle inutile ; les tiers non concernés sont floutés.
- ☐ Aucune information permettant d'identifier ou de localiser une personne n'est publiée.
- ☐ Les métadonnées des fichiers transmis ont été supprimées.
- ☐ Les destinataires sont limités à ceux prévus ; relecture faite par un tiers.
- ☐ Fin de mission : données supprimées à la date prévue.